Table of Contents

Foreword

This report presents the results of an eight-month investigation initiated when more than a dozen whistleblowers contacted POGO with unclassified evidence that the U.S. Department of Energy's nuclear bomb complex is vulnerable to a terrorist attack.

The contents of this report have been reviewed by trained and certified classifiers from inside and outside the government to ensure that this report contains no classified information.

Report Contributors

POGO Staff

Danielle Brian, Executive Director
Lynn Eisenman, Research Assistant
Keith Rutter, Director of Operations

Peter Stockton, is a paid consultant with POGO. He was Special Assistant to DOE Secretary Bill Richardson from 1999-2001. Mr. Stockton was the Chief investigator for Chairman John Dingell (D-MI) of the House Energy and Commerce Committee from 1972-1995, including during the Committee's investigations of DOE security failures.

Unpaid Contributors: Ron Timm, RETA Security President, Security Analyst hired by DOE to analyze security at DOE weapons facilities. The additional contributors to this report have requested anonymity for fear of retaliation for exposing security failures. They include DOE security analysts, current and former Special Forces who portray mock-terrorists in force-on-force drills, DOE contractors, and officials at various levels of DOE Headquarters and facilities.

Executive Summary

The Department of Energy (DOE) analyzes and tests the security of nuclear weapons facilities by conducting simulations and mock force-on-force exercises, often using U.S. military forces as adversaries. The government requires that nuclear facilities be able to defend against theft of nuclear materials or radiological sabotage by a few terrorists using surprise and readily available weapons and explosives, as well as against the theft of nuclear secrets.

According to experts who have conducted these tests in the past, the government fails to protect against these attacks more than 50% of the time – although the exact figure is classified. For example, in a test at the Rocky Flats nuclear production facility, Navy SEALs successfully "stole" enough material to make multiple nuclear weapons. In a test at a Los Alamos facility, the "terrorists" had enough time to construct an Improvised Nuclear Device. In addition, the theft of nuclear secrets remains as possible today as it was several years ago before the controversy over the downloading of classified information at Los Alamos.

DOE employees and others who have raised security concerns have largely been ignored and subjected to retaliation over many years. This report details several case studies of whistleblowers being fired, being forced to resign, losing contracts or losing security responsibilities because they were unwilling to quietly accept the inadequate security measures at DOE nuclear facilities. In one example, in a desperate attempt to raise public awareness last year about these problems, a DOE employee faxed two unclassified Inspector General reports to *USA Today* and the *Washington Post*, which highlighted the Department's failure to take corrective measures. His security clearance was suspended and he is no longer working on security issues.

DOE's disregard for proven threats to nuclear security and its institutional bull-headedness has thwarted the efforts of reformers, time and time again. According to a review by Senator Warren Rudman, "scores of critical reports from the General Accounting Office (GAO), the intelligence community, independent commissions, private management consultants, its Inspector General, and its own security experts...the Department's ingrained behavior and values have caused it to continue to falter and fail."

Ten major sites have weapons-grade plutonium (PU) and highly-enriched uranium (HEU) in sufficient quantities to make a nuclear device even though most of them have not had a national defense mission since the end of the Cold War. Several of these sites are located near major metropolitan areas including the Bay area of Northern California; Denver, Colorado; Albuquerque, New Mexico; and Knoxville, Tennessee (see chart on page 7). In addition, the DOE Transportation Safety Division regularly moves weapons-grade nuclear materials and nuclear weapons between facilities across the country. Because many tons of weapons-grade nuclear materials are at these facilities, a nuclear detonation at one of them would dwarf the impacts of Chernobyl, potentially kill or injure millions of Americans, and destroy the environment of a significant portion of the United States.

The Project On Government Oversight (POGO) has conducted a series of interviews and consultations with nuclear security and terrorism experts to identify the following major problems with nuclear facility security and their solutions:

PROBLEM: Nuclear Materials Are Spread Across the Country. Weapons-quantity special nuclear materials are stored at 10 fixed sites even though most have virtually no national security mission. DOE cannot currently adequately protect this material, and security at each site unnecessarily increases redundancies and costs. Not only do the unnecessary sites cost the taxpayers billions annually, but they also present a significant health and safety risk to nearby communities.

➤**SOLUTION: Close Unneeded Facilities.** The Base Realignment and Closure Commission should be empowered to recommend closing the unneeded and redundant DOE sites, as well as those sites that have no national defense mission. The Bush Administration is considering this step.

➤**SOLUTION: Consolidate Nuclear Materials.** Two of the most secure facilities in the world would provide enough storage for the entire DOE weapons complex – a secure underground weapons storage facility at Kirtland Air Force Base in New Mexico and the Device Assembly Facility at the Nevada Test Site.

➤**SOLUTION: Immobilize Excess Nuclear Materials.** There is a facility at Savannah River which could be used to meld excess nuclear materials with a radioactive barrier in glass. Once the materials have been immobilized or "vitrified", they would no longer be useful to terrorists.

PROBLEM: Bureaucracy Makes Security Tests Easier Rather than Fixing Problems. The DOE bureaucracy portrays facilities as being secure and impervious to terrorists and spies when, in fact, they are not.

➤**SOLUTION: Improve Effectiveness of Protective Forces.** Until disparate sites are consolidated, DOE should increase the size of its protective force and improve weaponry, tactics, and command, control, and communication to defend against both theft and radiological sabotage. Federalizing protective forces or exploring use of the military are two options.

PROBLEM: Independence in Nuclear Security is Lacking. The recently Congressionally-created National Nuclear Security Administration (NNSA) exacerbates the problem by elevating the same people who have managed this debacle over the last three decades.

➤**SOLUTION: Take Security Management Out of DOE.** POGO suggests exploring the option of setting up an independent agency to provide security from outside DOE entirely, and leave the many other duties of managing the nuclear weapons complex to the NNSA.

➤**SOLUTION: Move the Independent Oversight Office Out of DOE.** Make oversight of nuclear security independent from those charged with implementing security by making the DOE Office of Independent Oversight an Independent Nuclear Facilities Security Board that is independent of DOE. A model would be the Defense Nuclear Facilities Safety Board. This board would report directly to the Congress and be empowered to assess security in the nuclear complex.

PROBLEM: Computers Containing Nuclear Secrets Remain Vulnerable. It is virtually as easy today for a trusted "insider" to put weapons design information on a tape or disk and walk out the door as it was during the controversy at Los Alamos. All of our known spies have been insiders with the highest security clearances.

➤**SOLUTION: Convert to Media-less Computing.** The only way to stop an "insider" is to stop any media (disks, tapes, laptops, etc.) from coming in or out of priority classified areas. Computers would be locked in vaults and access to any media would require a "two-man rule" where two people would have to sign-off on any copies.

PROBLEM: DOE Security Forces Cut by 40%. According to a high-level DOE official, "Since 1992, the number of Protective Forces at DOE sites nationwide has decreased by almost 40% (from 5,640 to the current number of approximately 3,500) while the inventory of nuclear material has increased by 30%." The increase has resulted from the dismantling of nuclear weapons and the receipt of nuclear materials from the Former Soviet Union. During the same period the threat of terrorism has increased.

➤**SOLUTION: Consider Security Budgetary Needs Independently.** Decouple nuclear security funding from scientific research and the nuclear weapons program. Security funding currently competes with scientific research funding from within the National Nuclear Security Administration nuclear weapons budget. Security is always fighting for the scraps after the more politically appealing and bureaucratically popular scientific research and weapons projects are funded.

Introduction

The chances that chemical, biological or nuclear terrorism will occur on U.S. soil over the next ten years "is 100%," according to Richard Clark, U.S. National Security Council National Coordinator for Infrastructure Protection and Counterterrorism for the Clinton and Bush White Houses.

Over a dozen whistleblowers have contacted the Project On Government Oversight (POGO) with unclassified evidence that the U.S. nuclear bomb complex, containing tons of weapons-grade uranium and plutonium, is vulnerable to a terrorist attack. The particular vulnerabilities discussed in this report have been addressed by the Department of Energy (DOE), thereby making them no longer classified. However, new as well as recurring vulnerabilities continue to plague DOE's nuclear security program. This evidence confirms the findings of multiple Presidential and DOE Commissions. Such an attack would endanger the health and safety of the communities near each site to levels in excess of the accidental release at Chernobyl.

The DOE tests the security of these sites by conducting simulated and mock force-on-force exercises often using military forces as the adversary. The government requires that these sites be able to defend against theft of nuclear materials or radiological sabotage by a few terrorists using surprise and readily available weapons and explosives, as well as against the theft of nuclear secrets. According to experts who have conducted these tests in the past, the government fails to protect against these attacks more than 50% of the time – although the exact figure is classified. In addition, the theft of nuclear secrets remains as possible today as it was two years ago when controversy surrounded Los Alamos National Laboratory over the possible leaking of classified information.

As a result of that controversy, in June of 1999, the Chair of the President's Foreign Intelligence Advisory Board, former Senator Warren Rudman (R-NH) was asked to review security at the DOE nuclear weapons laboratories. Their report, "Science at its Best, Security at its Worst" was startlingly blunt in their criticism: ". . . the brilliant scientific breakthroughs at the nuclear weapons laboratories came with a very troubling record of security administration. . . . This report finds that DOE's performance, ***throughout its history***, should have been regarded as intolerable."[1] (Emphasis added)

More importantly, the Rudman report points out the longevity of these problems and the institutional hubris that continues to perpetuate them: "Second only to [DOE's] world-class intellectual feats has been its ability to fend off systemic change." Former Energy Secretary Richardson did much to promote institutional reform in the area of nuclear security, including bringing people in from outside the DOE bureaucracy to oversee nuclear security – specifically General Eugene Habiger and General John Gordon. However, Rudman points out that "the

---

[1] http://fas.org/sgp/library/pfiab/ – Downloaded September 13, 2001.

Department's bureaucracy is quite capable of undoing Secretary Richardson's reforms, and may well be inclined to do so."

DOE's disregard for proven threats to nuclear security and its institutional bull-headedness has thwarted the efforts of reformers, time and time again. Regardless of "scores of critical reports from the General Accounting Office (GAO), the intelligence community, independent commissions, private management consultants, its Inspector General, and its own security experts . . .the Department's ingrained behavior and values have caused it to continue to falter and fail." The report goes on to emphasize this point:

> "***More than 25 years worth of reports***, studies and formal inquiries – by executive branch agencies, Congress, independent panels, and even DOE itself – have identified a multitude of chronic security and counterintelligence problems at all of the weapons labs. These reviews produced ***scores of stern, almost pleading, entreaties for change***. Critical security flaws – in management and planning, personnel assurance, some physical security areas, control of nuclear materials, protection of documents and computerized information, and counterintelligence – have been ***cited for immediate attention and resolution . . . over and over and over . . . ad nauseam***." (Emphasis added)

Finally, the Rudman report states, "The panel has found that DOE and the weapons laboratories have a deeply rooted culture of low regard for and at times, hostility to security issues . . . The Department of Energy is a dysfunctional bureaucracy that has proven it is incapable of reforming itself. . ."[2]

More recently, in June of 2001, then-Chair Fred Thompson (R-TN) of the Senate Governmental Affairs Committee, highlighted the Department of Energy – and particularly their poor handling of security – in its report "Government at the Brink: An Agency by Agency Examination of Federal Government Management Problems Facing the Bush Administration."[3]

Examples of Recent Vulnerabilities

In October 2000, during a force-on-force drill at Los Alamos, New Mexico, the mock terrorists gained control of sensitive nuclear materials which, if detonated, would have endangered significant parts of New Mexico, Colorado and downwind areas. (Appendix A[4])

---

[2] Ibid.

[3] http://www.senate.gov/~gov_affairs/vol2.pdf – Downloaded on September 17, 2001.

[4] At the time this memo was written, this particular vulnerability had not yet been resolved, thus the identity of the facility was classified. Since that time, this particular vulnerability has been addressed to the satisfaction of General Gordon and the Office of Independent Oversight, making this information no longer classified. Details described in the memo, such as the "garden cart incident" and the plans for relocation, have since been attributed to TA-18 at Los Alamos National Lab, by Appendices T, V, & BB.

In an earlier test at the same location, a U.S. Army Special Forces team was able to "steal" enough weapons-grade uranium for numerous nuclear weapons and was able to carry the extremely heavy material with the use of a Home Depot garden cart – throwing the protective forces into disarray. The DOE argued that this test attack was unfair. (Appendix A)

In another exercise, Navy SEALs were able to make a hole in a chainlink fence surrounding Rocky Flats near Denver, Colorado, undetected and easily "stole" enough plutonium for several nuclear bombs. They were only discovered as they were successfully leaving the facility.

The Department of Energy Transportation Security Division moves nuclear weapons, as well as weapons-grade uranium and plutonium, from site to site across the nation on public highways. Over the last several years, there have been exercises testing the security of this Division where the DOE security force failed to protect nuclear cargo because they had inadequate weapons and insufficient numbers, as well as poorly conceived tactics. Due to these insufficiencies, the protective forces were defeated in six out of seven exercises in December 1998. (Appendix B)

In 1998, the Fall of 1999, and again in the Spring of 2000, two force-on-force exercises were run to test the Rocky Flats protective force. A "criticality alarm" – warning that a nuclear chain reaction is potentially imminent – was set off creating confusion, allowing the "terrorist" access to special nuclear materials. Such an alarm requires everyone to immediately leave the building. Hoping to "kill" the "adversaries" the protective force "indiscriminately shot" employees, controllers and each other as they were exiting the building in response to the alarm.[5] The protective force count these tests as successes because they kill all the adversaries – although they also killed all the employees and several of the protective forces as well. (Appendix C)

In addition to physical security, there also remain cyber security weaknesses. The major threat to the compromise of critical nuclear weapons information is the "trusted insider" – personnel with the highest security clearances. Voluminous amounts of information can be accessed quickly and easily. For example, a device the size of a Gameboy can download the equivalent of 1100 floppy discs off a computer in 3 minutes and 14 seconds. Another device called a memory stick, smaller than a stick of gum, can download the equivalent of 44 floppy disks in a couple of minutes. Incredibly, DOE has done virtually nothing effective to protect against the "insider" working on classified computers despite the many Congressional hearings and increased media scrutiny generated by the Los Alamos controversy.[6] (Appendix D)

---

[5] The protective force and mock terrorists are outfitted with Multiple Integrated Laser Engagement System (MILES) weapons laser-simulation equipment.

[6] http://fas.org/sgp/library/pfiab/ – Downloaded September 13, 2001.

Background on DOE Nuclear Weapons Complex

The U.S. nuclear weapons complex managed by DOE is spread across the country. Ten major sites have weapons-grade plutonium (PU) and highly-enriched uranium (HEU) in sufficient quantities for a nuclear device. Several of these sites are located near major metropolitan areas with large populations. (See chart below.) In addition, the DOE's Transportation Safety Division (TSD) moves weapons-grade Special Nuclear Materials (SNM) across the country on interstate highways. Although the total inventory of PU and HEU is classified, according to "DOE Facts" sheets, there are 994 metric tons of HEU[7] and 33.5 metric tons of PU (Appendix F), excluding the PU inventories at Pantex which remain classified. According to the Nuclear Control Institute, it takes less than 50 pounds of HEU or PU to craft a crude nuclear device.[8] In addition, there are significant quantities of completed nuclear weapons, and huge quantities of weapons in various stages of assembly and dismantlement – including those that have been stored for decades as a "war reserve" – that would be attractive to terrorists. The following DOE map shows the location of weapons-grade plutonium inventories. The eight sites identified with plutonium on the map, as well as the Oak Ridge National Laboratory in Tennessee and Sandia National Laboratory in New Mexico, also hold highly enriched uranium inventories.

Metropolitan Areas Within 100 miles of Nuclear Weapons Facilities[9]

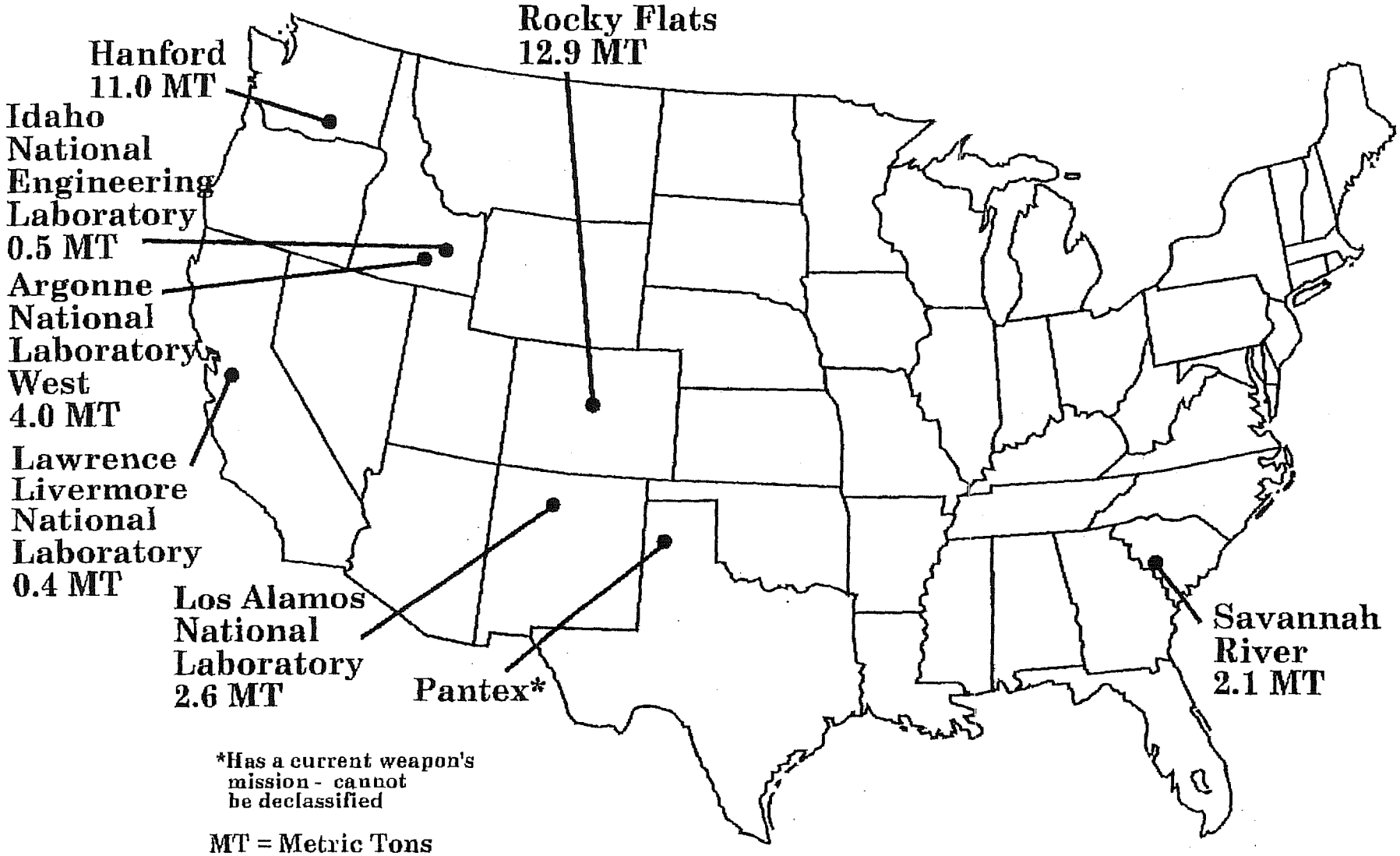
Site Name	Metropolitan Area	Population
Lawrence Livermore	San Francisco-Oakland-San Jose, CA	7,039,362
Rocky Flats	Denver, CO	2,581,506
Sandia	Albuquerque, NM	712,738
Oak Ridge	Knoxville, TN	687,249
Savannah River	Augusta-Aiken, GA-SC	477,441
Pantex	Amarillo, TX	217,858
Hanford	Richland–Kennewick-Pasco, WA	191,822
Los Alamos	Santa Fe, NM	147,635
Argonne & Idaho National	Pocatello, ID	75,565

[7] http://www.osti.gov/html/osti/opennet/document/press/pc13.html - Downloaded September 25, 2001.

[8] http://www.nci.org/new/nci-pro.htm - Download September 26, 2001.

[9] Figures compiled from U.S. Census, Metropolitan Areas Ranked by Population 2000. http://www.census.gov/population/cen2000/phc-+3/tabo3.pdf – Downloaded as of September 17, 2001

December 7, 1993 Announcements
Plutonium Inventories



*Has a current weapon's mission - cannot be declassified

MT = Metric Tons

Total = 33.5 MT

DOE Facts, Appendix F

An issue that exacerbates security problems is the age of these sites and the decay of the infrastructure. Oak Ridge, Savannah River, Hanford and Los Alamos, for example, were all built for the Manhattan Project in the 1940's. The isolated location of these sites made sense at the time for safety and security reasons. Now, population growth and more mobility have made a number of the sites extremely difficult to protect. For example, Technical Area-18 (TA-18) at Los Alamos, New Mexico, with tons of PU and HEU was built in a canyon to absorb the radiation from the reactors. TA-18 also houses several moveable burst nuclear reactors, which are small machines, from the size of a bowling ball to as large as 4 feet by 4 feet by 5 feet tall, containing PU and HEU fuel. The site is extremely vulnerable because terrorists could easily occupy the unprotected high ground around the canyon. A public highway passes within a few feet of the fence line and the facilities that house the PU and HEU. The infrastructure around many of these sites is in decay including storage facilities, fences, and alarm systems.

The Design Basis Threat

There is a classified "Design Basis Threat" (DBT) that describes the level of threat the contractor is required to defend against – the number of outside attackers and inside conspirators, and the kinds of weapons and explosives that would be available to terrorists. (Appendix G) The process that determines this threat was described by Edward McCallum, the former Director of the Office of Safeguards and Security in a letter to the Director of the Office of Security Affairs: "The FBI, CIA, DOE, and the military services as well as the Nuclear Command and Control Staff have developed the existing Design Basis Threat over a number of years. It has been extensively reviewed and supported by studies issued by the DIA [Defense Intelligence Agency]. Sandia, as well as the other labs, have been asked to comment and participate in the development process." (Appendix H)

Each site is then required to develop a Site Safeguards and Security Plan (SSSP) annually, which describes in detail how they would counter the most likely and most disastrous attack scenarios based on the DBT. The plan is developed by the contractors, and then analyzed and approved by the DOE field office and various Headquarter's program offices to confirm that the site is at low risk.

Despite the fact that the DBT goes through this studied, interagency process, the bureaucracy often complains that it is too high a standard to meet – "defending against that terrorist that is about thirteen feet in height" (Appendix E) or super-terrorists. But in fact, the DBT does not require DOE to defend against exotic weapons, but weapons that are readily available on the open market from private arms dealers. According to DOE's Independent Oversight Office, the opposite is true and in fact the capabilities of terrorists are underestimated in the planned scenarios:

"**Capabilities of Available Adversary Weapons Are Not Being Accurately Represented.** In the last year this office has catalogued a long list of readily available adversary weapons and tools that are not being used appropriately by the adversaries depicted in current SSSP/VAs. Among these are tactical smoke, irritant gases, anti-personnel and anti-vehicle explosive devices ("stay-behinds"), grenades, armor-piercing small arms ammunition, and communications disruption devices, to name but the most obvious. It has become "customary" in DOE to limit the use of such weapons and tools, creating the potential for artificially high calculations of protective force effectiveness." [This is inconsistent with tactics currently being taught in the Afghanistan training camps and used by terrorist groups in Columbia, the Philippines, Sri Lanka, Chechnya, the Balkans, and the Middle East.] (Appendix I)

The Design Basis Threat specifies that sites are only expected to protect against:

"A small group (including an insider)" [the actual number is classified]

"Characteristics:

- Capable of lethal and violent action; willing to kill and be killed.
- Capable of conducting coordinated paramilitary operations.
- Possess a wide range of military equipment, weapons and ordnance.
- Access to funds, communications, transportation and safehouses." (Appendix G)

This Design Basis Threat intends to protect nuclear weapons facilities from:

➢ Theft of nuclear material;

➢ Radiation sabotage – blowing up nuclear material and dispersing radiation into the surrounding areas (this could be achieved by an insider, an outside terrorist getting inside or more likely, with a truck bomb); and

➢ Exploding PU or HEU in such a way that it causes a nuclear chain reaction, through the creation of an Improvised Nuclear Device that could result in Hiroshima-like devastation. How such a crude weapon could be created is highly classified, however, experts point out that any self-respecting college physics student already has that knowledge. Explicit instructions on how to build a nuclear weapon are on the internet.

It is difficult to deal with the failures of DOE security because of the level of classification of information regarding the nuclear weapons complex. Of course, some classification is legitimate, but a good deal of information is classified because it is embarrassing.

Three Case Studies

Three case studies provide an insight into how the system has failed: the plant at Rocky Flats, outside of Denver, Colorado; Technical Area-18 (TA-18) at Los Alamos, New Mexico; and the Transportation Security Division, which travels the United States interstate highways. The repetition of problems in these case studies should make it clear that these problems are systemic, constant and recurring.

Rocky Flats

Rocky Flats, outside Denver, Colorado, was a major weapons production facility during the Cold War where the plutonium parts for nuclear weapons were milled and fabricated. Tens of tons of plutonium as well as uranium are stored at Rocky Flats. DOE is currently in the process of shutting down the plant and de-inventorying – sending the PU to Savannah River and the HEU to Oak Ridge. Currently, there are still large quantities of Special Nuclear Materials (SNM) at Rocky Flats that are attractive to terrorists. Wackenhut Security, a private security firm, supplies the protective force. Kaiser-Hill LLC is the prime contractor managing Rocky Flats.

In 1992, members of the Wackenhut security force were upset because they argued federal oversight was too overzealous. This tension between federal overseers and the contractor is highly unusual in the DOE complex. In a July 16, 1992 letter to Terry Vaeth, DOE Manager at Rocky Flats, Timothy P. Cole, President of Wackenhut Services Incorporated stated, after taking over security at the site in July 1990:

> "During our first few months we were racing to prepare for an upcoming DOE OSE Inspection and Evaluation. Further, the plant mission was undergoing intense scrutiny based on safety and environmental concerns. Those priority issues coupled with fundamental security needs put us in a position of vulnerability from a performance measurement standpoint. There weren't enough hours in the day. The Protective Force supervisory ranks and the number of cleared, trained Security Inspectors were inadequate for accomplishment of the security mission . . .
>
> "The purpose is not to make excuses, explain away, or otherwise disclaim our performance deficiencies. We have privately and publicly accepted responsibility for all of our actions and stepped up to problems and emphasized corrective actions rather than arguing the issues. . . .

> "I must tell you very frankly that we have been exposed to 'management terrorism' and 'organizational sedition' for well over a year. . . .
>
> "The DOE management oversight process at RFO [Rocky Flats Office] is, in my opinion, heavily slanted toward the negative to include specific 'targeting' of people in management as well as individual members of the Protective Force." (Appendix J)

As even Cole acknowledged, Wackenhut was having trouble performing some basic security duties. For example according to sources, in a surprise security test at that time, federal security overseers passed through a secured entrance with a pistol in a coffee can – an obvious breach of security.

Wackenhut President Timothy Cole's letter warned Rocky Flats federal security officials, "The distrust, doubt and fear our Security Inspectors have for certain DOE officials is unhealthy and *may lead to serious consequences*." (Emphasis added) The federal Director of Security was removed, and Wackenhut retained their contract. (Appendix J)

In 1995, two Wackenhut security force whistleblowers, Mark Graf and Jeff Peters, wrote to their Congressman, David Skaggs (D-CO), citing their concerns about the poor security at Rocky Flats being performed by Wackenhut. Their whistleblowing lead to a harrowing sequence of retaliations against both Graf and Peters, including their being sent for psychiatric evaluations. After both were put on administrative leave, Peters resigned. Graf was reinstated after winning his whistleblower retaliation lawsuit.[10]

The federal Office of Personnel Management interviewed Wackenhut Services Inc. (WSI) General Manager William R. Gillison during the Jeff Peters whistleblower case. Gillison acknowledged that he, "reported to WSI Corporate that the SNM was at high risk and it was not WSI's responsibility to assume responsibility for such material." (Appendix K)

In 1996, according to sources, DOE Headquarters rejected the Site Safeguards and Security Plan (SSSP) citing serious deficiencies.

In January 1997, the DOE "Report to the President on the Status of Safeguards and Security for 1996" gave Rocky Flats a marginal rating – meaning that nuclear material was not being protected adequately. (Appendix L)

---

[10] http://www.whistleblower.org/www/grafexcerpt.htm – Downloaded on September 17, 2001.

In March 1997, DOE determined that Rocky Flats was in fact not marginal, but "that there were vulnerabilities at the site that were not identified or addressed in the 1997 SSSP and that SNM was at risk under the then existing conditions." (Appendix M)

In April 1997, a subsequent Director of Security for DOE at the Rocky Flats site, Col. David Ridenour, resigned because he believed the health and welfare of the public was not being protected, and that top management would not allow him to perform his duties. He wrote in a letter to the Head of the Operations Office, "In my professional life as a military officer, as a Registered Professional Engineer. . . I never before experienced a major conflict between loyalty to my supervision and duty to my country and to the public. I feel that conflict today." (Appendix N)

The next week in April 1997, Col. Ridenour wrote in a letter to then-Secretary of Energy Federico Pena ". . . I was instructed by my direct supervisor . . . that my mission was to 'not negatively impact the contractor' and that I was to 'facilitate the contractor (a joint venture between Kaiser and CH2M Hill) winning the award fee'." (Appendix N)

In September 1997, again the SSSP was rejected. DOE Headquarters gave Rocky Flats 120 days to implement corrective actions. After 120 days, no action had been taken, and no one was held accountable – neither government employees nor contractors (Appendix M)

In 1997, unauthorized taped phone calls with DOE Headquarters Director of Security Col. Edward McCallum by Wackenhut whistleblower Jeff Peters revealed McCallum's concern that terrorists could gain access to large quantities of plutonium and cause a sizable nuclear detonation. McCallum stated, "I've said in front of the Deputy Secretary and people at that level, I think the citizens, the employees at the plant, and the citizens of Colorado are at extremely high risk for no reason." These concerns were first raised in 1995 – two years earlier – yet they had remained unresolved. (Appendix O)

In January 1998, the Independent Oversight team from DOE Headquarters conducted a force-on-force at Rocky Flats, concluding that security was "adequate by a narrow margin." For the third time, another SSSP was submitted and rejected by Headquarters – the site was not at low risk. (Appendix Q)

In May 1998, Deputy Assistant Secretary Glenn S. Podonsky of the Office of Independent Oversight and Performance Assurance (heretofore the Office of Independent Oversight) wrote that after a comprehensive inspection, ". . . the protection program elements measured during this inspection do not indicate that a fully effective program is yet in place. As evidenced by deficiencies identified in some areas of physical security systems, material control and accountability, computer security, and classified matter protection and control, there remain a number of legacy safeguards and security issues to be resolved." (Appendix P)

Several whistleblowers attended a summer 1998 briefing of all DOE Security Directors at Savannah River Site near Aiken, SC, by a Navy Captain regarding force-on-force drills conducted by the Navy SEALs at Rocky Flats. During the tests, the SEALs successfully entered the site through the perimeter fence, getting into a nearby building, and "stealing" a significant quantity of plutonium, exiting the building, getting out through the fence and escaping without being caught. After this embarrassment, for the next two force-on-force tests, Rocky Flats management "over controlled" and demanded that the SEALs could not go through the same hole from which they came in – they had to take the plutonium and climb a guard tower and rope it over the fence. (Of course, real terrorists could have just thrown it over the fence.) In these two contrived tests, the protective force successfully defended the facility. According to the whistleblowers, the SEAL Captain announced he would never waste the time of the SEALs coming back to a DOE site, because the tests were unrealistic.

In July 1999, then-Energy Secretary Bill Richardson sent a security team to Rocky Flats. Two glaring vulnerabilities were found, strikingly similar to those found in 1995 and again in 1997. Rocky Flats management vehemently denied the team's accusation that plutonium was kept out of the vault without additional protective forces in place, as is required. Several hours later in the meeting, they finally admitted they had plutonium out of the vault in a high-risk situation eight hours a day, five days a week. (Appendix R) The significance of this dangerous practice was highlighted when, according to security team members, only a few weeks earlier an employee had walked out of a key security door setting off the alarm – yet the protective force could never find the employee. Because the PU was inadequately protected, the employee could have taken some of it, walked out and thrown it over the fence – never to be discovered.

Also according to sources, the security team found the vehicle barrier on the wrong fence. A vehicle barrier is a heavy steel cable – strong enough to stop a speeding truck loaded with thousands of pounds of explosives – that should be attached to the inside fence of a two-fence perimeter. The Rocky Flats cable was on the outside fence, which does not have alarms. Therefore a terrorist could, undetected, cut the cable and drive through the outside fence, easily crash through the inside chain link fence in a truck loaded with explosives, park alongside a nearby vault, and detonate a bomb. This vulnerability had been identified in 1996, and had never been fixed. In late 1999, under pressure from Richardson's team, this problem was addressed within hours at minimal cost by placing large boulders around the fence.

In October 1999, the DOE security czar sent DOE and DOD experts to Rocky Flats to resolve the outstanding problems found by Richardson's team. At first, Rocky Flats DOE management refused to allow the team on the site. Once they were permitted inside, the experts still found the same problems Rocky Flats had agreed to fix two years earlier.

When the experts returned in March 2000 to validate the protective force changes, they found a different but alarming trend. Repeatedly during force-on-force drills, the protective forces were "shooting" everyone in sight – mock terrorists, scientists, "controllers wearing orange safety vests, and each other" – in a simulated test. The rules of deadly force were

completely abandoned to pass the tests and prove "low risk," the same problem noted in 1998 and again in 1999. This pattern is described in more detail on page 25. (Appendix C; Appendix M)

Los Alamos Technical Area-18

Technical Area-18 (TA-18), run by the University of California, is one of a number of technical areas at Los Alamos. It houses several nuclear burst reactors and tons of weapons-grade HEU and PU. The facility was built on the floor of a canyon in the 1940's so that the walls of the canyon would absorb the radiation from the reactors. However, today the lack of control of the high ground around the canyon makes the site extremely difficult to defend.

Special Nuclear Materials (SNM) are stored in vaults at several locations on the site. The security infrastructure has been in a state of disrepair. As recently as a few years ago it was found that someone could get inside the fence without being detected because of the poor quality of the closed-circuit TV cameras. Until recently one of the vaults storing SNM even had a window.

The House Subcommittee on Oversight and Investigations was concerned about the security of this site as early as the early 1980's. According to former Chairman John Dingell, "The Subcommittee's work on this matter began in 1981 in response to efforts to undermine independent review of security threats. . .[T]he safeguards at the most critical facilities — which included Los Alamos – were in shambles while, at the same time, DOE's Office of Safeguards and Security was giving the facilities a clean bill of health." (Appendix S)

In 1997, a special unit of the U.S. Army Special Forces was the adversary during a force-on-force exercise. The normal theft scenario is to "steal" enough SNM for a crude nuclear weapon that would fit in rucksacks. But, according to the *Wall Street Journal*, this exercise required that they "steal" more HEU than a person can carry. Not to be outmaneuvered, the Army Special Forces commandos went to Home Depot and bought a garden cart. They attacked TA-18, loaded the garden cart with nuclear materials, and left the facility. "[T]he invaders reached the simulated objective of the game: enough nuclear material to make an atom bomb." And they did so with relative ease. As the *Wall Street Journal* reported,

> "The Garden Cart attackers. . .used snipers hidden in the hills to "kill" the first guards [protective forces] who arrived. Because they happened to be the commanders of the guard force, the rest of the force was thrown into disarray. Many of them also were "killed" as they arrived in small groups down a narrow road leading to TA-18. '[The Special Forces] took them out piecemeal as they came in,' says one participant in the game, whose account wasn't challenged by DOE or lab officials." (Appendix T)

As the *Wall Street Journal* further noted, "The 1997 mock invasion succeeded despite months of guard [protective forces] training and dozens of computerized battle simulations showing that newly beefed-up defenders of the facility would win." (Appendix T)

In 1998, while completing their required annual survey, the Albuquerque Operations Office found the security at TA-18 and other Los Alamos sites unsatisfactory. By the time the report made its way through top management, the unsatisfactory became satisfactory, with no change in actual security. A force-on-force exercise was performed by the 1998 survey team, but they reported that the Los Alamos protective force had compromised the exercise. The DOE Inspector General found that DOE supervisors in Albuquerque refused to investigate the matter. A more detailed description of these incidents is found on pages 28-29 in the Field Operations Office annual surveys section of this report. (Appendix U)

In the Summer of 1999, Secretary Richardson's security team inspected Los Alamos and recommended that TA-18 be shut down and immediately de-inventoried because it could not be defended. However, DOE management persuaded Secretary Richardson not to shut down the site immediately, but instead to further study the matter. In the Fall of 1999, Secretary Richardson created a relocation team to recommend alternative sites for the TA-18 missions. (Appendix V)

In January 2000, while on a site visit to TA-18, members of the relocation team raised questions about an obvious vulnerability at this site. In a semi-hardened building, one of the burst reactors with large plates of HEU fuel was properly stored in an upgraded vault. Another almost identical reactor was sitting in the middle of an open area. The obvious security issue was to either put the reactor in a vault, or take the fuel out and store it in a vault. Los Alamos management refused to do either. (Appendix A)

In a meeting to determine the relocation team's recommendation to Secretary Richardson, Defense Programs (the predecessor organization to the National Nuclear Security Administration [NNSA]) was the lone voice out of ten DOE offices that resisted relocating the facility. Defense Programs took this position in the very memo where they pointed out it would be less expensive to move TA-18 to a more secure site. (Appendix V)

In April 2000, Secretary Richardson, against strong reactions from DOE Defense Programs, ordered that TA-18 be shut down and the SNM completely removed by 2004. He also ordered that a Memorandum of Decision (MOD) be completed by January 15, 2001, in which he would identify the new location for the TA-18 mission. Defense Programs dragged their feet and had barely started the necessary steps to complete the MOD, including the Environmental Impact Statement (EIS) by the deadline. (Appendix X)

In October 2000, the Headquarters Independent Oversight group ran a force-on-force attack – gaining access to the reactor fuel and potentially causing a sizable nuclear detonation that would have taken out part of New Mexico and caused havoc downwind. (Appendix A)

On November 22, 2000, shortly after a meeting with Secretary Richardson, NNSA Director General John Gordon sent an angry letter to Los Alamos Lab Director Dr. John Browne threatening to shut down TA-18 after the debacle in October. Gordon wrote:

> "The failure of the University of California to submit a suitable corrective action plan and to correct in a timely manner the deficiencies cited in an October 2000 assessment of TA-18 security capabilities is unacceptable. As you know, the assessment identified a number of improvements but also several significant weaknesses – most notably in the security strategy, the level of response training, and in the security forces' understanding of appropriate response procedures. **The problems that were noted can be fixed by changes in strategy without the need for the site to incur significant additional costs** (emphasis added). . .If any of these actions do not occur, all activities at TA-18 will be immediately suspended until the actions have been taken and verified." (Appendix Y)

A DOE Headquarters security team went to Los Alamos in December of 2000 to verify that Los Alamos had made adequate upgrades. While they had made upgrades, the changes had not been performance tested to ascertain their effectiveness. An internal DOE memorandum raised basic questions about the adequacy of the "new and improved" protection of this site. (Appendix A)

Transportation Security Division

The Department of Energy Transportation Security Division (TSD) moves nuclear weapons, as well as weapons-grade uranium and plutonium, from site to site across the nation on public highways. The protective forces in the Transportation Division are civilian federal employees. In late 1998, TSD submitted a Site Safeguards and Security Plan (SSSP) to Headquarters for approval. Preliminary examination of the testing scenarios revealed that the SSSP used simplistic attacks and "dumbed down" use of weapons.

During planning phases the TSD team of specialists and commanders were aghast at the proposed use of sniper rifles with armor-piercing incendiary rounds by the adversaries. The DOE Inspector General determined that DOE management considered the use of a sniper rifle unreasonable and that only "super adversaries" would use them. In fact, these weapons have been available since World War I. The GAO found in an undercover investigation that more than 100,000 rounds of Pentagon-surplus armor-piercing incendiary rounds have been sold on the civilian market. (Appendix Z)

At the DOE Pantex nuclear weapons-assembly facility, security officials believed that armored Humvees were death traps, because of the availability of armor-piercing incendiary rounds. The Pantex Security Director lamented that he would never allow his protective forces to fight from them, and that it would have been just as effective to buy Yugo's. Incredibly, the next day, Secretary Richardson's security team was at Sandia, and found officials in the process of

buying armored Humvees. Using these readily-available armor-piercing incendiary rounds, terrorists could shoot through the armored truck cabs, killing the driver and protective forces, making the transported nuclear materials ready for the taking.

In the simulation phase only four tests were run. According to sources familiar with the test, the TSD protective forces were literally annihilated in tens of seconds after an attack was started. In after-action briefings the convoy commander admitted that they had experienced similar results in force-on-force testing many months earlier. Part of the problem was that the guards' weapons were of inadequate range to reach the adversary.

A December 12, 1998 internal DOE memorandum reported on the computerized Joint Tactical Simulations (JTS) evaluations of the Transportation Division's SSSP conducted at Sandia: "JTS results on the first worst case scenario. . .were 3 losses and no wins. JTS results on the second worst case scenario. . .were 3 losses and 1 win. The high TSD JTS loss rate for the first two worst case scenarios caused TSD to request termination of JTS activity. TSD requested DOE Headquarters' assistance to analyze the poor results and begin to determine possible corrective actions." (Appendix B)

In early 1999, a special force-on-force test was run at Fort Hood for the luminaries from Washington – Deputy Secretary, Undersecretary and top security and program officials, to show that the TSD could handle the threat. The U.S. Army Special Forces provided the adversaries. The protective force won. However, according to a Special Forces representative, he noticed a piece of paper held by a protective force member that he had just "shot" – it was a complete outline of the mock terrorists' attack plan. The protective force was cheating. Secretary Richardson's Special Assistant, Peter Stockton, proved the cheating to the Albuquerque manager and the TSD manager. No action was taken. (Appendix W)

In November 1999, an Army Special Forces representative found that the new sniper rifles used by TSD were target range variety, not for combat in rugged terrain. In fact, the sights on the rifles were very sensitive and would not survive the rigors of combat. More than half of the unclassified recommendations made by the DOE Inspector General regarding the SSSP process were focused on improving the security of the TSD program. (Appendix MM)

Major Threats to the Complex

There are four particularly worrisome threats that cut across the complex: 1. The threat of attack by weapons of mass destruction; 2. The threat of truck bombs; 3. The threat of the creation of an Improvised Nuclear Device from the material at particular DOE sites; and 4.The threat of theft of nuclear secrets.

Weapons of Mass Destruction

In the summer of 1995, then-President Clinton issued Presidential Decision Directive 39 (PDD-39) to address the nation's concern over the use of weapons of mass destruction (WMD) against our citizens.[11] Weapons of mass destruction are biological, chemical, radiological, and nuclear. In May of 1998 he added a supplemental directive PDD-62 reaffirming PDD-39. These two directives "highlight the growing threat of unconventional attacks against the United States," including, "terrorist attacks, use of weapons of mass destruction, assaults on our critical infrastructures and cyber-attacks." [12]

The use of chemical and biological weapons has barely reached the level of consciousness in DOE. Security tests at the facilities do not include weapons of mass destruction in their scenarios. Chemical and biological weapons are not even considered in the Site Safeguards and Security Plans or SSSPs at any of the DOE nuclear sites. Keep in mind the use of chemical or biological weapons against DOE weapons facilities is as a limited engagement device for the terrorist to neutralize the protective forces and gain access to the SNM on site for theft, creation of an Improvised Nuclear Device (IND), or radiological dispersal sabotage. In a recent force-on-force drill at Los Alamos, the adversary force used a simulated irritant gas against the protective force. The protective force was totally unprepared for even the use of the gas mask. (Appendix A)

Five and a half years after PDD-39 was issued by President Clinton, DOE now has a classified study underway on developing strategies against chemical and biological attacks. It is believed that this study will recommend further study.

---

[11] Official policy positions by the President of the United States are issued through the National Security Council in the form of Presidential Decision Directives (PDD).

[12] http://www.info-sec.com/ciao/6263summary.html – Downloaded on September 14, 2001.

Truck Bombs

Since the U.S. Marine barracks in Beirut, Lebanon, were leveled by a truck bomb in 1983, DOE facilities have been required to protect against truck bombs. The U.S. Government has suffered significantly from truck bombs:

- U.S. Embassy in Beirut, Lebanon on April 18, 1983;
- U.S. Marine barracks in Beirut, Lebanon on October 23, 1983;
- U.S. Embassy in Kuwait on December 12, 1983;
- World Trade Center in New York City on February 26, 1993;
- The Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995;
- Khobar Towers in Dhahran, Saudi Arabia on June 25, 1996;
- U.S. Embassies in Nairobi, Kenya and Dar es Salaam, Tanzania on August 7, 1998; and
- USS Cole Naval Destroyer in Yemen (a rubber boat bomb) on October 12, 2000.

A September 2000 CIA Interagency Intelligence Committee on Terrorism report points out, "These massive vehicular bombs have illustrated the need for substantial vehicle access denial systems to afford a buffer area between bomb vehicle and the building or facility requiring protection." (Appendix AA)

A truck bomb at a nuclear weapons plant could be devastating, dispersing tons of PU or HEU over the surrounding communities. As discussed on page 14, Secretary Richardson's security team found that Rocky Flats was vulnerable to such an attack. They had placed the vehicle barrier cable on the outside fence rather than the inside fence. A terrorist could have cut the cable on the outside fence (which does not have alarms), driven a large truck through both fences and up against the wall of a vault containing tons of PU, and detonate a bomb before any credible response could be mounted by the protective force. Putting the cable on the inside fence would slow down an intruder once they have already broken through the outside fence, and set off the sensors between the fences thereby alerting protective forces to their presence. This is 16 years after the bombing of the U.S. Marine barracks in Beirut, 4 years after the Presidential Decision Directive on terrorism, and 2-1/2 years after this was initially discovered and Rocky Flats was ordered to fix it.

At the Pantex Plant during one of the Secretary's Special Assistant's visits in 1999 it was noted that the vehicle barrier on the primary road into the main storage area was installed backwards. Instead of stopping a vehicle the barrier would provide a ramp for the vehicle to drive over. Pantex, is the crown of DOE, and this area was the jewel in that crown. This area had been inspected and examined countless times by the assessment, survey and inspection groups since 1995.

The Creation of an Improvised Nuclear Device

A Improvised Nuclear Device (IND) explosion is qualitatively different from exploding SNMs with a homemade bomb. While exploding PU or HEU with a bomb would cause a major dispersion of highly radioactive materials as occurred at the Chernobyl Reactor in the Ukraine, an IND explosion could cause a chain reaction on par with the devastation of Hiroshima and Nagasaki, Japan. An IND can be created at a number of DOE sites because of the presence of nuclear weapons or special nuclear materials in bomb grade quality and quantity. This can cause nuclear detonations of varying sizes. Little time is required to accomplish this act. In a force-on-force test in October 2000 at TA-18, at Los Alamos, the protective force failed to stop the "terrorists" from gaining access – therefore a sizable nuclear detonation was possible. (Appendix BB)

Frighteningly, a terrorist group would not have to steal nuclear material, create a nuclear device, transport it in a suitcase to the United States, and detonate it in a major city. They could simply gain access to the material at a U.S. nuclear facility, some of which are near large cities where they could accomplish the same outcome. As the former DOE Director of Office of Safeguards and Security simply stated regarding Rocky Flats, ". . .you don't need to take it in the middle of Denver, it's going in the middle of Denver anyway." (Appendix O)

Although discussing the potential for an IND explosion is not classified, discussing the details of how such an explosion could be detonated has been classified by DOE as a Special Access Program (SAP). This vulnerability is widely recognized within the defense community, however DOE takes the stance that analyzing and fixing this vulnerability cannot be discussed by anyone other than those in the small "club" who have clearance for the SAP program. As a result, security experts have been forced to wait for these people to address this problem – and they have been waiting for decades.

Theft of Nuclear Secrets

In early 1999, the Los Alamos cyber security failures surprised DOE. Congress and the press were highly critical of DOE for its inability to protect classified information on their computer systems. The Rudman Panel bemoaned the constant use of ineffective commissions and panels to review ongoing security failures at DOE:

> "Management and security problems have recurred so frequently that they have resulted in nonstop reform initiatives, external reviews, and changes in policy directions. . . . During that time, security and counterintelligence responsibilities have been 'punted' from one office to the next. . . .Particularly egregious have been the failures to enforce cyber-security measures to protect and control important nuclear weapons design information. Never before has the panel found an agency with the bureaucratic insolence to dispute, delay, and resist

implementation of a Presidential directive on security, as DOE's bureaucracy tried to do to the Presidential Decision Directive No. 61 in February 1998."[13]

DOE's answer to this crisis was to initiate yet another multi-million dollar commission to study the matter. In the Fall of 1999, DOE's Defense Programs presented a foot-thick report entitled "Information Security Management" to the Undersecretary with a $1.3 billion price tag to solve the problem. Obviously it was not funded due to budgetary constraints. In the Summer of 2000, an internal review of cyber security of classified information found DOE had done nothing effective to stop a trusted insider from downloading the Mother Lode (bomb design information, etc.) and walking out the door – exactly the concerns raised at Los Alamos eighteen months earlier.[14] (Appendix D)

The major threat to the compromise of critical information at DOE is the "insider" – trusted employees. Virtually all of our known spies have been "insiders" with the highest security clearances. The DOE security team reviewed many of the interagency threat documents – all came to the same conclusion – the "insider" is a priority problem. Despite this, the vast majority of planning and preparations was aimed at protecting sensitive information from "outsiders."[15] (Appendix D)

A number of experts believe that there are ways of protecting priority information to near certainty for very little money – but it just doesn't happen. The Labs simply refuse to prioritize what should be protected because they are more concerned about convenience for the scientists rather than security. The Warren Rudman lead President's Foreign Intelligence Advisory Board (PFIAB) Panel concluded:

> ". . . many officials interviewed by the PFIAB panel cited the scientific culture of the weapons laboratories as a factor that complicates, perhaps even undermines, the ability of the Department to consistently implement its security procedures. . . . The prevailing culture of the weapons labs is widely perceived as contributing to security and counterintelligence problems."[16]

There is a device that looks like a child's Game Boy that can download the equivalent of 1100 floppy disks off a computer in 3 minutes and 14 seconds. There is also a device called a memory stick about the size of a stick of gum that can hold the equivalent of 44 floppy disks. Virtually the only way to stop the abuse of this technology is the use of "media-less" computing. To stop an "insider" you have to stop any media (disks, tapes, laptops, etc.) from coming in or going out of priority classified areas. On August 30-31, 2000, a meeting was held at Lawrence

---

13 http://fas.org/sgp/library/pfiab/ – Downloaded September 13, 2001.

14 Ibid.

15 Ibid.

16 Ibid.

Livermore with the Chief Information Officers of the key facilities and labs and the DOE officials from the Operations Offices. Everyone agreed that DOE had to move ahead quickly on the "insider" problem before the Hill or the press found out that virtually nothing effective had been done to stop a dedicated insider. (Appendix D; Appendix CC)

An implementation strategy was established at the Livermore meeting for near-term enhanced security for classified systems including implementing "media-less" computing systems. (Appendix CC) A schedule was developed during this meeting that would have had this system in place before the end of 2000 at a cost in the neighborhood of $10-15 million. The consensus was that these changes would have taken DOE from a low confidence level that a trusted insider could be stopped, to near certainty.

The effort was rejected by the NNSA representative, John Todd, in deference to the alleged functionality and morale concerns of the lab scientists. In the battle between morale of scientists and security, security always loses. In an October 30, 2000 memo to then-DOE Secretary Richardson, his Special Assistant Peter Stockton wrote,

> " . . .Todd argued that this effort should be delayed because it may have a negative impact on lab morale. Todd's solution was to install lock boxes like those he was implementing at Naval Reactors. He admitted that the lock boxes were not effective against a dedicated insider, and they would not increase security, but they would increase functionality for the scientists – they could leave their computers on when they left their offices. I visited Naval Reactors and met with their security officials to discuss their experience with lock boxes. They admitted that they would not be effective against the dedicated insider, and that they had obvious vulnerabilities. . .This is again based on the wants of the scientists rather than the real security needs of the system." (Appendix D)

Misleading Test Results – And they Still Lose 50% of the Time

Dumbed-down Security Tests

Past results have demonstrated that security forces and DOE field management have learned how to "game-the-game" to the extent that most tests are unrealistic, tactics are "canned" and expected, and the outcome of exercises are pre-ordained. Two techniques are used to performance test the protection system effectiveness – 1) force-on-force tests performed by mock terrorists from the DOE, Army Special Forces and Navy SEALs, and 2) computerized Joint Tactical Simulations (JTS).

A number of groups including the Army Special Forces, Special Operations Unit of the Special Forces, the Navy SEALs and DOE's Office of Independent Oversight have raised serious questions about realism of the force-on-force tests and the JTS computer simulations used to test

the effectiveness of protective force responses. They all argue that exercise artificialities make the protective forces appear far more capable than they actually are – yet even with the scales tipped in their direction, protective forces still lose over 50% of the time. (Appendix DD)

The protective forces are civilian private contractors not under military discipline or the military command structure. A postulated terrorist attack on these facilities would be not only a surprise but also extraordinarily violent, considering the conventional weaponry and explosives available to terrorists today. Some experts question whether the protective forces would have the training or experience or would continue to fight under these circumstances. It is not a question of the personal courage or dedication of the protective force, but the daunting circumstances under which they are placed by the system.

On August 30, 1999, the DOE Office of Independent Oversight sent an unusually candid memorandum marked "For Official Use Only" to the new security czar, describing in detail the weaknesses and artificialities of the security testing process at DOE. According to this office:

> "The. . .more serious concern pertains to the actual content and quality of the VAs [Vulnerability Analyses] that support the current SSSPs. This issue, which calls into question the very foundation of the risk calculations used throughout the Department, has received little attention from safeguards and security managers. It is this concern that forms the subject of this paper. . .
>
> "**There Are Significant Errors in the Database Supporting the JTS Combat Simulation Model.** . . .In addition to the identified errors, a significant number of readily available weapons and munition types are not included in the database. . .
>
> **"Adversary Tactics Are Poorly Thought-Out.** Observed adversary tactics used during JTS simulations and validation and verification force-on-force tests are frequently crude, and often do not rise to the level expected of troops who have completed basic infantry training. . .Personnel assigned to portray adversaries in modeling and performance testing are generally given only a few days to prepare tactical plans. A special problem with JTS simulations is that, generally, one computer operator is assigned to control the entire adversary team, while three (sometimes more) operators are employed to represent the protective force. This leads to situations where one adversary element is well managed in the simulation, while other elements are neglected and relatively ineffective. . .
>
> **"Currently, no one in DOE outside of the Office of Safeguards and Security Evaluations [of the Office of Independent Oversight] appears to have a consistent interest in either cultivating the adversary mind-set or an understanding of adversary capabilities."** [Emphasis added] (Appendix I)

This document clearly articulates the grave concerns of the DOE Independent Oversight Office regarding the inadequacies of the simulation and exercise test system used by DOE, and its inability to accurately predict security capability or status.

There is virtually no surprise in a force-on-force test. Once the protective force is outfitted with the Multiple Integrated Laser Engagement System (MILES) weapons laser-simulation equipment, they know the attack will take place within an hour or two. The specific location of the attack is always tipped off by the controllers and the observers during the "safety walk down." A walk down is performed across the whole area where a battle will be simulated to ensure no obstacles or other land variations would trip or otherwise injure the protective forces during the exercise – obviously not creating a realistic scenario. This is far more than leaning forward in the foxhole.

Another indicator of the artificiality of force-on-forces' are the baffling reactions of the protective forces during the tests. For example, in the force-on-force test at Rocky Flats in 1998, 1999 and again in 2000, the protective force "indiscriminately shot" scientists, controlling referees in orange vests, and each other as they were exiting the building in response to the alarm.

> "Two Multiple Integrated Laser Engagement System (MILES) enhanced exercises were observed where protective force members 'killed' building evacuees, controllers wearing orange safety vests, and each other. During the critique conducted immediately after the exercise, protective force and other site management personnel failed to raise concerns related to the inappropriate use of deadly force. In fact, no critical observations were surfaced by management at the critique. . .In law enforcement training environments, the typical 'penalty' for killing a 'friendly' is failure of the test. At RF [Rocky Flats], there are currently no negative consequences for the inappropriate use of deadly force. In fact, if the adversaries are 'killed' in the process, the result is actually a win from the site's current perspective. This situation is unacceptable and must be addressed immediately." (Appendix C)

This obviously is not a realistic demonstration of how the protective forces would react to a terrorist attack, making the force-on-force test next to useless. DOE Headquarters had already warned Rocky Flats about this inappropriate use of deadly force.

During the March 2000 force-on-force drill, extreme restrictions were placed on the adversaries by Rocky Flats management. The commando adversary team was prohibited from using their own radios and "could not effectively communicate." In addition, the commandoes were not even allowed to drive around a road block "simulated by a PF [protective force] vehicle being parked on the side of the road and a traffic cone placed in the center of the road," which led to the facility. To suggest terrorists would not drive around a car and traffic cone to reach their target stretches reasonable expectations. (Appendix C)

In a force-on-force test at Los Alamos in October 2000, a convoy of protective forces responding to an attack at another site hit a "minefield." Despite the fact that the first vehicle hit a mine and would have been destroyed, the other vehicles continued on through the minefield. Military doctrine and common sense clearly calls for a convoy to stop when hitting a minefield. Los Alamos management's response was that they didn't have time to stop. (Appendix A)

Overstatement of Protective Force Combat Effectiveness

A recent force-on-force test illustrates the problem of combat ineffectiveness. In a memo to then-Energy Secretary Richardson his Special Assistant Peter Stockton wrote, "[D]espite the absolutely critical requirement for "denial" [not allowing an adversary in a building]. . .denial failed." It is clear that if denial were to fail in a real attack, such a facility cannot be recaptured because of the extraordinary percentage of protective forces killed in the initial skirmish. Military doctrine dictates when losses exceed 20%, forces become combat ineffective due to loss of command and communications and basic squad-sized tactics deficiencies. In this force-on-force test, the site lost 50% of their protective force in the initial attack – with eight dead on the doorstep of the facility. At this point, according to combat veterans, there would likely be no further offensive action to recapture the facility by the protective force. In a number of force-on-force scenarios developed by DOE, even when the protective force is successful in repelling an attack, they lose up to 80-95% of the force. This is simply unrealistic. Los Alamos security officials admit this is a problem, but they claim they have unusually brave people. Real bullets may make a difference in their calculation. As an Army Special Forces Commander wrote:

> "As a unit sustains casualties (dead or wounded) elements of the fire and maneuver schemes or 'close quarter battle' drills begin to come apart. . . .[I]f casualties are high (in excess of 10%) qualified replacements become increasingly problematic and command and control begins to be lost. Units are normally considered "combat ineffective" and are rotated off the line when they have sustained 15-20% casualties. At this point maneuver, fire rates, communications and command and control can no longer be relied on to support the mission. Continuation would be expected to result in unnecessary and increasingly high casualties with little expectation of success." (Appendix A)

The clear solution is to shut down sites that can't be protected; if they have a critical mission, move sensitive materials to a site that can be protected.

Simple "access denial systems" are available to the U.S. government which would delay terrorist access to sensitive materials. These systems were developed by DOE and are currently deployed at DOD facilities but not at DOE.

Security analysts claim that Protective Forces are not robust in tactics, weaponry or numbers and result in a low probability of success – all of which results in force-on-force failures in more than 50% of the tests. (Appendix DD) Even with improved tactics and weaponry, the

protective force at the 10 critical fixed DOE sites are still at half the manpower level deployed in 1992.

Naturally, safety is a constant concern for all DOE employees. However, the same safety standards that apply to an office worker also apply to the protective force. Because of this universal application of safety standards the protective forces are encouraged not to, and in many cases prohibited from, engaging in any activity that could possibly result in **any** injury. All this contributes to a protective force unable and unwilling to respond when they are most needed.

Security Oversight – A Weak Record

In Congressional testimony, DOE has led the public to believe that its security at these sites is a well-oiled machine, and there is nothing to worry about. After all, they argue the government has been building bombs at these sites for 60 years, and no one has attacked them yet. Given the recent tragedies in New York and Washington, DC, this argument falls flat. In fact, they are one-eyed toothless watchdogs. Each level of oversight fails for varying reasons: conflict of interest, protection of the contractor, embarrassment, protection of the program, political sensitivities, and bureaucratic survival. The following is an analysis up the chain of command of this "redundant" security oversight apparatus:

Up the Security Chain of Command

➢ *Contractor self-assessments* are a basic conflict of interest. It is not in the interest of the contractor to reveal problems which could lead to further investigation and a cut in their performance bonuses and award fees. The Inspector General (IG or OIG) recently found in interviews that most of the employees performing contractor self-assessments felt they were under pressure from the contractor not to find problems:

> "[T]he OIG found that 8 of the 28 LANL Security Operations Division personnel interviewed (approximately 30 percent) who had conducted self-assessments believed they had been pressured to change or "mitigate" security self-assessments. Several of these individuals said LANL management appeared to be more concerned about making LANL and the Security Operations Division "look good" than reporting the actual security conditions at LANL. The OIG was informed of two instances where LANL management became so upset with issues raised by the initially assigned reviewers, that management reassigned other reviewers who subsequently determined that there were no issues to be raised and that the organizations were satisfactory." (Appendix U)

The IG also found that Los Alamos National Lab (LANL) had been paid by the government for self-assessments that were not done: "In addition to finding that some

self-assessments were not conducted, the OIG also found an instance where a self-assessment report was written without a self-assessment review being conducted." (Appendix U)

➢ *Federal Area Offices* – The DOE Inspector General found the Los Alamos Area Office not technically capable of performing their security oversight function. "Several DOE personnel told us that LAAO [Los Alamos Area Office] security was understaffed and did not have the technical expertise required to conduct all their oversight responsibilities." (Appendix U)

➢ *Field Operations Office annual surveys* – During the 1998 Albuquerque annual survey reviewing security at Los Alamos (LANL), it was determined that security was unsatisfactory or marginal in most categories. By the time the report journeyed through the political review process at the Field Office, the ratings were substantially improved – most to satisfactory. The IG found there was no written justification for the change, and in fact, a number of key documents necessary to justify such changes in ratings had been destroyed:

> "During the 1998 Albuquerque Security Survey at LANL, Albuquerque management upgraded several topic area survey ratings, and most importantly, the overall composite rating. . . During our inspection we noted that the 1997 and some 1998 Albuquerque Security Survey work papers were destroyed . . . As a result, there was no complete record to show how the survey teams developed the ratings." (Appendix U)

In addition, the IG reported that during the same 1998 annual survey, a force-on-force exercise was reported to have been compromised – or rigged. One of the force-on-force mock terrorists reported the compromise, as well as his concerns regarding the Protective Force response, to the Albuquerque Field Office. According to the IG, "Albuquerque [Field Office] management did not fully assess concerns" about the incident, yet that office boldly stated "there was no evidence of 'cheating' and that 'the losers always complain that the winner cheated." The IG reported:

> ". . . [H]ad the compromise of the force-on-force exercise been included in the 1998 Albuquerque Security Survey report, the composite rating would have been 'unsatisfactory'. Instead LANL was given a 'marginal' rating." (Appendix U)

The following Inspector General chart reveals the changes made by the Field Operations Office management from ratings of "unsatisfactory" to ratings of "marginal" or "satisfactory":

Appendix C

1998 Security Survey Rating Changes[11]

Program Topic Areas:	Team Leader	Murder board	Final Report
Program Management			
Program Management and Administration	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Program Planning	Satisfactory	Satisfactory	Satisfactory
Personnel Development and Training	Satisfactory	Satisfactory	Satisfactory
Facility Approval and Registration of Activities	Satisfactory	Satisfactory	Satisfactory
Foreign Ownership, Control, or Influence	Satisfactory	Satisfactory	Satisfactory
Safeguards and Security Plans	Unsatisfactory	Unsatisfactory	Unsatisfactory
Surveys and Self Assessment	Satisfactory	Satisfactory	Satisfactory
Resolution of Findings	**Satisfactory**	**Marginal**	**Satisfactory**
Incident Reporting and Management	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Protection Program Operations			
Physical Security	Marginal	Marginal	Marginal
Security Systems	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Protective Force	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Security Badges, Credentials and Shields	Satisfactory	Satisfactory	Satisfactory
Transportation Security	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Information Security			
Classified Guidance	Satisfactory	Satisfactory	Satisfactory
Classified Matter Protection and Control	**Satisfactory**	**Marginal**	**Marginal**
Special Access Programs and Intelligence Information	Satisfactory	Satisfactory	Satisfactory
Classified Automated Information Systems Security	Satisfactory	Satisfactory	Satisfactory
Technical Surveillance Countermeasures	Satisfactory	Satisfactory	Satisfactory
Operations Security	Satisfactory	Satisfactory	Satisfactory
Unclassified AISS (Optional)	Unsatisfactory	Unsatisfactory	Unsatisfactory
Protected Distribution System (Optional)	Satisfactory	Satisfactory	Satisfactory
Communications Security (COMSEC) (Optional	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	Marginal	Marginal	Marginal
Nuclear Materials Control and Accountability			
Basic Requirements	**Marginal**	**Unsatisfactory**	**Marginal**
Material Accounting	Unsatisfactory	Unsatisfactory	Unsatisfactory
Material Control	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
OVERALL RATING	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Personnel Security			
Access Authorization (Personnel Clearance)	Satisfactory	Satisfactory	Satisfactory
Security Education Briefings and Awareness	Satisfactory	Satisfactory	Satisfactory
Control of Visits	Satisfactory	Satisfactory	Satisfactory
Unclassified visits and Assign by Foreign Nationals	**Satisfactory**	**Marginal**	**Satisfactory**
Personnel Assurance Program	Satisfactory	Satisfactory	Satisfactory
Personnel Security Assurance Program	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory	Satisfactory
1998 Composite Rating	**Unsatisfactory**	**Unsatisfactory**	**Marginal**

Items in **Bold** indicate changes in ratings.

[11] There is no documentation for the 1999 Security Survey that provides a similar Team Leader rating breakdown.

➢ *The Office of Independent Oversight* reports directly to the Secretary of Energy. This office is a qualified and capable group. Their 1999 memo to the security czar, quoted extensively on pages 10 and 24 details their strong analysis and urgent concerns regarding DOE security. However they are in a position not only to take direction from the Secretary but also to play to perceived political sensitivities. It takes a high wire act to survive in this position. Rarely does it serve the political purposes of the Secretary to have documented and potentially embarrassing security problems surfacing that could be discovered by Congress or the press. There are instances where this oversight group has pulled punches or simply not tested certain sites, knowing they would fail at a politically sensitive time. A draft December 1999 GAO report entitled, "Nuclear Security: Improvements Needed in DOE's Safeguards and Security Oversight" revealed that "The director of OSSE [Office of Safeguards and Security Evaluations, DOE Independent Oversight] informed us [the GAO] that inspections were not conducted annually from 1994 through 1998 because Secretarial interest in the safeguards and security area waned and staff allocated for safeguards and security inspections was reduced." (Appendix EE)

The following draft GAO table shows the conflicts between the security ratings given by the Office of Independent Oversight (referred to in chart as OSSE), DOE Field Operations Offices, contractor performance evaluations, and the final reports to the President:

Table 1: Safeguards and Security Ratings for Los Alamos National Laboratory From 1994 through 1999.

Year	OSSE	Operations Office	Contract Performance	Report to the President
1994	No rating given	Marginal	Exceeds expectations	Marginal
1995	Inspection not conducted	Satisfactory	Far exceeds expectations	Satisfactory
1996	Inspection not conducted	Survey not conducted	Far exceeds expectations	Satisfactory
1997	No rating given	Marginal	Meets Expectations	Report not issued
1998	No rating given	Marginal	Excellent	Marginal
1999	Satisfactory	Marginal	To be determined	To be determined

Table 2: Safeguards and Security Ratings for Lawrence Livermore National Laboratory From 1994 through 1999.

Year	OSSE	Operations Office	Contract Performance	Report to the President
1994	Inspection not conducted	Survey not conducted	Excellent	Satisfactory
1995	Inspection not conducted	Satisfactory	Far exceeds expectations	Satisfactory
1996	Inspection not conducted	Satisfactory	Far exceeds expectations	Marginal
1997	No rating given	Satisfactory	Far exceeds Expectations	Report not issued
1998	No rating given	Marginal	Good	Marginal
1999	Marginal	Marginal	To be determined	To be determined

➢ *Reports to the President on the Status of Safeguards and Security at DOE* were produced annually by the Office of Safeguards and Security (OSS). Back in the 1980's Chairman Dingell found DOE misleading the President and the National Security Council about the status of security in these reports. In 1996, a critical report was drafted by the Director of OSS, Edward McCallum, but not released by DOE to the President. Finally, the National Security Council demanded its release. Shortly thereafter, McCallum was then put on administrative leave and investigated. The investigation was later dropped. The next year, no report was issued. (Appendix L; Appendix FF)

National Nuclear Security Administration
Different Name, Same Problem

In the wake of the Los Alamos security breach, the Congress reacted by legislatively mandating the reorganization of the nuclear weapons program in DOE by creating a semi-autonomous agency reporting to the Secretary – National Nuclear Security Administration (NNSA). Even though the Agency was named the National Nuclear **Security** Administration, security is only one of the many duties entrusted to it.

For example, on June 27, 2001, Administrator of the National Nuclear Security Administration General Gordon testified before the House Armed Services Committee on the work and budget needs of the NNSA. Out of 44 single-spaced pages of testimony, General Gordon only devoted 1 ½ pages to physical and cyber security. This testimony demonstrates the extraordinary span of General Gordon's responsibilities: there is no way security (and safety for that matter) can compete with nuclear submarines, non-proliferation deals with Russia, and stockpile surety. This hodgepodge is clearly, as General Gordon says, "fragile" if not worse.[17]

The Los Alamos case was a cyber security problem and an alleged counter intelligence issue. There have been no hearings since the early 1990's addressing the myriad of issues involved in physical security. The reorganization did nothing to address the physical security problems. In fact it exacerbated the problems. It was simply a rearrangement of the deck chairs in a bureaucracy that has failed. In a memo from NNSA's Principle Deputy Administrator, Bob Kuckuck even stated, "This reorganization is predominantly a functional realignment – with many employees continuing to perform their current functions." He went on to say that many employees would even "continue to report to their current supervisor." (Appendix GG) Furthermore, several of the new appointments to top NNSA positions were the very same people who oversaw the agency's predecessor, DOE Defense Programs. At that time, Representative John Dingell (D-MI) warned that this was a mistake:

> "I am gravely concerned about recent proposals to elevate the Department's dysfunctional weapons bureaucracy to the status of an almost completely autonomous agency. . .We are concerned that the same bureaucrats, who have

[17] http://www.nnsa.doe.gov/docs/JAG_HASC_Testimony_6-27.pdf – Downloaded September 13, 2001.

refused to implement President Clinton's recent security order and who resisted reform efforts by both the Bush and Clinton Administrations, would be running this agency, with even greater latitude and far less oversight than is currently in place. **Allowing these proposals to become law would be tantamount to using gasoline to extinguish a fire. . .This would indeed be a remarkable act of political jujitsu where the very institutions responsible for the security problems at DOE would emerge from scandal not merely intact, but even more powerful and autonomous than before.**" (Emphasis added) (Appendix S)

As it has turned out, the Congress has already realized they simply created another unwieldy bureaucracy. In the FY2002 House Appropriations Report, it was observed that, "Congress assumed that creation of the NNSA would lead to efficiencies and streamlined management. However, the result has been an increase in staff at Headquarters and in the field." (Appendix HH)

Lack of Congressional Oversight

In testimony before the House Commerce Committee on April 20, 1999, the GAO stated "we are concerned that, given DOE's past record, it may not be up to the challenge without congressional oversight to hold it accountable for achieving specific goals and objectives for security reform." (Appendix II)

There are two things that move any bureaucracy: one is sustained press attention to a problem and second is congressional oversight. For example, recently there was sustained press attention to the plutonium contamination of workers at a DOE facility at Paducah, Kentucky which finally lead DOE to compensate the injured workers and their families. Over the last 20-30 years, there has never been sustained press attention paid to security debacles at DOE because the Department has been able to hide behind overclassification.

Throughout the 1980's and early 1990's, Chairman John Dingell (D-MI) of the House Energy and Commerce Committee conducted numerous investigations of security lapses. One major problem that Chairman Dingell faced was that he did not have clear jurisdiction over the budget of the nuclear weapons program. He was unable, therefore, to use the most effective threat to the Department – budget cuts.

Despite the efforts of both the GAO and Representative Dingell's Committee, the DOE bureaucracy remained entrenched. According to the President's Foreign Intelligence Advisory Board, "The panel has found that DOE and the weapons laboratories have a deeply rooted culture of low regard for and, at times, hostility to security issues, which has continually frustrated the efforts of its internal and external critics, notably the GAO and House Energy and Commerce Committee."[18]

[18] http://fas.org/sgp/library/pfiab/ – Downloaded September 13, 2001.

The Congressional hearings spurred by the Los Alamos cyber security breaches focused on two specific incidents of security failures, but did not deal with the systemic physical and cyber security problems at the nuclear weapons complex. As this report illustrates, without sustained and intensive scrutiny and oversight, DOE briefings and testimony will not reveal the actual status of security.

Rewards and Punishment Turned On Its Head

Promotions for Security Failures

Whenever a security crisis occurs at DOE, the Secretary usually assures the Congress and the press that the responsible officials will be held accountable. It virtually never happens. As the Rudman report points out, "the lack of accountability . . . has become endemic throughout the entire Department."[19] On the other hand, if someone internally raises an issue about security, they are always retaliated against and find themselves without any further security responsibilities. In other words, the reward and punishment system is turned on its head.

For example, Dr. John Browne, the lab director at Los Alamos, was in charge during the Wen Ho Lee case, the hard drive debacle and the force-on-force in October 2000 that would have led to a nuclear detonation. He is still the lab director. Steve Younger, the head of the X Division at Los Alamos where these debacles took place remained in his job, until appointed by President Bush to become the head of the Pentagon's Defense Threat Reduction Agency. The security director at Los Alamos, Stan Busbaum, is still in his job.

Rocky Flats, which is operated by contractor Kaiser-Hill, had severe security problems in the 1996-98 time frame and again in 1999. In 1997, outgoing Secretary of Energy Hazel O'Leary became a paid Director of Kaiser and outgoing DOE Assistant Secretary for Environmental Management (overseeing Rocky Flats) Tom Grumbly became Senior Vice President for Kaiser. The current DOE Undersecretary Robert Card was President and CEO of the Kaiser-Hill Company. The DOE Manager of the Rocky Flats Field Office from 1996 to 1999, Jessie Roberson, is now the DOE Assistant Secretary for Environmental Management.

The head of the DOE Office of Security Affairs, Joe Mahaley, who was responsible for security at all the sites, and whose office was involved in many of the following retaliations, was promoted to becoming the new security czar.

---

[19] Ibid.

Whistleblowers: Shooting the Messenger

"In every investigation concerning problems at the DOE weapons facilities and laboratories, the individuals responsible for the operation of defense programs consistently and repeatedly denied the problems, punished the whistle blowers, and covered up the problems to their superiors and Congress."

Representative John D. Dingell (D-MI) (Appendix S)

Retaliation at DOE does not necessarily entail attempting to fire federal employees. In the majority of cases in the security area, DOE supervisors attempt to revoke the whistleblower's clearance on trumped-up charges. Then they remove them from any responsibility for oversight of security. On the other hand, contractors often lose their contracts, or their jobs, for blowing the whistle. The frequency of retaliation against nuclear security whistleblowers reached such a crescendo, that in 1999 then-Secretary Richardson sent a memorandum to all DOE and contract employees stating: "Management must also create and foster a work environment that allows free and open expression of security concerns, where workers fear no reprisals or retaliation." (Appendix JJ)

Over the last three years, in the face of Richardson's "zero-tolerance" of retaliation against security whistleblowers, DOE still succeeded in eliminating all of the whistleblowers, or "speed bumps" in the road, as one federal official put it. In fact, months after this "zero-tolerance" policy was in effect, when the DOE Inspector General was investigating security failures at Los Alamos, "a number of individuals requested confidentiality. They indicated they feared retaliation for disclosing information to the Office of Inspector General." (Appendix U) Currently, there are few DOE employees left in the bureaucracy with the knowledge or willingness to risk the damage to their careers to raise concerns about the lack of security. Retaliation against whistleblowers has been a clear object lesson to the rest of the bureaucracy.

Going back to the early 1980's, there has been a pattern of retaliation against federal and contractor employees who raise issues about security problems. For example:

- In 1980, DOE did not like the fact that John Hanatio, a security analyst at DOE Headquarters, was cooperating with the House Subcommittee on Oversight and Investigations. They immediately went after his security clearance and tried to fire him. Under Subcommittee Chairman John Dingell's (D-MI) protection he is still employed by DOE but has never been placed in a position of significant responsibility or dealt with security issues again.

- In 1996, Colonel David Ridenour, a former Strategic Air Command missile officer, became the Director of the Safeguard and Security Division at the Rocky Flats Field Office. Immediately upon taking the position, Ridenour was being harassed for trying to do his job of overseeing the security contractor at Rocky Flats. In a letter to then-Energy Secretary Federico Pena, he said "I was instructed by my direct supervisor. . .that my

mission was to 'not negatively impact the contractor' and that I was to 'facilitate the contractor (Kaiser-Hill) winning the award fee'." He resigned several months later, claiming "In my professional life as a military officer, as a Registered Professional Engineer. . .I never before experienced a major conflict between loyalty to my supervision and duty to my country and to the public." (Appendix N)

➢ Lt. Mark Graf was Alarm Station Supervisor for the Wackenhut protective force at Rocky Flats. Jeff Peters was Director of Protective Force Operations, also at Wackenhut. Both had serious concerns about security at Rocky Flats and wrote to Congressman David Skaggs (D-CO) about these concerns. Peters was placed on administrative leave, his badge and weapon taken from him. He was ordered into counseling. Federal Office of Personnel Management investigators concluded Wackenhut had acted inappropriately and "retaliated" against Peters. In June of 1996, Peters resigned from his position and left Rocky Flats after reaching a settlement agreement with Wackenhut. Lt. Graf's workload was inexplicably raised to 262 hours, from the staff average of 187 hours. After Graf was sent by Wackenhut for psychiatric review, a psychiatrist concluded that Lt. Graf was fit for duty, noting that the reason for Graf's referral was "based on his preoccupation with security safeguards at Rocky Flats and discussion with outside individuals and the media."[20] Lt. Graf was nonetheless fired and finally won a Department of Labor whistleblower case requiring Wackenhut to reinstate him to his original position and pay compensatory damages.

➢ Edward McCallum was a Colonel in the Special Forces with service in Vietnam. He worked in DOE security for twenty years, and authored the 1996 DOE Annual Report to the President on the Status of Safeguards and Security, which was highly critical of security and caused a serious eruption at DOE. He was immediately put on administrative leave and investigated. In early 1999, McCallum's concerns about the lack of security at Rocky Flats were made public. At about the same time, Secretary Richardson issued a zero-tolerance order against whistleblower retaliation – "Management must also create and foster a work environment that allows free and open expression of security concerns, where workers fear no reprisals or retaliation." (Appendix JJ) It didn't work. McCallum was put on administrative leave based on a security violation accusation that was later dropped. Representative Curt Weldon (R-PA) wrote to his colleagues,

> "Throughout the past decade, this former Green Beret officer attempted numerous times to alert the Administration to grievous lapses in security which left our nation's nuclear facilities vulnerable to foreign espionage and terrorist attack. Officials at the highest levels, including three Secretaries of Energy and White House personnel, consistently ignored Lt. Col. McCallum's warnings, placing our national security in jeopardy. . .Lt. Col. McCallum deserves accolades for what he did to protect our

[20] www.whistleblower.org/www/graf.htm – Downloaded September 14, 2001.

national security – not the continued destruction of his reputation and career." (Appendix FF)

McCallum took a job at the Pentagon, and is no longer working on security issues at DOE.

➢ Ron Timm, and his corporation RETA Security, were experienced security analysts under contract to the DOE Headquarters Office of Safeguards and Security. RETA Security was the principal analyst for review of all SSSPs for DOE Headquarters since 1997. He told the IG that he had suffered retaliation for raising concerns about public health and safety. Timm's work assignments analyzing SSSP's for all DOE facilities over the previous five years had plummeted. The IG found no retaliation, as Timm's company was performing other DOE work for Secretary Richardson. As soon as the IG inquiry concluded, Timm's contract was terminated. Timm sent a second letter to the new DOE Secretary, Spencer Abraham, in January 2001 thinking the new administration would look into the ongoing security failures at nuclear facilities. Timm wrote, ". . . time has shown that the existing bureaucracy at DOE have not adequately acted upon the issue of risk to the public other than in ineffective and reactive ways." However, Secretary Abraham delegated the response to the letter to one of the office which Timm accused of covering up security problems, the Office of Independent Oversight. In the six page response Director Glenn Podonsky concluded, "The Department's protection program may not be perfect, we firmly believe it to be effective." Timm is no longer working on Headquarters security issues at DOE and has filed a whistleblower complaint. (Appendix KK; Appendix LL)

➢ According to an IG Report:

> "one support services contractor believed that an OSS [Office of Safeguards and Security] program manager threatened him with a reduction in contract activity for his role in supporting the SSSP QA [quality assurance] process and for assisting the [Secretary Richardson's] special assistant. The contractor said that he did not receive any contract work in the area of field assistance after the alleged threat was made, and that he viewed the elimination of his field assistance activities as retaliation." (Appendix MM)

The IG concluded that because he did not seek to file a formal whistleblower retaliation complaint and that he continued to receive contracts from the DOE security czar, he had not suffered retaliation. As soon as DOE security czar General Habiger left however, he lost all DOE Headquarters contracts. (Appendix MM)

➢ In a desperate attempt to shed light on inadequate physical security at the DOE National Labs, a DOE employee faxed two unclassified IG reports that exposed security failures at

DOE to *USA Today* and the *Washington Post.* (These IG Reports are included at the end of this report as Appendices U and MM) As a result, the employee's security clearance was "suspended due to his admitted release, without prior authorization, of a draft DOE Inspector General report on sensitive DOE security matters. His action was in direct contravention of his signed 'Security Responsibility Statement' promulgated by the DOE Office of Security Affairs specifically to prevent such releases," – an illegal internal DOE gag order prohibiting direct contact with the news media. (Appendix KK) According to the Office of Safeguards and Security Notification Letter, the employee "thought that if [he/she] brought this [security] inadequacy to light, then senior DOE officials might be 'sparked' into improving that program. Accordingly, [he/she] decided to send a copy of the draft OIG report to the news media to 'make things better'." That whistleblower is no longer working on security issues for DOE. (Appendix NN)

As Admiral Rickover once warned, "You can sin against God, and God will forgive you – if you sin against the bureaucracy, they will never forgive you!" This old adage certainly describes the culture at DOE.

Budget

"[T]he annual report I wrote. . . said that we were about $150 million dollars underfunded, we've lost 42% of our protective forces and 50% of our SWAT capability. I said that at a time when we've increased our SNM holdings by 70 metric tons. It doesn't take a brain surgeon to figure this one out."

Edward McCallum, Director of Safeguards and Security, DOE (Appendix O)

The security budget competes with the far more politically popular issues in the weapons programs such as stockpile stewardship and weapons research, that command far more Congressional interest. As a result, security ends up as a poor stepchild. For example, during the battle over relocating TA-18 at Los Alamos, the Acting Deputy Administrator for Defense Programs (the predecessor to NNSA) General Thomas Gioconda stated, "Defense Programs' limited capital funding is already allocated to higher priority Stockpile Stewardship projects." (Appendix V)

The former Director of DOE's Office of Safeguards and Security stated, "since 1992, the number of protective forces at DOE sites nationwide has decreased by almost 40% (from 5,640 to the current number of approximately 3,500), while the inventory of nuclear material has increased by more than 30%." At the same time, the total federal budget devoted to DOE security was cut by one-third. No one argues that the terrorist threat had been reduced, in fact, the intelligence community believes the threat is greater today than during the Cold War. (Appendix OO)

In the mid 1990's the cuts were so deep that several sites including Livermore had to disband their SWAT teams. Livermore then had to depend on the Alameda County Sheriffs Department for a SWAT team. The only problem was it took the Sheriff's SWAT team over an hour to mobilize and deploy a force to Livermore – long after a possible attack had taken place. Livermore found a way to overcome this response time problem. According to whistleblowers, in a 1995 force-on-force, the Army Special Forces adversaries found an Alameda County Sheriff's Department helicopter in the air and their SWAT team near the perimeter fence before the attack had started – was the site cheating? The Sheriff told DOE investigators he had been told by the site that prepositioning his forces was acceptable. He understood the test to be one of capability not of timing. Clearly both are important. In 1998, Livermore decided the situation was untenable, and took an additional two years to reconstitute and train a new SWAT team.

In 1999-2000, Secretary Richardson attempted to split the security budget out of the weapons program budget, putting it under the security czar. This was finally accomplished. However, it only lasted for a matter of months before the Congress put the security budget back under the new semi-autonomous National Nuclear Security Agency.

PROBLEMS/SOLUTIONS

PROBLEM: Nuclear Materials Are Spread Across the Country. Weapons-quantity special nuclear materials are stored at 10 fixed sites. This dispersion is a leftover from the Cold War, when there were many more missions for the various sites. Now, a number of sites have virtually no national security mission, however, they continue to store and try to protect tons of nuclear materials at great cost. DOE can not currently adequately protect this material, and security at each site unnecessarily increases redundancies and costs. However, DOE has resisted consolidation as it would threaten fiefdoms and potentially even lead to the closing down of facilities.

SOLUTION: Close Unneeded Facilities. The Base Realignment and Closure Commission should be empowered to recommend closing the unneeded and redundant DOE sites, as well as those sites that have no national defense mission. Not only do the unnecessary sites cost the taxpayers billions annually, but also present a significant health and safety risk to the nearby communities. There have been a number of studies considering the restructuring of the weapons complex over the past ten years. The Bush Administration is currently considering this path. The following are suggestions for closure and consolidation:

- Shut down Idaho National Engineering Lab and the Argonne National Laboratory – West, as they have little or no national defense mission.

- Shut down Hanford, as it has little or no national defense mission.

- Combine Lawrence Livermore in California and Los Alamos National Labs at Los Alamos, NM – we don't need two redundant bomb design labs. Livermore is now in the middle of a highly populated community, yet large amounts of plutonium are stored there.

- Combine Oak Ridge and Savannah River Facilities as both have significantly reduced missions of producing plutonium and fabricating uranium. Rather than repairing or replacing the decaying infrastructure at both sites, it would be more efficient to combine the two.

SOLUTION: Consolidate Nuclear Materials. Another solution to this problem would be to consolidate nuclear materials to fewer, more easily-protected sites. Not only would this save money, it would reduce the risk to the public. A plan by the DOE to consolidate nuclear materials at two sites that should have been operational by now, has been derailed by the bureaucracy. However, two of the most secure facilities in the world are already available. These two facilities would provide enough storage for the entire DOE weapons complex. One is underground in the middle of Kirtland Air Force Base in New Mexico (Kirtland Underground Munitions Storage Complex), and the other is a brand new (and totally unused) highly secure facility, the Device Assembly Facility, at the Nevada Test Site. For the past decade, DOE has been planning a national storage facility for PU at Savannah River and a storage facility for HEU at Oak Ridge. Both are bogged down in a bureaucratic morass with no end in sight.

SOLUTION: Immobilize Excess Nuclear Materials. There is a facility at Savannah River which could be used to meld excess nuclear materials with a radioactive barrier in glass. Once the materials have been immobilized or "vitrified", they would no longer be attractive to terrorists because it would be virtually impossible to reconstitute the immobilized SNM into weapons grade material.

PROBLEM: Bureaucracy Makes Security Tests Easier Rather than Fixing Problems. Without leadership and accountability, there are few incentives for the DOE bureaucracy to address problems. As a result, DOE portrays facilities as being secure and impervious to terrorists and spies when, in fact, they are not. This is largely achieved by sweeping undesirable messages and test results under the bureaucratic carpet and "dumbing down" the current system to hide embarrassing test failures. Ongoing publicized problems at such sites as Los Alamos and the Transportation Safeguards Division attest to this assertion.

SOLUTION: Improve Effectiveness of Protective Forces. Until disparate sites are consolidated, DOE should increase the size of its protective force and improve weaponry, tactics, and command, control, and communication to defend against both theft and radiological sabotage. One possibility would be to explore the option of moving the responsibility for protection of nuclear weapons quantities of special nuclear material to DOD military personnel. The military personnel should not be used for general site

protection of classified information, personnel, or facilities, but only for the protection of SNM. Another possibility would be to explore whether TSD convoys of special nuclear materials should be supported by military personnel. A 1990 GAO report also suggested exploring the possibility of federalizing the protective forces at the sites similar to the protective force of the Transportation Security Division. In interviews the guards [protective force] themselves told GAO investigators, "a federal force would take security more seriously" and that they would "receive better training." (Appendix PP)

PROBLEM: Independence in Nuclear Security is Lacking. The recently Congressionally-created National Nuclear Security Administration (NNSA) exacerbates the problem by elevating the same people who have managed this debacle over the last three decades. As the Rudman report states, due to the "deeply rooted culture of low regard for and, at times, hostility to security issues. . .a reshuffling of offices and lines of accountability may be a necessary step toward meaningful reform, *but it will almost certainly not be sufficient.*"[21]

SOLUTION: Take Security Management Out of DOE. POGO suggests exploring the option of setting up an independent agency to provide security from outside DOE entirely, and leave the many other duties of managing the nuclear weapons complex to the NNSA.

SOLUTION: Move the Independent Oversight Office Out of DOE. Make oversight of nuclear security independent from those charged with implementing security by making the DOE Office of Independent Oversight an Independent Nuclear Facilities Security Board that is independent of DOE. A model would be the Defense Nuclear Facilities Safety Board. This board would report directly to the Congress and be empowered to assess security in the nuclear complex.

PROBLEM: Computers Containing Nuclear Secrets Remain Vulnerable. It is virtually as easy today for a trusted "insider" to put weapons design information on a tape or disk and walk out the door as it was two years ago. All of our known spies have been insiders with the highest security clearances.

SOLUTION: Convert to Media-less Computing. The only way to stop an "insider" is to stop any media (disks, tapes, laptops, etc.) from coming in or out of priority classified areas. At each workstation, the scientist or engineer would only have a monitor, keyboard, and mouse, while the actual computer is locked in a vault. Access to any media would require a "two-man rule" where two people would have to sign-off on any copies.

PROBLEM: DOE Security Forces Cut by 40%. According to testimony from a high-level DOE official, "Since 1992, the number of Protective Forces at DOE sites nationwide has decreased by almost 40% (from 5,640 to the current number of approximately 3,500) while the inventory of nuclear material has increased by 30%." (Appendix OO) The increase has resulted

[21] http://fas.org/sgp/library/pfiab/ – Downloaded September 13, 2001.

from the dismantling of nuclear weapons and the receipt of nuclear materials from the Former Soviet Union. During the same period the threat of terrorism has increased.

SOLUTION: Consider Security Budgetary Needs Independently. Decouple nuclear security funding from scientific research and the nuclear weapons program. Security funding currently competes with scientific research funding from within the National Nuclear Security Administration nuclear weapons budget. Security is always fighting for the scraps after the more politically appealing and bureaucratically popular scientific research and weapons projects are funded.

APPENDICES

Appendix A: Memo from Peter D. H. Stockton, DOE Special Assistant to: Secretary of Energy Bill Richardson, December 20, 2000.

Appendix B: Memo from Richard J. Levernier, Program Manager Assessment and Integration to: Col. Edward J. McCallum, Director Office of Safeguards and Security, December 12, 1998; and

Memo from Richard J. Levernier, Program Manager Assessment and Integration to: Col. Edward J. McCallum, Director Office of Safeguards and Security, April 19, 1999 – with attachments.

Appendix C: Memo from Richard J. Levernier, Program Manager Assessment and Integration to: James L. Ford, Acting Director Field Operations Division, April 11, 2000 – with attachments.

Appendix D: Memo from Peter D. H. Stockton, DOE Special Assistant to: Secretary of Energy Bill Richardson, October 30, 2000.

Appendix E: Partial transcript of speech by General Eugene Habiger at the 41st Annual Meeting of the Institute of Nuclear Material Management.

Appendix F: "Declassification of United States Total Production of Weapon-Grade Plutonium," DOE Facts, December 7, 1993.

Appendix G: "Design Basis Threat for Department of Energy Programs and Facilities (Unclassified)," U.S. Department of Energy Office of Safeguards and Security, December 1998.

Appendix H: Memo from Joseph S. Mahaley, Director Office of Security Affairs to: Acting Deputy Secretary, February 9, 1999 – with attachments.

Appendix I: Memo from Barbara R. Stone, Director Office of Safeguards and Security Evaluations Office of Independent Oversight and Performance Assurance to: General Eugene E. Habiger, Director Office of Security and Emergency Operations, SO-1, August 30, 1999 – with attachment.

Appendix J: Letter from Timothy P. Cole, President Wackenhut Services Inc. to: Terry Vaeth, Manager U.S. Department of Energy, Rocky Flats, July 16, 1992.

Appendix K: Office of Personnel Management interview with William R. Gillison, General Manager, Wackenhut Services Inc., between March 6, 1996 and April 10, 1996.

Appendix L: Report to the President on the "Status of Safeguards and Security for 1996," Office of Safeguards and Security, Office of Security Affairs, Department of Energy, January 1997.

Appendix M: "Verification Assessment Report of the Rocky Flats Environmental Technology Site Safeguards and Security Plan," Department of Energy Internal Memo July 17, 1998.

Appendix N: Letter from Col. David Ridenour, Director Office of Safeguards and Security to: Ms. Jessie Roberson, Manager, DOE Rocky Flats Office, March 31, 1997; and

Letter from Col. David Ridenour, Director Office of Safeguards and Security to: Secretary of Energy Federico Pena, April 16, 1997.

Appendix O: Excerpts of transcript of telephone conversations between Jeffrey Peters, Operational Security Manager, Wackenhut Services, Inc., and Col. Edward J. McCallum, Director Office of Safeguards and Security, May 7 & 8, 1997 .

Appendix P: Letter from Glenn S. Podonsky, Office of Independent Oversight to: J. Owendoff, Acting Assistant Secretary for Environmental Management, EM-1 & Jessie Roberson, Manager Rocky Flats Field Office, May 14, 1998.

Appendix Q: "Comprehensive Inspection of Rocky Flats Filed [sic] Office and the Rocky Flats Environmental Technology Site (U)," Department of Energy Internal Memo, May 1998.

Appendix R: Testimony of Peter D. H. Stockton, former-DOE Special Assistant, U.S. District Court, Colorado, Civil Action No. 97-WM-2191, U.S., ex rel., Col. David Ridenour et al. v. Kaiser-Hill Company, July 2001. This testimony was witnessed and cleared by a Department of Energy classifier to ensure that no classified information was revealed.

Appendix S: Letter from Representative John D. Dingell, Ranking Member, House Commerce Committee to: former Senator Warren Rudman, President's Foreign Intelligence Advisory Board, March 24, 1999; and

Statement of Representative John D. Dingell at the Joint Hearing of the Commerce Committee Energy and Power Subcommittee & the Science Committee Energy and Environment Subcommittee on Restructuring the Department of Energy, July 13, 1999.

Appendix T: "Debate Widens Over Most Effective Way to Secure Energy Department's Los Alamos Nuclear Site," John J. Fialka, *Wall Street Journal*, March 15, 2000.

Appendix U: "Summary Report on Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self-Assessments at Los Alamos National Laboratory," U.S. Department of Energy Office of Inspector General, May 2000.

Appendix V: Memo from General Thomas F. Gioconda, Acting Deputy Administrator for Defense Programs to: the Secretary of Energy Bill Richardson, March 2000.

Appendix W: Letter from Ronald E. Timm President, RETA Security to: General Eugene Habiger Director, Office of Security & Emergency operations, SO-1, January 5, 2000.

Appendix X: Letter from Maureen McCarthy and Ellen Livingston to: Secretary of Energy Bill Richardson, November 21, 2000.

Appendix Y: Letter from General John A. Gordon, Administrator National Nuclear Security Administration to: Dr. John Browne, Director Los Alamos National Lab November 22, 2000.

Appendix Z: "Weaponry: Availability of Military .50 Caliber Ammunition," General Accounting Office Report # OSI-99-14R, June 30, 1999.

Appendix AA: "Improvised Explosive Devices (IEDs) and Other Criminal and Terrorist Devices: A Basic Reference Manual," Director of Central Intelligence, Interagency Intelligence Committee on Terrorism, September 2000.

Appendix BB: "DOE Probes New Security Lapse And Accident at Los Alamos Lab," John J. Fialka, *Wall Street Journal*, December 11, 2000.

Appendix CC: Overheads from Integrated Cyber Security Initiative, August 29 & 30, 2000.

Appendix DD: Letter from Peter D. H. Stockton, former DOE Special Assistant to: Senator Richard Shelby, September 13, 2001.

Appendix EE: "Draft Statement of Facts, Nuclear Security: Improvements Needed in DOE's Safeguards and Security Oversight," General Accounting Office Draft Report, December 14, 1999.

Appendix FF: Dear Colleague letter from Representative Curt Weldon, June 22, 1999.

Appendix GG: "Memorandum for the Headquarters NNSA Team," Bob Kuckuck, Principle Deputy Administrator, National Nuclear Security Administration, August 20, 2001.

Appendix HH: Energy Appropriations FY2002 House of Representatives Report.

Appendix II: "Department of Energy: Key Factors Underlying Security Problems at DOE Facilities," General Accounting Office Testimony #T-RCED-99-159, April 20, 1999.

Appendix JJ: "Memorandum for All Department and Contract Employees," Secretary of Energy Bill Richardson, June 17, 1999.

Appendix KK: Letter from Glenn S. Podonsky, Director of Office of Independent Oversight to: Ronald E. Timm, President RETA Security, March 5, 2001.

Appendix LL: Letter from Ronald E. Timm, President RETA Security to: Secretary of Energy Spencer Abraham, February 9, 2001.

Appendix MM: "Summary Report on Allegations Concerning the Department of Energy Site Safeguards and Security Planning Process," Department of Energy Office of Inspector General, September 2000.

Appendix NN: DOE Notification Letter from Owen Johnson, Director Office of Safeguard and Security, October 26, 2000.

Appendix OO: Statement of Col. Edward J. McCallum, Director Office of Safeguards and Security, June 8, 1999.

Appendix PP: "Nuclear Safety: Potential Security Weaknesses at Los Alamos and Other DOE Facilities," General Accounting Office Report #RCED-91-12, October 1990.

Acronym Glossary

DIA - Defense Intelligence Agency

DBT - Design Basis Threat

EIS - Environmental Impact Statement

GAO - General Accounting Office

HEU - Highly Enriched Uranium

IND - Improvised Nuclear Device

IG - Inspector General

JTS - Joint Tactical Simulations

LANL - Los Alamos National Lab

MILES - Multiple Integrated Laser Engagement System

M&O - Management and Operations

NNSA - National Nuclear Security Administration

OIG - Office of Inspector General

OSS - Office of Safeguards and Security

OSSE - Office of Safeguards and Security Evaluations of the Office of Independent Oversight and Performance Assurance

PDD - Presidential Decision Directive

PF - Protective Force

PU - Plutonium

QA - Quality Assurance

SAP - Special Access Program

SNM - Special Nuclear Materials

SSSP - Site Safeguards and Security Plan

TA - Technical Area

TSD - Transportation Security Division

VA - Vulnerability Analysis

WMD - Weapons of Mass Destruction

Appendix A:

Memo from Peter D. H. Stockton DOE Special Assistant to: Secretary of Energy Bill Richardson
to Secretary of Energy Bill Richardson

December 20, 2000

Peter D.H. Stockton
40332 Mt. Gilead Rd.
Leesburg, VA 20175
(703) 589-1718

December 20, 2000

To: Secretary Richardson
From : Peter D.H. Stockton
Re: The Continuing Western Saga

The Latest Upgrades

In early December, "the site" made another in a long series of "reactive" upgrades at "the security area" as a result of a recent security debacle in October. The changes were made only after pointed direction from Washington. This upgrade has not been performance tested, ergo it is not clear that it is effective. It is interesting to note that it was recommended by OA that "the reactor" be dismantled in the early '90s. In January 2000, our "secure area" alternative siting team raised questions as to why "the reactor" was sitting in the open, and why it wasn't dismantled. It was only after the event in October and direction from Washington, that "the site" spent four hours taking the fuel out of "the reactor" and storing it in a more secure manner. Again, the upgrades are specific to the latest OA target – not an evaluation of the effectiveness of the entire security at the site. I could almost guarantee you that if the Grizzly Hitch ran a full-up force on force with the full DBT, the site could not be protected.

The Phoney SSSP

The Dingell Subcommittee held hearings on "secure area" in the '80s which led to significant upgrades. However, attention and spending tailed off in the '90s. The infamous "garden cart" incident occured in 1997 that lead to more reactive upgrades, which only lead to further problems in 1998 and 1999.

In January 2000, the "the site's" SSSP was approved in the face of analytical evidence that "the site" was at high risk. In October 2000, less than nine months later, Podonsky's group again found that critical assets could not be protected. Even the one-eyed toothless IG found it curious that the SSSP could be approved under these circumstances. However, no one in DOE has questioned how this happened – there is just full blind support for DP (NNSA) and "the site."

Was This an Unfair Attack?

Hardly. Officials at "the site" claimed it was unfair to use gas. Wasn't gas used in WWI? Hadn't there been a Presidential Decision Directive around for years on gas? Podonsky even trained several "site" guards on gas last summer. Apparently it didn't sink in that the use of gas was in the offing. Yet the guard force was totally disoriented in the face of gas and the use of gas masks.

In addition, Podonsky did not use the full DBT – no active insider, no 50 caliber API rounds that would immediately reduced the HMMVs to rubble, and no serious diversions.

Combat Effectiveness

In addition to the problems Podonsky pointed out, there are fundamental flaws in basic tactics and bizarre claims by "site" security (the same security officials who brought you the hard drive problems).

First, to guard this site, they are dependant on outside responders coming down a public road from another site. This is a unique requirement in the weapons complex.. Podonsky mined the road. Despite the fact the responders knew the first vehicle was destroyed by a mine, they continued through the mine field. This is bizarre. Military doctrine dictates that a convoy stop in this situation. Not at "the site." Unbelievably, they claimed their time lines were too short to stop.

Even more importantly, despite the absolutely critical requirement for denial at one facility – denial failed. It is clear that if denial failed, in the initial carnage, such a facility cannot be retaken because of the extraordinary percentage of losses – in the neighborhood of at least 50% – in the first engagement. Military doctrine dictates when losses exceed 20%, forces become combat ineffective due to communications and basic squad sized tactics. "The site" lost 50% – with eight dead on the doorstep. At this point, according to combat veterans there would be no further offensive action to recapture the facility by the guard force. In a number of scenarios, even when the guard force is successful in repelling an attack, they lose up to 80-95% of the force. This is simply unrealistic. "Site" security officials admit this is a problem, but they claim they have unusually brave people. Real bullets may make a difference in their calculation.

Cost of Security

– The cost at "the secure area" alone is over $30 million – both direct and indirect costs. In addition, there are substantial costs to operate the area.

– "The site manager" claims they only do about $3 million worth of work – not a good investment even for DOE.

– As we pointed out in April, we can move the site, make it more secure, and spend less than a third of current expenditures on security.

SOLUTION: IMMEDIATELY DEINVENTORY THIS SITE

– A credible plan was developed in April to do just this: move mission-justified reactors and material to DAF and move excess material to Oak Ridge and Savannah River.

– In April you opted to move the site with an EIS to be completed on Dec. 15th and a MOD on the location on Jan. 15th. DP defied your order with a slow roll so you wouldn't be able to make a decision on relocation before you left. The current estimated date of an EIS is Sept '01 in the Bush Administration.

If we can't make a reasoned decision on this issue, when can we?

THE EFFECT OF CASUALTIES ON MILITARY OPERATIONS.

- Fighting units are traditionally made up of standard numbers and configurations of combatants. The need to fire at an adversary and maneuver to engage more effectively requires teams that not only coordinate timing and effort but also coordinate weapons systems for effectiveness. In infantry language this means one guy fires while the other moves. Further teams are divided into support and maneuver elements as well as supporting fires teams (machine gun or mortar support). Single combatants seldom last long on the battlefield!
- Communications, reporting to the command structure or command post and coordination of the above maneuver elements requires additional specialization and manpower.
- As a unit sustains casualties (dead or wounded) elements of the fire and maneuver schemes or "close quarter battle" drills begin to come apart. Individuals are left uncovered and unable to maneuver without increasingly costly losses, units find their flanks exposed as high attrition rates slow down coordinating elements and the attack sputters and loses momentum or the defense begins to gap and turns into a route. Think here of hand-to-hand combat with knives and bayonets-just the kind of thing we want for our sons, daughters or employees!
- Individual replacements are moved into position by command elements as quickly as possible when trained replacements are immediately available. However, if casualties are high (in excess of 10%) qualified replacements become increasingly problematic and command and control begins to be lost.
- To avoid the geometric effect of these type loses the military has developed a number of rules-of-thumb for infantry combat. When small units take significant casualties they are replaced by the organizations "reserve force" until they are reconstituted (replaced, rearmed, trained and rested). Units are normally considered "combat ineffective" and are rotated off the line when they have sustained 15-20% casualties. At this point maneuver, fire rates, communications and command and control can no longer be relied on to support the mission. Continuation would be expected to result in unnecessary and increasingly high casualties with little expectation of success.
- When a mission is critical it is mandatory that there be not only adequate numbers of well trained and well armed forces but also tested contingency plans and an adequate reserve force to reconstitute the fighting unit immediately as casualties are sustained and before momentum shifts to the adversary. If any of these elements are not present the mission is either not critical or the leadership is incompetent.

Appendix B:

Memo from Richard Levernier, Program Manager Assessment and Integration to:
Edward J. McCallum, Director Office of Safeguards and Security

December 12, 1998; and

Memo from Richard Levernier, Program Manager Assessment and Integration to:
Edward J. McCallum, Director Office of Safeguards and Security

April 19, 1999

With attachments

Memorandum. To: Edward McCallum. From: Richard Levernier. Dec. 12, 1998.

(U) The purpose of this memorandum is to provide a preliminary summary of some potentially significant informa6tion that was developed during the JTS evaluation of the TSD SSSP conducted at Sandia Laboratories during the period of December 7-17, 1998. The final report of this activity, including the ALPHA analysis and physical security system review, is expected to be available in January 1999. The first week was devoted to developing worst case scenarios and developing assumptions necessary to allow JTS modeling. OSS, TSD, SNLA and DP representatives participated in this activity. Three worst case scenarios were developed which were consistent with the TSD SSSP worst case scenarios. The second week was dedicated to conducting simulations.

(U) JTS results on the first worst case scenario (single facility subsistence stop) were 3 losses and no wins.

(U) JTS results on the second worst case scenario (bridge out) were 3 losses and 1 win.

(U) The high TSD JTS loss rate for the first two worst case scenarios caused TSD to request termination of JTS activity. TSD requested OSS assistance to analyze the poor results and begin to determine possible corrective actions.

Memorandum: To: Edward McCallum. From: Richard Levernier. Subject: Results of Draft Transportation Safeguards Division (TSD) Site Safeguards and Security Plan. April 19, 1999.

(U) During the review process, draft copies of the ALPHA, JTS, and PSSR reports were provided to TSD along with a request for their review and comment. The ALPHA and JTS reports were provided to TSD January 28, 1999. The PSSR report was provided to TSD on April 1, 1999. TSD has indicated that they plan to provide an integrated response that addresses all three reports. To date, TSD has not provided comments on any of these reports.

(U) The OSS QA review examined the draft TSD SSSP and the available supporting documentation. A draft document was reviewed pursuant to an agreement between NN, TSD and AL management (Joe Mahaley, NN; Debbie Miller, TSD; Larry Kirkman, AL). The purpose of reviewing the draft was to expedite processing of the document by addressing HQ concerns prior to AL and TSD final approval. However, the draft documents was stated to be an accurate description of current TSD operations. Accordingly, issues identified during the review require expeditious resolution since they pertain to currently existing vulnerabilities and weaknesses.

(U) A root cause analysis of the basic factors of special agent effectiveness can be summarized in three areas referred to in the JTS protocol document as "robustness factors." The robustness factors are: (1) strength of the TSD force, (2) tactics, and (3) weapons/equipment. A detailed review of these factors is also in the ALPHA report.

(U) As the attached chronology of events shows, DP management was briefed on these issues by NN on March 1, 1999, and again on March 4, 1999. TSD has had the ALPHA and JTS reports, which describe the critical issues, since early February 1999.

(U) On February 4, 199 via memo (Solich to Miller, copy attached), NN requested TSD comments by February 16, 1999 to "potentially very significant issues." TSD has not replied to the memo, although a staff member sent an e-mail to FOD stating the TSD would respond after the receipt of the PSSR. TSD received the PSSR on April 2, 1999.

Briefing Material for General Habiger. August, 1999. 3 unclassified slides.

Hafner memo. June 30, 1999 Subject: TSD SSSP (U).

(U) TSD has stated a response to those reports and the subsequent risk level those reports indicate will be forth coming by June 30, 1999.

TSD FAILS TO RECOGNIZE PROBLEM

- TSD INTERIM DISPOSITION OF NN COMMENTS (RECEIVED 8/15/99) DEFERS ALL ISSUES TO FY 2000 SSSP
- NO IMMEDIATE COMPENSATORY MEASURES PROPOSED BY TSD
- TSD CONDUCTED ADDITIONAL JTS MODELING W/O NN PARTICIPATION AND DID NOT DISCLOSE RESULTS
- TSD CONDUCTED BARRIER TESTING W/O NN PARTICIPATION AND DID NOT DISCLOSE RESULTS
- FOCUSED ONLY ON 1998 ANNUAL REPORT TO THE PRESIDENT ISSUES THAT CONTRIBUTED TO "MARGINAL" RATING

ISSUES

- TSD HAS FAILED TO ACKNOWLEDGE THE "HIGH RISK" CONDITION AND INSTITUTE COMPENSATORY/CORRECTIVE ACTIONS
- TSD CANNOT ACHIEVE A "SATISFACTORY" OR "GREEN" STATUS IN THE 1999 ANNUAL REPORT TO THE PRESIDENT UNTIL THE "HIGH RISK" CONDITION IS ADDRESSED

KEY EVENT CHRONOLOGY

10/98 NN RECEIVED DRAFT SSSP

1/99 VA ANALYSIS AND JTS REPORTS, WHICH IDENTIFIED HIGH RISK, PROVIDED TO TSD

2/99 TSD COMMENTS ON JTS & VA ANALYSIS REPORTS DUE (TO DATE, NO COMMENTS)

2/99 INTEGRATED QUALITY ASSURANCE REPORT COMPLETED - DISCLOSES TSD AT "HIGH RISK" IN WORST CASE SCENARIOS

2/99 NN-50 BRIEFED ON TSD HIGH RISK

3/99 DP BRIEFED ON TSD HIGH RISK

4/99 PHYSICAL SECURITY SYSTEMS REPORT, WHICH ID'd SINGLE POINT OF FAILURES, PROVIDED TO TSD (TO DATE, NO COMMENTS)

Department of Energy
Germantown, MD 20874-1290

JUN 30 1999

MEMORANDUM FOR STEVEN HAFNER, DIRECTOR
TRANSPORTATION SAFEGUARDS DIVISION (TSD)

FROM: OWEN B. JOHNSON, ACTING DIRECTOR
OFFICE OF SAFEGUARDS AND SECURITY

SUBJECT: TSD Site Safeguards and Security Plan (SSSP)

Based on our review of the draft SSSP, there remain some issues that need further elaboration prior to meeting SSSP standards. Please accept the attached comments for consideration in the next version of the SSSP. The attachment contains specific concerns which, as you are aware, were previously briefed to NN and Defense Programs management.

Our recommendation is that work on the current draft version be terminated. However, should you choose to go forward with the current draft, we recommend that TSD use that document as a description of current operating conditions. All other SSSP related activities can then be focused on development of the new SSSP. The new document should address the attached comments and build upon progress to date and work projected to be completed over the next 12-18 months. My staff is available to work with you on this and any other issues of benefit to the TSD mission.

If you have any questions, please contact John Cronin, of my staff, at 301-903-6209.

Attachment (S/NSI)

cc:
W. Hensley, DP-45
L. Kirkman, AL

When separated from attachment,
handle this document as UNCLASSIFIED.

Appendix C:

Memo from Richard J. Levernier, Program Manager Assessment and Integration to: James L. Ford, Acting Director Field Operations Division

April 11, 2000

With attachments

Department of Energy
Germantown, MD 20874-1290

APR 11 2000

MEMORANDUM FOR: JAMES L. FORD, ACTING DIRECTOR
FIELD OPERATIONS DIVISION

FROM: RICHARD J. LEVERNIER, PROGRAM MANAGER
ASSESSMENT AND INTEGRATION

SUBJECT: ROCKY FLATS PROTECTIVE FORCE REDEPLOYMENT

References:
1. Memorandum, H. Dalton to E. Habiger, dated January 14, 2000, subject: Protective Force Reployment Schedule
2. E-mail message, D. Noble to O. Johnson, dated February 24, 2000, subject: Rocky Flats Reconfiguration JTS
3. Memorandum, R. Levernier to J. Ford, dated March 28, 2000, subject: Deadly Force Training Deficiencies at Rocky Flats
4. SO-212.1 Trip Report, dated April 11, 2000, subject: Rocky Flats Trip, March 21-26, 2000

The purpose of this memorandum is to summarize our activity in support of the above captioned subject. On January 14, 2000, the DOE Rocky Flats Field Office (RFFO) invited our participation in their vulnerability assessments (VAs), performance testing and computer modeling, using Joint Tactical Simulations (JTS), of the proposed protective force redeployment (see reference #1). I was assigned to lead the Office of Safeguards and Security (OSS) team in conjunction with the Rocky Flats Facility Officer.

The OSS team participated in the JTS runs February 14-18, 2000. Reference #2 contains a summary and conclusions concerning that activity. The team returned to Rocky Flats again March 21-26, 2000, to observe Force-on-Force (FOF) exercises. References #3 & 4 contain summaries and conclusions of that activity.

DOE Order 470.1, Chapter III, 3.b. states, "The adequacy of new and existing protective systems shall be confirmed through testing prior to operational use and periodically thereafter". DOE Order 470.1, Chapter I, 4.d.1. also states, "Changes to the Plans (SSSP's) that significantly alter the agreed-on protection philosophy or performance standards of protection systems shall require approval by the Head of the Field Element and concurrence by the cognizant program office and the Director of Security Affairs." The Rocky Flats VAs, JTS and performance testing were conducted, at least in part, to satisfy these requirements. It is the consensus opinion of the OSS team that Rocky Flats has not confirmed the adequacy of the new protective force deployment through testing prior to operational use. Accordingly, it is recommended that the Director of Security Affairs non-concur with the proposed redeployment until the required confirmatory testing is completed.

cc: O. Johnson, SO-21
L. Wilcher, SO-211.3
D. Solich, SO-212.2
S. Callahan, SO-212.1
K. Coady, SO-212.5
D. Noble, SO-212.1
J. Pope, PNNL
J. Sandoval, SNL-NM

United States Government | Department of Energy

memorandum

Rocky Flats Field Office

DATE: JAN 14 2000

REPLY TO ATTN OF: AMFD:SSD:RGB:00-01116

SUBJECT: Protective Force Redeployment Schedule

SO-20 who do you propose to send?

TO: Eugene E. Habiger, Director, Office of Security and Emergency Preparedness, SO-1
Maurice W. Daugherty, Safeguards and Security Team Leader, Office of Integration and Assessment, EM-5, HQ

The Rocky Flats Environmental Technology Site (Site) is currently preparing to implement a revised Protective Force Deployment. The revised deployment was developed to provide maximum protection for special nuclear material while supporting the Site's accelerated closure mission. The redeployment will be implemented by April 8, 2000. The week of February 14, 2000, has been set aside to conduct Joint Tactical Simulation runs and validate the procedures, vulnerability assessments, and performance tests. A force on force exercise is scheduled for March 25, 2000.

The purpose of this memorandum is to invite the participation of your organizations in the evaluations, which shall be led by the Director of the RFFO Safeguards and Security Division.

If you have any questions, contact Richard Bartlett, of my staff, at (303) 966-3214.

Henry F. Dalton, Assistant Manager
Facilities Disposition

From: Noble, Douglas
Sent: Thursday, February 24, 2000 7:53 AM
To: JOHNSON, TOBY
Cc: Ford, Jim; Solich, Donald; FRAGOYANNIS, NANCY; Levernier, Richard; Noble, Douglas; Joe Sandoval (E-mail); Jack Pope (E-mail); Freemont (Monty) Mortensen (E-mail)
Subject: Rocky Flats Reconfiguration JTS

Toby, attached is a summary of last week's visit to the Rocky Flats Field Office (RFFO). Please let me know if you think its appropriate for us to forward this document to EM and RFFO or simply discuss our conclusions with them. This document was coordinated with Rich Levernier, Joe Sandoval, Monty Mortensen, Jack Pope, and Nancy Fragoyannis.
Doug

rfjts022000summary.wpd

Rocky Flats PF Redeployment JTS Testing Summary
February 14-18, 2000

Representatives of the Offices of Safeguards and Security and Environmental Management were present at the request of the Rocky Flats Office (RFFO), to observe the use of the Joint Tactical Simulation (JTS) system to validate the proposed Protective Force (PF) redeployment. These representatives from DOE Headquarters were Toby Johnson, Director, Office of Safeguards and Security, SO-21; Rich Levernier, Program Manager, Assessments and Integration, SO-212.1; Doug Noble, Headquarters JTS Administrator, SO-212.1; Nancy Fragoyannis, RF Desk Officer, SO-212.2; Joe Sandoval, Sandia National Laboratory Albuquerque (SNLA); Jack Pope, Pacific Northwest National Laboratory (PNNL); Monty Mortensen, Idaho National Engineering and Environmental Laboratory (INEEL); Randy Scott, Director, Office of Safety, Health and Security, EM-5; Maurice Daugherty, EM-62 and Keith Hedman, EM-62.

On Monday, February14, 2000, a briefing was conducted by DOE and Wackenhut Services, Inc. (WSI) management to outline the week's proposed activities. Jim Steward, DOE Safeguard and Security Director stated that he was the lead for the project with support provided by Richard Bartlett (RFFO) and Al Garrett (RFFO). He stated that RFFO is the approving authority for the redeployment. He also stated that Force-on-Force (FOF) exercises are scheduled for the month of March, 2000. Depending on the results of the JTS and FOF testing, a decision by RFFO will be made whether or not to implement the Redeployment Plan by April 1 or April 8, 2000,

Wackenhut was responsible for conducting the JTS simulations with Marty Anderson - Simulation Director, Bill Brunsdon - Senior JTS Controller, Mike Henry - JTS System Controller, Dave Cutlip- Blue Controller, Cecil Richburg/Mac Thacker - Red Controller, Ken Ferguson, Steve Yonkoff/Dave White - Red Commanders, Paul Metzger, and Bill Williams, Mike Merlino, Rich Watson - Blue Commanders. Wackenhut employees were used as the JTS operators.

JTS runs began Tuesday, February 15 at 8AM and continued until 5PM Friday, February 18, 2000. At the end of each day, a DOE Debrief (DOE RF and DOE HQ) discussion was held. Additional JTS runs will be continued during the week of February 21-25, 2000. Two "worst-case" scenarios were used for the JTS runs with a couple of "dummy" scenarios interspersed to prevent "gaming." A JTS final report is to be issued by RF on March 29, 2000.

After the observation of 21 JTS runs as of COB Friday, February 18, it is the coordinated opinion of Rich Levernier, Doug Noble, Nancy Fragoyannis, Joe Sandoval, Monty Mortensen, and Jack Pope that due to the limited capabilities of the JTS operators, a valid conclusion on the result of the JTS runs could not be made. The operators had trouble (1) maintaining the critical time lines for the Pro Force and the Adversaries as stated in the reconfiguration Vulnerability Assessment (VA), (2) using the JTS user interface to order the PF and Adversaries to complete tasks, and (3) completing tasks in a realistic time-frame. These conclusions were shared with RF site personnel. While the JTS simulations were inconclusive from a validation of the redeployment perspective, they were valuable from a training standpoint.

Department of Energy
Germantown, MD 20874-1290

MAR 28 2000

MEMORANDUM FOR JAMES L. FORD, ACTING DIRECTOR
FIELD OPERATIONS DIVISION

FROM: RICHARD J. LEVERNIER, PROGRAM MANAGER
ASSESSMENT AND INTEGRATION

SUBJECT: Deadly Force Training Deficiencies at Rocky Flats

The purpose of this memorandum is to describe a problem, with potentially serious consequences, that currently exists at Rocky Flats. Several recommendations to address this issue are also provided for management consideration. While validating the Rocky Flats (RF) Site Safeguards and Security Plan (SSSP) in October 1999, the HQ SSSP Assistance Team review of protective force performance test documentation disclosed an alarming trend concerning the inappropriate use of deadly force. During protective force performance tests of response to criticality alarm building evacuations, site reports noted, "...the response of the protective force, when their orders to halt were disregarded, was to fire indiscriminately into the crowd of evacuees." The same report also stated, "It is difficult to justify the wholesale killing of the building evacuees, when none among them - even the adversaries - had yet exhibited any behavior which offered a clear risk to either special nuclear material (SNM) or the life of any protective force member." The report also stated, "Subsequent performance testing conducted Saturday, February 28 (Scenario #2), also revealed similar issues involving the use of deadly force against building evacuees who demonstrated no immediate threat to either SNM nor security police officers (SPOs), but who simply disregarded SPO orders to "halt" while evacuating in response to a criticality alarm. This situation offers potential liability, is of concern, and deserves further inquiry." (Reference RF Protective Force Test Report April 1998). Additionally, the July 1998 DOE Office of Independent Oversight and Performance Assurance Report on RF cited problems in the use of deadly force during protective force performance test exercises.

In response to the HQ SSSP Assistance Team concerns on this matter, RF provided documentation that showed remedial training had been conducted concerning the use of deadly force. Additionally, RF representatives stated that subsequent performance tests would be carefully monitored and evaluated from a use of force perspective. This information appeared reasonable and sufficient to address the issue from a SSSP standpoint.

In March 2000, HQ participation in the RF protective force redeployment initiatives and subsequent performance testing again disclosed similar serious concerns regarding the inappropriate use of deadly force by the RF protective force. Two Multiple Integrated Laser Engagement System (MILES) enhanced exercises were observed where protective force members "killed" building evacuees, controllers wearing orange safety vests, and each other. During the

Reference #5

critique conducted immediately after the exercise, protective force and other site management personnel failed to raise concerns related to the inappropriate use of deadly force. In fact, no critical observations were surfaced by management at the critique. Site analysis of these exercises is still ongoing.

Some of the exercise controllers and evaluators, with the primary responsibility for evaluating protective force performance, were not qualified to evaluate protective force members decisions concerning the use of deadly force. Administrative personnel, safety professionals, personnel security specialists, and others lacking a comprehensive understanding of the DOE Deadly Force Policy were utilized in these critical roles. Accordingly, the feedback concerning protective force performance, including the application of deadly force, was flawed.

As we all know, in the real world (versus MILES enhanced exercises) serious consequences are associated with the use of deadly force. Since we rely heavily on MILES enhanced exercises for protective force training and testing, we must ensure that appropriate serious consequences exist concerning the use of deadly force in these environments. In law enforcement training environments, the typical "penalty" for killing a "friendly" is failure of the test. At RF, there are currently no negative consequences for the inappropriate use of deadly force. In fact, if the adversaries are "killed" in the process, the result is actually a win from the sites current perspective. This situation is unacceptable and must be addressed immediately.

Recommend that HQ request RF and the cognizant Program Office to address this critical issue immediately. We must jointly ensure that the RF protective force fully understands the DOE Deadly Force Policy and applies it appropriately in training and testing environments. We must ensure that the remedial training is effective and validated with appropriate testing. Finally, we must document our actions and ensure this issue is monitored carefully in the future. Please let me know if you have any questions.

cc:
Toby Johnson, SO-21
Skip Bowser, SO-211.1
Larry Wilcher, SO-211
Don Solich, SO-212.3
Kelly Coady, SO-212.3

SO-212.1 TRIP REPORT FOR ROCKY FLATS MARCH 21-26, 2000

BACKGROUND:

DOE-RFFO is planning to transition to a new protective force (PF) reconfiguration in order to maximize effectiveness based on material consolidation activities, consolidation of high-value special nuclear material operations and potential restructuring of the protected area. A series of JTS runs and Force-on-Force (FOF) exercises have been scheduled to performance test and analyze the proposed reconfiguration.

At the request of DOE-RFFO, a Rocky Flats (RF) assistance visit was conducted on March 21-26, 2000, to: (1) observe the Rocky Flats Protective Force (PF) reconfiguration Force-on-Force (FOF) exercises, (2) review the JTS files supporting the PF reconfiguration, and (3) review any vulnerability assessments (VAs) supporting the PF reconfiguration. The SO sponsored assistance team consisted of Rich Levernier - SO-212.1, Sam Callahan - SO-212.1, Doug Noble - SO-212-1, Jack Pope - PNNL and Joe Sandoval - SNL-AL.

The following are the observations and conclusions derived from the assistance visit activities.

GENERAL:

ISSUE # 1: SO HQ representatives ability to complete the assigned mission:

- HQ reps (Levernier, Callahan, Noble & Sandoval) were asked to leave the site on March 22 because Mr. Hank Dalton stated the visit had not been coordinated with his office. SO-21 contacted Mr. Dalton and reminded him that we were there as a result of a written invitation from DOE-RFFO to SO-1. We were authorized site access at about noon on March 22.

- HQ reps were denied access to VA time line information that was needed to evaluate the relationship between the worst case scenarios in the VA's, JTS and performance tests.

- RF provided the redeployment JTS tapes to SNL-NM too late for any analysis to be performed prior to the scheduled performance tests.

IMPACT: Continued denial of access to the site and/or information severely degraded the ability of the SO HQ team to "verify" the accuracy of the FOF vs. the JTS runs vs. the VAs. The lack of information access forced the SO HQ team into a pure observer role without the means to determine if the FOF was truly representative of the worst-case. Note: The FOF scenario was significantly modified from the November 1999 worst-case scenario.

ISSUE #2: Vehicle search procedures.

- Two HQ representatives observed routine access control procedures at vehicle

portal 1 and observed the following sequence of events: (1) the truck to refuel the PF vehicles entered the vehicle portal (inner gate closed, outer gate open), (2) the driver exited the vehicle and open all external doors and compartments, (3) the driver exited the vehicle portal and proceeded to the personnel portal to "process-in", (4) outer gate closed and the inner gate opened, (5) the driver exited the personnel portal and returned to the truck, (5) the driver closed all doors and compartments and got in the fuel truck, and (6) the driver/fuel truck entered the Protected Area to begin refueling the PF vehicles. The vehicle was not searched as per DOE-RFFO procedure.

IMPACT: The observed vehicle search did not comply with DOE policy or stated DOE-RFFO procedure. The RF site VA assumes some level of protection/credit for vehicle searches, if the observed vehicle search is representative of the normal vehicle search program the credit taken by the site will need to be re-assessed.

ISSUE #3: Use of Grizzly Hitch in a training mode versus a "verification" mode.

- DOE-RFFO management requested that Grizzly Hitch provide a military style scenario briefback to site management. Grizzly Hitch complied with the request, but noted in the briefing that they had no role in scenario development, i.e., the scenarios were developed by the RF personnel without external input (e.g. Grizzly Hitch).

- The MILES enhanced exercises that were observed were NOT tests. The exercises did provide valuable training and orientation to the proposed redeployment.

IMPACT: The exercises as observed were not for validation of the reconfigured PF. The exercises were designed to test the command, control and communications of the PF in the new response positions but do not serve as a "validation" of the reconfiguration plan. Additionally, there is no indication that RF plans to validate the PF reconfiguration prior to implementation. The use of Grizzly Hitch for training activities is not an efficient use of a limited resource. A DOE comprised team could have accomplished the RF established adversary objectives.

FOF ISSUES:

ISSUE #4: Artificialities of the FOF exercise scenario development and execution.

- The Protective Force (PF) received a briefing before the exercise on what type of explosives (size, shape, characteristics, etc.) would be used by the adversaries. While the PF needed to be informed that the adversary may be using explosives, the information regarding the exact types and configurations was unwarranted. The PF controllers should have been given the briefing and indicated to the PF when they had been affected by these devices.

- The exercise scenarios were not worst case and were different from the scenarios

in the VA's and redeployment JTS.

- RF lacked the MILES equipment required by Grizzly Hitch personnel to replicate the weapons mix modeled in JTS. 7.62 mm MILES transmitters were placed on M-16's to simulated 7.62 sniper rifles and no .50 caliber weapons/simulators were available to the adversary team. The team was provided with 9mm submachine guns which were of extremely limited use by the adversary team. Only one Light Anti-tank Weapon simulator was available to the adversary team. This weapons mix was not adequate to engage a force the size of the RFETS protective force.

- The RF MILES weapons assigned to the Grizzly Hitch personnel were only operating at about 1/3 of their effective range. This limitation significantly degraded their capability and necessitated changes in tactics to attempt to compensate for this limitation. This weapons range limitation is the primary factor that resulted in the scenarios being considered less that worst case. Three M-4's were provided as well as two M-16's with scopes to simulate sniper rifles. No 7.62mm sniper rifles or .50 calibers were available.

- The MILES equipment utilized by exercise participants had premature (false) kills, sensitivity problems (no kills) and other calibration concerns.

- RF prohibited Grizzly Hitch personnel from using their own radios and frequencies, due to safety concerns. The radios provided for OPFOR use by RF were capable of being monitored by the protective force and provided unreliable (intermittent) communication and for the majority of the exercise Grizzly Hitch could not effectively communicate.

- Most of the protective force personnel participating in the exercises responded in unmarked vehicles without warning lights and sirens. The marked vehicles were assigned to the shadow force. The result was that exercise responders had an unrealistic advantage (stealth) in their response.

- Although the scenarios called for the OPFOR to breach fences during their escape, RF did not allow the adversary team to cut or climb fences due to operational and cost considerations. Administrative holds were used to allow adversary team members to cross fences with a ladder. These actions allowed protective force members to regroup, rethink, determine the exact point of exit from the target area and also breaks the momentum of both protective forces and adversaries.

- Vehicles were not allowed to travel off of roadways. Road blocks were simulated by a PF vehicle being parked on the side of the road and a traffic cone placed in the center of the road. Adversaries vehicles were not allowed to drive off the road and around these road blocks.

- RF protective force managers and uniformed supervisors were well aware of the redeployment worst case scenarios that were being evaluated in the exercises. Additionally, the scenarios were briefed to numerous persons that were not in a "trusted agent" status. The target buildings and the order of the attacks were known to all exercise participants prior to the exercises.

- Not all PF wore complete MILES gear and thereby were able to survive repeated rounds from adversary weapons.

- Briefer stated that no PF would respond to roof in an actual "Crit" alarm although the roof was in play during the execrise.

- The number of adversaries allowed in the PA was limited and was not representative of the numbers utilized in the November 1999 worst-case scenarios.

IMPACT: The FOF cannot be considered a validation of the RF PF reconfiguration. The artificialities engineered into all phases of the FOF raise serious doubts as to the validity of the FOF as a validation exercise. The benefit derived as a training mechanism prior to reconfiguration is significant, but the subject FOF did not meet the criteria as a validation exercise.

ISSUE #5: Systemic use of deadly force beyond accepted policy.

- Significant deficiencies were noted in the RF protective force use of deadly force and the qualifications of some exercise controllers and evaluators to evaluate the application of deadly force by protective force members. Reference memo: Levernier to Ford, 3/28/00, Deadly Force Training Deficiencies at Rocky Flats.

IMPACT: RF PF members continue to use deadly force in a manner inconsistent with departmental policy. DOE-RFFO had agreed in November 1999 to institute training designed to eliminate this concern. However, the FOF clearly demonstrates that the issue still exists.

Comment: Uncleared controllers were used for outside (the PA) PF responders. This seems to violate the premise that the contents of the exercise were sensitive if not classified.

Comment: On the positive side, most of the controllers did seem to keep a distance from their players and tried not to give away player positions as was observed during the Fall 1999 FOF. Players also seemed to sit down and remain motionless once they had been neutralized. This was also a change from the Fall 1999 FOF. Additionally, during a battle near the fence, the PF commandeered an adversary van and was able to use it to pursue additional adversaries.

CONCLUSION:

The consensus of the team following the assistance visit is: (1) the FOF exercises as conducted cannot be considered validation exercises but rather training exercises, (2) the artificialities built into the FOFs severely degraded the quality of the information gathered and, (3) systemic issues continue to exist at RF regarding the appropriate use of deadly force.

OFFICE OF SECURITY AND EMERGENCY OPERATIONS (SO-1)
ROCKY FLATS ENVIRONMENTAL TECHNOLOGY SITE (RFETS)
SITE SAFEGUARDS AND SECURITY PLAN STAFF ASSISTANCE TEAM
OBSERVATION COMMENTS
ON 10/23/99 FORCE-ON-FORCE (FOF) EXERCISE SCENARIOS (U)

Two FOF exercise scenarios were conducted on 10/23/99 for the purpose of evaluating a planned protection strategy for RFETS security interests. Four SO-1 Team members (Rich Levernier, Team Leader [SO-212], Doug Noble [SO-212], Ronnie Edge [SO-211], and Jack Pope [PNNL]) attended required pre-exercise briefings, observed the FOF scenarios, and attended the exercise de-brief. Comments regarding SO-1 team observations made during these activities are provided below.

PRE-EXERCISE

1. Two senior Wackenhut Services Limited Life Corporation (WSLLC) managers (i.e., General Manager and Manager, Security Planning and Integration Department [SP&I]) advised that the FOF was more "diagnostic" than "evaluative" in nature, due to the fact that no hands-on training had occurred involving the new "redeployment strategy" (i.e., Configuration B). The General Manager advised that exercise play might be stopped to reposition PF personnel since no physical, hands-on training had occurred. The training on Configuration B to date had consisted of "read only" materials. Further training is planned for the November-December 1999 time period.

2. During the briefing M. Anderson, the WSLLC SP&I Manager, briefed (without elaboration) the controllers that several of the PF did not have Engagement Simulation Systems (ESS) handguns and they would have to make controller calls during close contact action. When asked about this after the FOF Anderson advised that the PF did not all have ESS handguns because: 1) usually PF personnel did not use their handguns during a FOF, and 2) due to the fact that the adversaries needed handguns because of scenario requirements, there was a shortage of handguns. Logistically, the second reason is understandable; however, the first reason given is not. The lack of the PF having all assigned weapons available to them does not provide assurance that realistic testing data will be gathered if scenario flow causes handguns to be used (e.g., lack of rifle ammunition, lengthy weapons engagements, weapons malfunctions, adversary capture of "downed" PF weapons, etc.).

   It was also noted that some PF personnel had been issued ESS weapons (MP-5s and M-60's) that they do not field as part of current or planned protection strategies. Prior to the exercise PF union representatives discussed this concern with the WSLLC General Manager.

EXERCISE

1. It is questionable as to why the exercise was conducted during daylight hours when the SO-1 team was advised that a Hotel Condition could last over 24 hours. Conducting the FOF in darkness would have facilitated adversary deployment, impacted PF observation of adversary locations, and would have been a more realistic worst case situation. During both scenarios, the PF was more readily able to see adversary locations. Conducting the scenarios in daylight hours provided excellent training opportunities; however, conducting the scenarios during hours of darkness would provide for more realistic performance testing and evaluation activities. In the second scenario involving Building 707 an adversary sniper was spotted by the PF prior to the exercise window opening. This was noted by the senior controller; however, the adversary was not re-positioned prior to the window being opened.

2. During the FOF the SO-1 team was confined to an observer vehicle or in a tower to ensure their presence did not impact the exercise. While in a protected area perimeter tower during the first scenario the SO-1 team observed a senior RFFO representative and a senior KH representative roaming freely and standing and sitting on the west of Building 371, in the middle of adversary/PF engagements and the planned adversary escape route. Their presence may have seriously impacted the FOF by prompting PF personnel of possible adversary actions in the area by their mere presence and causing undue attention to that side of the building.

3. It was noted that all PF vehicles are distinctly marked with large letters and numbers, for unit identification purposes, and are easily identifiable from long distances. This practice is questionable as it may allow an adversary to quickly identify senior PF command and other key PF response elements.

4. During the Building 371 scenario it was observed that several "killed" exercise players (both adversary and PF) remained on their feet and moved about after being killed. This caused considerable confusion among the PF as to who was where, who was up, etc. Controllers with these "killed" units also moved about and remained in a highly visible state, which also added to the confusion. Collectively, this severely impacted the realism of the FOF.

5. It was also observed that both adversary and PF controllers were easily spotted by their orange vests which allowed both sides to locate player positions. Again, most of this observation was a result of conducting the FOF during daylight hours. However, the following actions should be considered to ensure more realistic play: 1) where possible controllers should attempt to remain a reasonable distance away from assigned units unless absolutely necessary, 2) controllers should use appropriate tactics to hide the orange controller vests from player observations (e.g., use cover and concealment, low crawl, etc.), 3) controllers moving with adversaries in the brush should wear camouflage fatigues and not put their vests on until absolutely necessary, and 4) controllers assigned to "killed" adversaries and PF personnel should maintain a low profile, where possible.

6. During the Building 371 scenario three Special Response Team (SRT) personnel with a machine gun were observed moving from the north east side of the building into an area without utilizing any cover and concealment or speed where other PF personnel had been engaged and killed. After the players positioned the machinegun on a berm, one of the SRT was observed establishing a rear guard position covering facing the northeast exposed and in the open without proper cover.

7. During the Building 371scenario a PF player was observed at the northeast of the building without his/her protective mask on at least five to seven minutes after the adversaries on that side of the building had employed simulated chemical irritants. A controller was observed speaking to the PF player, at which time the player removed his/her mask from its carrying case and donned it. Since the scenarios were training driven and the controller was prompting the player to don the mask, this would be acceptable. If the exercise had been of a more evaluative nature, then this would not have been appropriate.

8. During the same scenario a PF player on the roof of Building 707 was heard to advise over the radio that "we have been hit by sniper fire" and then there was no further traffic from that unit. This presents a question as to whether or not the PF member had transmitted this information prior to or after being taken out. That unit's controller should be queried to ascertain this fact.

9. It was noted during the Building 371 scenario that there was very little PF communication regarding intelligence as to the status of adversaries (numbers, locations, downed, etc.) for intelligence and tactics purposes.

10. The SO-1 observers received conflicting information regarding the second scenario. The scenario, as briefed, required the adversaries to enter a building through an alarmed door and fight down a hallway to a target area. It was noted that the adversaries could have come in a different doorway very near the target without having to fight down the hallway, thus decreasing traversal time and interruption probabilities. After the exercise the WSI SP&I Manager advised that the original scenario called for the adversaries to breach at a location near the faraway door and not come in that door. The door was opened in an administrative function. It was then pointed out that if the scenario called for such a breach then the door alarm would not come into play, thus drastically decreasing detection of the adversaries. It was also noted that the scenario called for adversaries to escape using a route to the east side of the protected area, which was the longest and least advantageous route. This portion of the scenario was not realistic, especially due to the time of day the exercise was conducted.

    Additionally, if the adversaries activated a door alarm the PF would have, in all probability, viewed this as part of the evacuation activities caused by the criticality alarm and not as an intrusion.

11. During the first 707 scenario Exercise Hold PF supervisors were heard on the radio talking and instructing to contact each other via "land lines" (telephone). PF controllers should not have allowed this activity to occur. Such activity does not provide assurance that scenario flow is not compromised.

POST-EXERCISE

1. During the exercise "hot wash" the adversaries presented their planned actions per the scenarios and their actual actions conducted as a result of exercise play. The PF supervisor in charge of the PF deployment during the FOF was not present; therefore, no information of any value regarding PF actions during the FOF (for either scenario) was briefed. The second in command PF supervisor was asked to speak and he only stated that "everyone did a good job" and "communications were good." PF participants were overheard to say among themselves that use of the new call signs was confusing during the exercise.

2. An issue involving the classification of a document associated with the exercise has been discussed separately with M. Anderson, WSLLC.

3. ESS vehicle engagement systems (harnesses) were not utilized for PF and adversary vehicles. Controller calls were required to be made to determine vehicle/occupant kills. During the safety/controller briefing conducted on 10/22/99 it was briefed that unless individuals' (driver and occupants) harness was activated they would be allowed to exit the vehicle and continue to participate in the exercise. While this may be valid for small arms, a vehicle kill from large arms (LAW, RPG, AT-4) would probably result in both vehicle and occupants being neutralized. The fact that ESS vehicle harnesses were not used is also significant due to the large number of vehicles involved in the response plan. Data regarding the results of adversary actions against these vehicles could be critical towards validation of planned response actions.

4. Two engagements were observed in which PF personnel were using concealment for cover while being engaged by adversaries. The ESS laser will not penetrate concealment (bushes, trashcans, etc.). Several instances of poor use of cover by the PF were observed. There were no controller calls made during these instances and these actions may have impacted scenario results.

5. During the pre-exercise briefing information was presented that the adversaries would be using smoke to simulate chemical irritants. Green smoke was to be used to simulate explosions. Rules of engagement required both adversaries and the PF to don protective masks when smoke was deployed. The adversaries were not given the tactical option of using smoke as a diversion and to mask their movements. This seriously impacted adversary tactics as use of masking smoke during daylight hours would be heavily incorporated into assault and escape plans.

6. Due to the SO-1 Team not reviewing controller evaluator data collection forms, it is not known to what extent PT Plan/scenario objectives were met.

7. Several positive observations were noted during observed FOF activities:

- PT Plans reviewed were comprehensive and detailed.
- Safety briefings were comprehensive and thorough.
- An effective process was in place to ensure no live ammunition was introduced into the exercise play area.
- Effective logistics support was in place (communications [radios, batteries], participant meals, ESS equipment [issue procedures, safety, god guns], etc.).
- The PF conducted thorough roof and area checks as part of Configuration B pre-Hotel Condition requirements. (Consideration should be given as to how the PF ensures these areas are still clear and secure during extended Hotel Conditions.)
- Shadow Force response to actual alarms during an Exercise Freeze was timely.
- The FOF provided the first opportunity for the PF to train during FOF conditions with their protective masks.

The cost of conducting a FOF in terms of funding, personnel, equipment, etc., is significant. As always, conducting a FOF and utilization of a Shadow Force increases identified risks. In order to gain the most valid information in the most cost effective manner it is prudent to develop, train, test, and then implement new protection measures, strategies, and responses; rather than develop, test, and then train.

In conclusion, the FOF activities as conducted and evaluated, provided limited information regarding validation and assurance of system(s) performance; therefore, the FOF did not fully meet DOE directives requirements for performance testing of planned protection measures. The FOF did; however, provide the PF a valuable and critically needed opportunity to train in planned Configuration B.

Appendix D:

Memo from Peter D. H. Stockton, DOE Special Assistant to:
Secretary of Energy Bill Richardson

October 30, 2000

October 30, 2000

To: Bill Richardson, Secretary of Energy

From: Peter D. H. Stockton

Subject: Classified Cyber Security Still at Risk

Recently, at General Habiger's request, I reviewed the status of DOE cyber security with the help of a number of experts. After analyzing threat documents and talking to about 30 people at DOE, NRO, DOD and the CIA, the weapons complex has done virtually nothing effective to protect against the "insider" on the classified side since the Wen Ho Lee flap of over a year ago. It is almost as easy today for a trusted insider to put weapons design information on a tape or disk and walk out the door with it as it was a year ago.

One of the keys to security when you have limited resources is to prioritize – protect your most sensitive assets, weapons design information, etc. The Los Alamos hard drives are a perfect example. Field sites are not effectively doing this in either physical or cyber security.

The major threat to the compromise of critical information at DOE is the "insider" – trusted employees. Virtually all of our known spies have been "insiders" with the highest security clearances. I have recently reviewed many of the interagency threat documents – all coming to the same conclusion – the "insider" is the priority problem. Intelligence agencies believe that the outsider threat is exaggerated. Everyone in the weapons complex is aware of this – but don't do a damn thing about it. In the face of this threat, it is unthinkable that 26 people had unfettered access to the hard drives, and 53 others had loose, escorted access.

Defense Programs' Information Security Management (ISecM) effort was a cover-your-ass scam developed by the national laboratories– give us $1.3 billion to implement the system or we do nothing. They didn't get their $1.3 billion, and they have done virtually nothing effective. A number of experts believe that there are ways of protecting priority information to the 80-90% confidence level with very little money – but it just doesn't happen. University of California simply refuses to prioritize what should be protected in the labs because they are more concerned about convenience for the scientists rather than security. Defense Programs (NNSA) lets them get away with it in the name of "functionality" and morale. (As an aside, functionality and security diametrically oppose eachother – complete functionality results in zero security and total security results in zero functionality. The balance is risk acceptance. Our national labs have tilted this scale too far in favor of functionality.)

General Habiger, John Gilligan and I had several meetings where we agreed upon a common sense strategy to immediately upgrade the classified side. At one of the meetings I had someone from the DOE Computer Forensics Lab demonstrate a device that looks like my kid's Gameboy. It can copy the equivalent of 1100 floppy discs off a computer in 3 minutes and 14 seconds.

There is also a device called a memory stick about the size of a stick of gum that can hold the equivalent of 44 floppy disks. Virtually the only way to stop this technology is the use of "media-less" computing. This seems to make it clear that to stop an "insider" you have to stop any media (disks, tapes, laptops, etc) from coming in or out of priority classified areas. On August 30-31 we held a meeting at Livermore with Gilligan and Bill Hunteman of NNSA, the CIOs of the key facilities and the feds from the operations offices. Virtually everyone agreed that we had to move ahead quickly on the "insider" problem before the Hill or the press found out that virtually nothing effective has been done to stop a dedicated insider. I assume the consequences for the Department would not be pleasant if this was the subject of a Congressional hearing.

The implementation strategy established on the first day of the August meeting at Livermore for near-term enhanced security for classified systems included the following:

- Identify the most sensitive/high-risk information types, i.e. bomb design information including Sigma 14 & 15, etc. that should be protected immediately;
- Reduce the number of classified systems and system administrators;
- Enforce more rigorous authorization and validation of need-to-know implementation;
- Implement "media-less" computing systems;
- Prohibit media going in or out of high priority areas (except under strict two-man rule);
- Use encryption for certain files.

As planned, most of these efforts were expected to have been completed by now. However, based on John Todd's (the new security czar of NNSA) objections, the near-term strategy that was developed by the top cyber-security people from the labs, the other weapons facilities and the senior feds has been shelved.

On the second day, General Habiger and John Todd were briefed on what had been agreed upon. Habiger was totally on board with this approach. However, toward the end of the meeting Todd argued that this effort should be delayed because it may have a negative impact on lab morale. Todd's solution was to install lock boxes like those he was implementing at Naval Reactors. He admitted that the lock boxes were not effective against a dedicated insider, and they would not increase security, but they would increase functionality for the scientists – they could leave their computers on when they left their offices. I visited Naval Reactors and met with their security officials to discuss their experience with lock boxes. They admitted that they would not be effective against the dedicated insider, and that they had obvious vulnerabilities. In addition to these lock boxes, NNSA is planning to use their $20 million supplemental to plan for another version of the vaunted $1.3 billion ISecM. The new program, ICSI, creates an enterprise-wide "secure" network that relies upon new, unproven technologies, such as computerized need-to-know engines and one-way diodes. This is again based on the wants of the scientists rather than the real security needs of the system.

RECOMMENDATION

YOU SHOULD TASK GENERAL GORDON AND THE OTHER LPSOs TO ADDRESS THIS ISSUE IMMEDIATELY AS HIS HIGHEST PRIORITY.

Appendix E:

Partial transcript of speech by General Eugene Habiger at the 41st Annual Meeting of the Institute of Nuclear Material Management

Tape 1 of 2

Let's take our seats and maybe we can get this session started. Some of our speakers have a rather tight schedule. I urge you to come as close to the front as you can. I'm Jim Langley. I'm the Chair of the Government Industry Liaison Committee which is one of the standing committees of the Institute. One of the committee's primary duties is to organize what has now become the closing plenary session for two years now. This is the second year that the Government Industry Liaison Committee session has actually been the closing plenary session. In years prior to that of course we had the session that always met on the day following the close of the annual meeting. I would like to read briefly our committee members and acknowledge the help they have given us in arranging the program. Bob Barrens, Jerry Oskowaga, John Modder, Bruce Moran, Vince DeVito, Bran Smith, Peter O'Kwan, Megan Watt, Anita Nilson, Mike White, Toru Haginawa, and the vice chair is Amy Whitworth at the podium, and not all of our members are present at the meeting of course but we do a lot of this business by e-mail. We have two speakers this afternoon who I will introduce. They have some tight schedules, so I think we'll have to take some direct questions to each immediately following this presentation and I'm not going to have a break between the two speakers in hope that we can have a good, fast-moving session and not be interrupted by breaks. Both speakers have agreed to take questions and like I said, we will do this immediately following each of their presentations.

The first speaker is Gen. Eugene E. Habbiger, US Air Force Retired. He is the Department of Energy's Director of Security and Emergency Operations. As the Department's security officer he is responsible for implementing the Secretary of Energy's security reform plan and oversees all security functions including safeguards and security policy, security critical infrastructure protection, foreign visits and assignments and emergency operations. He is charged by the Secretary with changing the security culture at the Department of Energy and establishing a program to re-energize and restore confidence in the Department's security program. Gen. Habbiger has over 35 years of experience in national security and nuclear operations. In his last assignment as the Commander in Chief of the United States Strategic Command he was responsible for all US Air Force and US Navy strategic nuclear forces supporting the national security objective of strategic deterrents. The General began his career by enlisting in the Army, he went on to complete Air Force Officer Training School in September 1993 as a distinguished graduate. He was a command pilot with more than 5000 flying hours, primarily in bombers. During the Vietnam war he flew 150 combat missions. It is my pleasure to present Gen. Gene Habbiger and the title of his talk is "Security and International Collaboration—a Proper Balance." General Habbiger.

Thank you very much for that warm introduction and warm welcome here at the 41st Annual Meeting of the Institute of Nuclear Materials Management. I didn't even know you existed until you invited me. You need to get some more publicity out there. You're a low-key organization. You report you have lost some secret documents and you get the visibility you need perhaps, huh? I see you are a rather sleepy group perhaps, and I need to wake you up a little bit. Well I appreciate the opportunity to talk to you. Obviously, I've done a lot of thinking about security over the course of 35 years military and this past year as the Security Czar of the Department of

it be for us to remain back up to three warheads per missile? So [Colin Gen. Surgeev and this] nuclear weapons storage area, I had an actual re-entry vehicle, a nuclear weapon, on top of the third stage of a minuteman-III. I didn't ask anybody. I just did it, because he said he really needed to be able to explain this to his politicians back home. So I took him in. Oh by the way, as a four star when I went into my nuclear weapons storage facilities, they had streamlined procedures because it's a very labor-intensive, time-consuming process and as I was going to take Gen. Surgehev into this site, the Security people the week before had said, "OK boss, streamline procedures? Wrong." But it's cold, it's February. Take the entire time. I wanted him to see how stringent our security requirements were. Anyway, I took him in, showed him the new bulk head, showed him the warhead and he said, "Gene, that was invaluable. Thank you." That opened up a line of trust and confidence building that led to me going over to Russia six months later and I was the first American ever to be taken into a Russian nuclear weapons facility—ever. When the inspectors go to Russian facilities and when Russian inspectors come to our facilities, we tend to play games with each other. We cover things with cloth shrouds so you can make out the outline that something's there, but you can't see it. When I went to Kostroma, the Urel mobile ICBM base, and they walked me through every car on this train—every car. The power generation car, the security car, the control car, and then they showed me the car where the actual missile itself with its ten warheads was located. And I said, "What do you show our inspectors when the come? Do you show them this same thing?" "Oh no, no, no." "What do you show them?" The general said, "Let me demonstrate for you." So they shut off all the lights in the car and a Russian got at the other end of the car and I stood at the other end and he turned on his flashlight and he said, "This is what we show the American inspectors when they come, because we play games with each other." One message I have for you in the arenas that you deal in, "Don't play games." Be up front, be forthright, begin to develop confidence building. The

reason I bring this up in little vignettes that I've just given you is that I found surprising similarities between how the Russians deal with their personnel who are associated with nuclear weapons and technical data that are very, very similar to ours. We have something called the Personnel Reliability Program in the US whether you are talking about the DOD or the DOE and you have to be up to a very high level of psychological stability, medical stability, not have any alcohol problems, drug problems of any kind. It was interesting to find out that the Russians have a very similar program. As a matter of fact, in some cases the Russians are more stringent in the control of personnel dealing with nuclear matters and nuclear materials and nuclear weapons. For example, when their missile crew members go on alert duty and their guards go on alert duty, they are given an examination by a medical doctor and a psychologist. Now it's not an extensive evaluation, but they make sure somebody's home and that the individual is alert, looks good, smells good, acts good. We don't do that in this country. The Russians have a three-person policy when they deal with nuclear weapons. We have a two-person policy. The Russians have gotten a lot of bad wraps over the past several years about their nuclear weapons security, but I will tell you from what I've seen, and I've seen quite a bit, that they take this very, very seriously. As a matter of fact, the biggest difference I saw is that in Russia they are not into technology yet. They are very much manpower intensive. We learned after Vietnam and we went to the all-volunteer force with no draftees that manpower is very expensive so we went to technology to eliminate manpower. In Russia manpower is still relatively inexpensive so they haven't gone to technology. My counterpart and I agreed that we would exchange security experts. My intent was to show them how we've applied technology. Interestingly enough, after one of their teams came and visited a few of my bases and looked at our security systems, I visited with Gen Volenkin who is on the general's staff who is responsible for the Russian nuclear weapons as long as they are in military units. We were talking and jousting back and forth and we were at one of his naval facilities. I was harassing him a little bit about the condition of the fence going down a shear cliff and he wasn't in a terribly good mood and he said half jokingly, "Well you can harass me about the fence, but my security people tell me that they saw contractors inside your nuclear weapons storage areas cutting grass. Well we do that under armed guards." My counter to him is that you in Russia are not as much into grass cutting as we are in the United States. He didn't take that too well. The point is they take this business very seriously.

Well let's get to the basic thrust. In the Department of Energy we do things across the spectrum of diversity that even surprises me. From science to some of the most sensitive nuclear weapons materials work that anyone can conceive of. We have 116,000 employees in the Department of Energy and what I'm about to tell you most people haven't thought about before, but of those 116,000 people, almost 90,000 of them are contractors. Of the 116,000 only 14,000 are federal employees. That presents some interesting problems associated with ownership and accountability. Not problems that are insurmountable but problems that cause us a special challenge. But this is nothing new for us. As a matter of fact if you go back to our Manhattan Project days in the late 1940s, international collaboration was critical in the development of our weapons program. Neils Boor (Denmark), Edward Teller (Hungary), Enrico Fermi, Emilio Serge (Italy), Hans Beta (Germany). International collaboration goes on even more today. One of the things that I've learned in this job is that while we take great credit in our national laboratories, our laboratories conduct less than 2% of the world's research and development. So over 98% of

the world's research and development in these scientific areas is conducted in laboratories other than those here in the U.S. That is a big deal. That requires scientists to be able to talk to each other, to communicate with each other. I've also learned that scientists are a different breed. They like to talk. They like to talk a lot. They like to communicate. They like to pass things back and forth. And another thing I've found it that one size doesn't fit all. What's good for Los Alamos is not necessarily good for Stanford or for Cal-Berkeley. And that's been a hard lesson for me to learn, but I think we've made great progress to accommodate our scientific brethren to ensure that we understand the difference between guns and guards and gates and mass spectrometrics. Badges, a very emotional issue in the Department of Energy. And initially my thought was to issue everyone at all of our laboratories whether they're doing classified work or unclassified work and as a czar I can do this, mandate that everybody wear a badge. Wrong answer. Wrong answer because one size doesn't fit all. So we accommodated the scientists for good reason. At Cal-Berkeley and Stanford a badge will be worn, but it will only be worn areas in which there is no classified information that is processed at those two facilities as examples. In certain areas around accelerometers where there are safety issues and those kinds of things, a badge will be worn. And the other issue had to do with foreign nationals who work in these facilities. At our nuclear laboratories or laboratories who do classified work, we require foreign nationals to have a red badge with the name of their country printed at the bottom of the badge. Very, very emotional. Especially from our friends at Brookhaven who didn't like that idea at all. But we were able to accommodate that because such a small percentage of the work done at Brookhaven was classified we put all the classified work areas, we combined them into just a few geographical areas and we were able to accommodate the concerns of the scientists. These concerns are real, but there's got to be a balance. A very, very special balance. And I think we have gone to great lengths to ensure that we are not neutrally exclusive.

I talked about badges. Some things we have control over, some things we don't. One of the things we don't have much control over right now is foreign visitors from our so-called sensitive countries. As they visit our three nuclear weapons laboratories (Los Alamos, Sandia, and Lawrence Livermore). Congress passed the law that imposed the moratorium on visitors from these countries until such time as the CIA and the FBI certified that our program was satisfactory. The legislation was so severe that every visitor from those 25 or so sensitive countries has to be personally approved by the Secretary of Energy. The Secretary of Energy continues today to personally certify individuals from those sensitive countries and I think that is a superb example of the accommodation we've made for our foreign scientists to come visit our facilities.

Polygraphs. Very emotional issues with scientists, but something we must do. We have polygraphed over 800 people this year so far and we will polygraph more. A lot of people get so emotional that it surprises even me. And my response to these emotional outcries goes something like this. Now let me get this straight. You work on some of the most sensitive programs in the US and we're going to ask you to take a test in which you are going to be asked four questions: 1) Have you ever given secrets away to a foreign national? That's the one I had trouble with until I explained to my polygrapher what I had done--and this is part of the process. He said the first question is going to be... and I said, "Time out. I've got to talk to you about that." He said, "What do you mean?" I explained to him what I did with the Russian coming to my facility and seeing a nuclear warhead. That's a secret. We walked it through and he said,

(I've got a little bit of electronics on me that some of you with some physics on you and some of you with the right kind of workshop) if we had the special nuclear materials, we could build an improvised nuclear device very, very quickly. Once you release or that information is compromised, you never get it back. That's why our security requirements will remain rather severe, in my view, forever.

In the Department of Energy we have over 400 metric tons of plutonium and highly enriched uranium that we protect. We spend about $500 million a year protecting that material. That's a lot of money. We also have to protect the technical data. There are two threats. No. 1, the external threat. The terrorists trying to get the special nuclear material. I feel more comfortable, more confident in our capability to deal with that threat than any other. Because we have painted the terrorists at about 13 feet in height. We're defending against that terrorist who is about 13 feet in height. Now in reality he's not going to be 13 feet tall, he's going to be about 6'1" or 6'2", but we're protecting to a very high level.

The other external threat that I'm very, very concerned about are the hackers of the world. Ladies and gentlemen I cannot emphasize enough the disparity between the offensive capability of the hacker and the defensive capability that we have to protect the information on our sites. In the Department of Energy we have three levels of data. We have white databases which are totally unclassified. The kind of stuff they do at Thomas Jefferson in Newport News, VA and Stanford and Cal-Berkeley and we have yellow systems that include personal data (Social Security Nos), sensitive but unclassified information, and then we have red data which is the truly classified material. I'm confident to a very, very high degree in our ability to keep safe our red networks but there are sophisticated tools that we are beginning to see that put at risk our yellow systems. I would submit that we really need to start putting money into advanced defensive kinds of things. I'm not talking about firewalls. I'm talking about things beyond

Appendix F:

"Declassification of United States Total Production of Weapon-Grade Plutonium," DOE Facts

December 7, 1993

DOE FACTS

DECLASSIFICATION OF UNITED STATES TOTAL PRODUCTION OF WEAPON-GRADE PLUTONIUM

The Department of Energy has declassified the total United States production of weapon-grade plutonium.

SPECIFICALLY:

- **The United States produced 89 metric tons of weapon-grade plutonium.**
  - The Savannah River Site near Aiken, South Carolina, produced 36 metric tons of weapon-grade plutonium from 1953 through 1988.
  - The Hanford site near Richland, Washington, produced 53 metric tons of weapon-grade plutonium from 1945 through 1987.
- The Hanford site also produced 13 metric tons of reactor-grade plutonium and 13 kilograms of tritium.

BACKGROUND:

- The plutonium was produced to support the United States nuclear weapons program from 1945 through 1988.
- There have been requests for this information for health and safety calculations for independent studies to determine public radiation dosages.
- The Congressional Office of Technology Assessment has also suggested the release of this information.

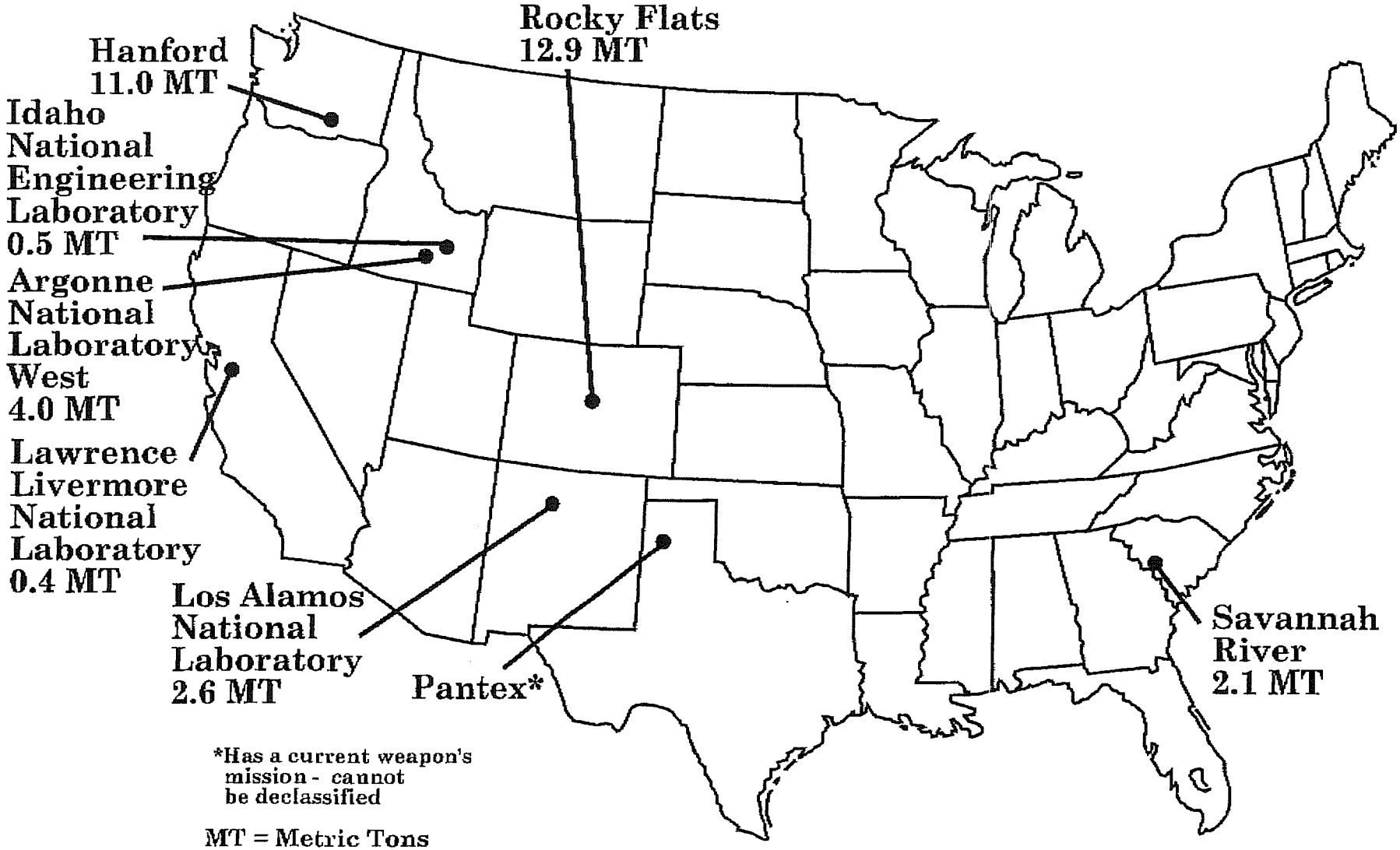
BENEFITS:

- As part of the Secretary's Openness Initiative, the Department is declassifying the information concerning the total United States plutonium production. As a result of this declassification, the public will have information that is important to the current debate over proper management and ultimate disposition of plutonium.

(MORE)

U.S. Department of Energy
Office of Public Affairs
Contact: Sam Grizzle
(202) 586-5806

December 7, 1993 Announcements
Plutonium Inventories



*Has a current weapon's mission - cannot be declassified

MT = Metric Tons

Total = 33.5 MT

Appendix G:

"Design Basis Threat for Department of Energy Programs and Facilities (Unclassified),"
U.S. Department of Energy Office of Safeguards and Security

December 1998

FYI

Design Basis Threat
for
Department of Energy
Programs and Facilities
(Unclassified)

Short Title:
Unclassified Design Basis Threat

U.S. Department of Energy
Office of Safeguards and Security
December 1998

Design Basis Threat for Department of Energy Programs and Facilities

(Unclassified)

Short Title: Unclassified Design Basis Threat

1. INTRODUCTION. This statement identifies and characterizes potential adversary threats to Department of Energy (DOE) programs and facilities. DOE interests shall be protected against activities which include unauthorized access; theft, diversion or loss of control of nuclear weapons, weapons components, special nuclear material, associated technologies and hardware and critical technologies; sabotage; espionage; loss or theft of classified matter or Government property; and other acts which may cause unacceptable adverse impacts on national security, the health and safety of employees, the public, or the environment.

   In view of continuing changes in the international geopolitical environment, special emphasis should not only be placed on protection of DOE classified, and sensitive, but unclassified information and material having economic, technology transfer, and/or nuclear proliferation implications, as well as U.S. business proprietary, confidential or sensitive unclassified information.

   The Design Basis Threat shall be used to:

   - Develop Safeguards and Security Program and requirements;
   - Provide a basis for site safeguards and security program planning, implementation and facility design;
   - Provide a basis for evaluation of implemented systems;
   - Support Counterintelligence Program and requirements;
   - Provide a basis for evaluation of Counterintelligence risks posed to DOE interests.

2. LOCAL THREAT DEVELOPMENT. This statement describes a baseline Departmental threat spectrum. In the development of this threat, site-specific geographical, environmental, or other unique facility or location characteristics were not considered. Local threat statements should be developed to take into account site-specific and region-specific threat considerations to supplement the Departmental Design Basis Threat.

3. THREAT TYPES. Adversary groups addressed herein include: terrorists, criminals (white collar and organized), psychotics, disgruntled employees, violent activists, and intelligence collectors. The descriptive characteristics of a particular group may include attributes that are common to some or all other types, as well as characteristics unique to that group. The following threat types and characteristics shall be considered in safeguards and security and counterintelligence program planning, implementation, and evaluation.

A. TERRORISTS.

(1) Definition. Persons or groups who unlawfully use force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

(2) A small group (including an insider).

(3) Characteristics.
- Capable of lethal and violent action; willing to kill and be killed.
- Capable of conducting coordinated paramilitary operations.
- Possess a wide range of military equipment, weapons and ordnance.
- Access to funds, communications, transportation and safehouses.

(4) Explanatory Notes.

a. Terrorist Targeting. Facilities considered to be targets of terrorist activity are those that:
- Receive, use, process, or store Category I and credible roll up quantities of Category II special nuclear material;
- Manufacture, store, or test nuclear weapons, nuclear test devices, or completed nuclear assemblies; or
- Contain materials which might be targets of radiological and/or toxicological sabotage.

b. Explosives: Man-portable, mailed and vehicle transported explosives may be used in targeting DOE facilities.

B. CRIMINALS: WHITE-COLLAR.

(1) Definition. An individual who seeks classified and/or sensitive unclassified, information or material for the purpose of gaining economic advantage, or attempts to alter data maintained by DOE, or attempts to steal or embezzle government funds or commit contract fraud for the purpose of economic advantage to the individual or the individual's employer.

(2) Size. Normally a single individual (may be an insider).

(3) Characteristics.
- Unarmed and non-violent.
- Willing to destroy (render usable) information and equipment

- Knowledge of current business practices to include budget and accounting systems.
- Maintains anonymity.

C. CRIMINALS: ORGANIZED.

(1) Definition. Persons who conspire to, and/or perpetrate criminal acts against DOE or DOE contractors for profit or economic gain.

(2) Size. A small group (including an insider).

(3) Characteristics.
- Possess conventional weapons.
- May possess commercial or improvised explosives.
- Rely on ruse and deceit.
- Highly motivated for financial gain.
- Not willing to sacrifice own life.

D. PSYCHOTIC.

(1) Definition. A person suffering from a mental disorder who experiences periodic or prolonged loss of contact with reality.

(2) Size. An employee, former employee or other person with a real or perceived grievance against the Department acting alone.

(3) Characteristics.
- May possess commonly available weapons.
- Possess or able to obtain commercial explosives.
- May possess technical training and expertise.
- Willing to lay down own life.

E. DISGRUNTLED EMPLOYEE.

(1) Definition. An individual who engages in vindictive, violent, or malicious acts at or directed against the place of employment

(2) Size. One employee acting alone.

(3) Characteristics.
- May possess commonly available weapons and commercial explosives.

- Motivated by work related grievances.
- Normally committing low risk crimes.
- May possess technical training and expertise.
- Current access to security areas and knowledge of security procedures.

F. VIOLENT ACTIVISTS.

(2) Definition. A group or individual who commits violent acts out of opposition to Departmental programs for ecological, political, economic, or other reasons.

(3) Size. An individual or a core of up to five people (may include an insider).

(3) Characteristics
- Possess conventional firearms and explosives.
- Highly motivated.
- Tactics include demonstrations, facility seizure, sabotage and theft.
- May infiltrate legitimate, peaceful opposition groups.

Explanatory Note. This category does not include lobbyists, pressure groups, nonviolent demonstrators, and others opposed to the development and use of nuclear energy, nuclear weapons, or other Departmental or Federal programs and who engage in lawful actions to bring about a cessation of these activities.

G. INTELLIGENCE COLLECTORS.

(1) Definition. For the purposes of this design basis threat there are two types of intelligence collectors: agents of foreign intelligence services and foreign researchers and other visitors/assignees. An agent of a foreign intelligence service is an individual (most likely a DOE employee) who has been recruited or volunteered to serve a foreign government as a spy. This individual uses human intelligence methods and engages in clandestine intelligence gathering on behalf of, or at the direction of a foreign intelligence service. - A foreign researcher and other visitor/assignee is a person (or persons) working for a foreign business entity, university, government agency or intelligence service, who collects classified, sensitive unclassified, proprietary, economic or scientific information through the use of personal and/or professional contacts, visits and/or assignments to DOE facilities, conferences, symposia or in connection with official state visits or arms control treaty inspections.

(2) Size. One or more individuals

(3)Characteristics.

- Utilize HUMINT, SIGINT, IMINT and Open Source techniques.
- Considerable financial and technical support.
- Exploits employee vulnerabilities and weaknesses.
- Exploits unclassified and classified management information systems.
- Encourages exchange of scientific information.

4. INSIDER CONSIDERATIONS.

A. General. An insider is anyone with authorized, unescorted access to DOE facilities and programs. Any of the adversaries identified in paragraph 3 could be insiders. An insider could be violent, use physical force, actively support outsiders by directly participating in the act, and/or passively support outsiders by simply supplying information. Emphasis must be placed on addressing the most probable insider threat; i.e., the single employee. However, the potential for multiple insider threats must also be considered in site safeguards and security planning.

B. Human Reliability Programs. The insider actions described above, whether or not in concert with external groups, shall always form a basic consideration in safeguards and security countermeasures planning and system evaluation. In the absence of effective and approved human reliability programs, for planning, analysis, and evaluation purposes, the insider shall be considered to be active and violent. Where a Departmentally approved human reliability program is fully implemented, and when it is combined with other elements of a multi-faceted insider threat mitigation program (e.g., personnel security, materials control, material accountability, administrative procedures, employee assistance programs, and/or mental health programs, etc.), the insider may be considered to be passive and non-violent.

C. Mitigation. To mitigate potential insider acts from active to passive, a human reliability program shall minimally consist of the following elements:

- A security determination (clearance or access authorization);
- Initial and random substance abuse testing;
- Initial and periodic medical assessment to include psychological evaluations; and
- Supervisory review at least annually.

5. SAFEGUARDS AND SECURITY PROGRAM STRATEGY.

Protection program strategies are identified in DOE 5632. IC, PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS, and DOE 5632. 1C- 1, MANUAL FOR THE PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS, each of 7-15-94. The appropriate strategy to be implemented shall reflect consideration of the Design Basis Threat and local threats, the graded protection concept, the assets being protected, the potential damage to national security, the health and safety of DOE and contractor employees, the public, and the environment.

Security System Performance. Safeguards and Security systems and critical system elements shall be performance tested to ascertain their effectiveness in providing countermeasures to address design basis threats. In addition confidence level tests should be conducted above the baseline to to help identify security weaknesses and help sites determine whether incremental increases in adversary capabilities would result in catastrophic safeguards and security system failure.

6. ASSISTANCE. Questions concerning this Design Basis Threat should be directed to the Program Manager, Protection Program Operations, telephone 301-903-5693

Appendix H:

Memo from Joseph S. Mahaley Director Office of Security Affairs to:
Acting Deputy Secretary

February 9, 1999

With attachments

Department of Energy

Washington, DC 20585
February 9, 1999

MEMORANDUM FOR ACTING DEPUTY SECRETARY

THROUGH: ROSE GOTTEMOELLER
DIRECTOR
OFFICE OF NONPROLIFERATION AND
NATIONAL SECURITY

FROM: JOSEPH S. MAHALEY
DIRECTOR
OFFICE OF SECURITY AFFAIRS

SUBJECT: Comments Regarding the Hagengruber Draft Phase One Report.

The overriding fault with Hagengruber's Draft Phase One Report is that it was expected to be technical security review offering expert technical opinions on very challenging specific security problems facing the DOE. It is not, and in that respect it is a failure.

The following paragraphs offer additional specific comments.

First, rather than focusing on the key issues that had been raised during the development of site specific safeguards and security plans, as Hagengruber himself proposed in his December 18, 1997 "Security Review Team Proposed Process Outline,"[1] the report repeatedly reassures some unidentified audience that the state of security is very high in DOE facilities (see pages 1,3,8) while carrying out a deliberate and continuous attack on the Office of Safeguards and Security (OSS). In his attack, Hagengruber cites Inspector General and field office comments to buttress his own comments to the effect that OSS has imposed unjustified security requirements, almost by whim, on the DOE field activities. To me, this is perhaps the most disingenuous and profoundly disturbing facet of Hagengruber's report. This is because I personally know that Hagengruber himself is aware that the OSS, acting at my direction, seeks to establish these so-called unjustified policy requirements on field activities for explicit reasons that are inextricably intertwined with highly classified DOE programs that most Program Secretarial Officers, field office managers, the Office of Security Evaluations (OSE), and the Inspector General have not been afforded access

---

[1] The Background section of the December 12, 1997 Outline stated at page 3 that the Hagengruber team was to "...address and resolve key issues that have been raised during the development and review of site specific safeguards and security plans . The team will focus on the overall security system performance as opposed to assessing compliance to the design basis threat alone. Some effort will also be put on examining the computer models currently being used to develop requirements, the basis for modeling assumptions regarding risks, the need for expanded performance tests, and the options for the use of technology to enhance and control costs."

to. However, Hagengruber has access to and knowledge of these programs, which was why my Office and OSS supported him being tasked to undertake this effort when his name was suggested to then Deputy Secretary Moler by Assistant Secretary for Defense Programs Reis in 1997. Indeed, I have met and discussed these issues several times with Hagengruber over the past year. He has never stated during any of our meetings that the requirements that OSS, and my Office, seeks to implement that are based on these highly classified issues are unjustified. In this respect, his report is a misrepresentation and distortion of the true situation, of which he has direct personal knowledge.

Second, Hagengruber appears to have used his technical review assignment to assume a security ombudsman role to gather what amounts to a series of complaints from the field about security management roles and responsibilities. Again, it must be noted that this was not his assignment, as he himself described it in his December 18, 1997 "Security Review Team Proposed Process Outline." Indeed, had such a task been openly proposed as part of his assignment, I would have strongly objected to it, because of the obvious conflict of interest between his reviewing DOE management roles and responsibilities and his position as a senior corporate officer of a current DOE contractor. Moreover, the comments he gathered in his meetings with Federal employees and contractors relating to their complaints over the current fragmented security management system at DOE and the problems associated with that system have been raised before in many other prior reviews that were intended to address DOE security management as a principle objective.

Third, the report calls for DOE headquarters entities to refrain from so-called micro-management of field activities, and even recommends that the primary DOE offices responsible for security policy play no role in concurring on site safeguards and security plans. This logically inconsistent approach reaches its nadir in the report's recommendations, where it it states that my Office, NN-50, "...should establish policy, issue guidelines, rules and procedures...for safeguards and security... " but should "...curtail efforts that have the effect of managing or directing field operations." The report is silent on how such magic is to be performed, absent a dedicated effort by my Office and its components to issue policy and procedures that are irrelevant to DOE field activities, i.e., formulate totally useless security policies, guidelines, rules and procedures. I believe that this proposal to deny NN-50 any further meaningful role or responsibility for actual DOE security management is merely the first step in a plan to hamstring and ultimately eliminate a DOE Headquarters entity that has caused problems for DOE contractors by highlighting security deficiencies. In my opinion, the report's call to let the field handle it, including the proposal to treat all security costs as indirect costs, is merely a call to return to the AEC, ERDA and early DOE practice of letting the field activities run the Department, which, in 1999, is simply a bankrupt concept. That past practice left DOE huge problems of environmental cleanup, out-of-control contract costs that were virtually unrecoverable by the Government, major information security problems (the dimensions of which are still being investigated to this day) and tremendous waste as site contractors and lab directors did pretty well whatever their field office "barons" let them do. Whatever this Department does to effect improved management of its

security mission,[2] it should not reestablish the old regime of field autonomy that some "grizzled veterans" clearly desire. They were not the good old days for the U.S. Government or for the American people.

Fourth, assuming arguendo that the Hagengruber special security review was actually undertaken with the primary objective of analyzing DOE security management roles and missions, it is a patently defective attempt at such an analysis. The most glaring fault is that while there is much criticism of OSS and other Headquarters entities actions, no attempt is made to analyze those actions against the current roles and responsibilities assigned to those entities by currently effective Departmental Orders, Regulations and other binding management direction issued by or on behalf of the Secretary of Energy. This complete omission in the report is stunning, particularly in light of its unequivocal characterization of OSS and other entities actions or requirements as improper or unjustified. For example, there is no mention in the Report of DOE Order 470.1, the Department's primary Safeguards and Security Program directive. That Order is the basic reference for current Headquarters and field activities safeguards and security roles and responsibilities. There is no indication, however, that any member of the Hagengruber team performed any scholarly review of this very relevant reference as part of their unchartered review of security management roles and responsibilities. Indeed, as I reviewed this draft work done by a U.S. National Laboratory, I was shocked to discover there are no references provided with the report. Does this mean that this special review, conducted at a cost of one and a half million dollars and lasting over a year, bases its conclusions and recommendations solely on its team members personal observations, opinions and recollections of the conversations they had with unnamed personnel they talked with during these visits? Were no administrative or technical references used at any time in the year-long effort? If they were used, why are they not identified for the reader? If the purported analysis of roles and responsibilities was performed utilizing any framework of the existing roles and responsibilities currently incumbent upon DOE organizational components, there is no evidence of that in the draft report. If the critical comments regarding the actions of OSS and other Headquarters entities in the report were developed without any reference to the existing DOE roles and responsibilities of OSS and the other entities, they are a grossly unfair analysis and represent nothing more than unsupported opinions of review team members or other unnamed persons about the way the Department ought to be run.

Finally, I would be remiss if I failed to also note that the Hagengruber report reflects a similarly unsupported critical evaluation of the current DOE Design Basis Threat (DBT). There is, for example, no evidence in the report or the appendices that any member of the Hagengruber team has reviewed the 1997 Nuclear Command and Control System Staff review of the DOE DBT or its Department of Defense equivalent. In addition, I am informed no member of Hagengruber's team attended or participated in the meetings of the interagency Nuclear Security Steering Group, which reviews and updates the DBT, even though the Group met while the review was being

---

[2] I strongly disagree with the report's assertion that security is not a mission of the Department. Security has been a primary mission of the Department and its predecessor agencies since their inception, as is made clear in the Atomic Energy Act.

conducted. I am also informed there was no attempt to interview Group members at some other time during the year-long review. I have no doubt that the DBT and how we use it can be improved, but I was dismayed to discover that the report's review of the DBT, which I always considered to be a prime part of Hagengruber's task, was apparently not based on any serious research and resulted in what I believe to be inaccurate criticism and superficial treatment.

In conclusion, I am so profoundly disappointed in the Hagengruber Draft Phase One Report that I recommend that no further Nuclear Safeguards and Security funding be authorized for this effort. I further recommend that any planning efforts for follow-on phases be terminated. In addition, I respectfully request that a review of this effort be conducted to identify lessons learned so that we may avoid any similar failures in the future.

I have attached to my comments those of the Director, Office of Safeguards and Security, and the detailed review comments developed by the OSS staff.

Attachment

Department of Energy
Germantown, MD 20874-1290

February 3, 1999

MEMORANDUM FOR JOSEPH S. MAHALEY, DIRECTOR
OFFICE OF SECURITY AFFAIRS

FROM: EDWARD J. MCCALLUM, DIRECTOR
OFFICE OF SAFEGUARDS AND SECURITY

SUBJECT: HAGENGRUBER STUDY

I have completed my initial review of the subject document and offer the following impressions. These thoughts are not intended to be all inclusive; nor do they address all of the facts that I find questionable. In this regard, I have directed the Office of Safeguards and Security (OSS) Program staff to conduct a thorough review of the entire report with respect to its factual accuracy. Upon completion of this review, detailed comments regarding factual inaccuracies will be forwarded. Beyond the factual accuracy of some of the items found in the report, however, it is evident that this study not only misses the mark of the task assigned, but if left unchallenged could serve to damage the Department's standing in the security and intelligence community at large.

In reading the report, I am struck by the elementary understanding it portrays of the Safeguards and Security (S&S) Program; specifically as it relates to the national level directives that provide much of the foundation for many of the areas called into question. There is no mention of the Presidential Decision Directives (PDD) or the requirements contained therein governing federal agencies and their policies toward counterterrorism, explosives detection, radiological sabotage, and chemical/biological weapons defense. In fact the assertions offered are in direct contradiction to President Clinton's policy on Counterterrorism promulgated in PDD-39. For a study that spent the better part of a year examining the Department's S&S Program, I find this glaring omission of national policies to be alarming. Furthermore, it conveys a lack of understanding of the environment in which the Department operates that consequently diminishes the value of any findings or recommendations.

Beyond the lack of depth of understanding of S&S Program requirements, however, I find the team failed to answer the only question that was posed to them. Specifically, whether current DOE practices ensure that Special Nuclear Material (SNM) and Nuclear Weapons are adequately protected against Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) threats. The short statements in the report that we need to change policies to require a higher standard of protection of SNM is gratuitous and provides no new information. The single graphic depicting greater quantities of explosives relative to SNM types was recognized long ago when the Atomic Energy Commission began this program, and again in 1988 when the graded safeguards table for SNM protection was established. I was disappointed to find that the validation of specific time lines of existing guidelines currently in the Secretary's office awaiting completion of this study were completely avoided.

Equally disappointing is the amount of effort and detail directed at the management and organizational issues that have been previously reported in numerous studies to include your Report to the Secretary of October 1997 and the OSS Annual Report to the Secretary of January 1997. That the fragmented and divisive S&S structure is difficult to manage is well acknowledged and has been addressed repeatedly by DOE through reorganization and restructuring (e.g., SAI 26). There is no new information here, and the recommendations offered are confusing and inconsistent with one another. The solution as I understand it would further decentralize authority and responsibility to field sites thereby recreating the exact same environment as existed in Counterintelligence prior to the issuance of PDD 61.

The report wades through a plethora of symptoms and offers the often repeated Laboratory rhetoric to limit Headquarters involvement and trust the contractor to carry out the government's mission. Trust is not the question, execution is. As you know, cost is an essential element of risk management. The House of Representatives, Committee on Commerce, Oversight and Investigations Subcommittee challenged the DOE on the oversight of its contractor's S&S programs throughout the 1980's and early 1990's. Senator Glenn asked the same questions in Senate, Government Affairs Committee hearings. These facts are either unknown or ignored by the report team. I have yet to hear an allegation that DOE provides too much oversight of our contractors except from the Labs. Consequently, the suggestion that S&S should be funded through a site's overhead budget is simply irresponsible. It is unclear to me how this would be the preferred method of funding. Such a move would further remove the Department's control over this critical area. It is precisely this approach to safeguards and security as an "overhead" function that has led to many of our difficulties. It further underscores the lack of understanding of the mission essential element of safeguards and security as it relates to the Department's overall mission. It is precisely this type of thinking that Admiral Crowe's January 1999 report on the embassy bombings in Nairobi and Dar Es Salaam warns against. In his cover letter to Secretary Albright he expresses concern about the "...relative low priority accorded security concerns throughout the US government - by the Department, other agencies in general, and on the part of many employees both in Washington and in the field." Admiral Crowe goes on to advise that, "Saving lives and adequately addressing our security vulnerabilities on a sustained basis must be given higher priority by all those involved if we are to prevent such tragedies in the future."

Again, this lack of understanding leads to another disturbing assertion found in the report. Specifically that: "Safeguards and security is not a mission of DOE. Rather, safeguards and security is the responsibility of the DOE and contractor management at individual sites." Such a statement is contrary to Department of Energy's Strategic Plan of September 1997. Under the Strategic Plan's National Security Strategic Goal is the objective to "ensure the vitality of DOE's national security enterprise." In support of this objective is a strategy to "ensure the protection of nuclear materials, sensitive information and facilities." The fact that safeguards and security is found in the Strategic Plan as well as in the Secretary's Performance Agreement with the President clearly raises its level of import to more than "a requirement of operation."

A final point worthy of note is the complete lack of understanding of the Department's Design Basis Threat (DBT) process. The FBI, CIA, DOE, and the military services as well as the Nuclear Command and Control Staff have developed the existing Design Basis Threat over a number of years. It has been extensively reviewed and supporting studies issued by the DIA. Sandia, as well as our other Labs, have been asked to comment and participate in the development process. To describe the process and approach as flawed further underscores the superficial nature and questionable analysis found in the report.

Perhaps most distressing is the lack of balance in its approach to the critical safeguards and security issues facing the Department. Rather, what is provided is a very parochial Defense Programs/Laboratory view that ignores not only the external drivers found in national level policies, but a total lack of understanding of specific procedures implementing these policies. Suffice to say, I am strongly opposed to the continued funding of Phases II and III of this effort. If Phase I is any indication of the quality of effort that might be expected, any further funding in this regard would be imprudent at best. Nonetheless, if the program is continued, I strongly suggest we manage the direction and quality of the next phase.

As stated in this and other studies, successful resolution of the issues facing this Department relative to safeguards and security will require a concentrated effort on the part of all interested parties to include the Office of Defense Programs and the National Laboratories. What concerns me is that critical information concerning these issues is missing from this study. While such an omission may serve certain short term interests, it is not in the best interest of the Department or the nation. As an agency, we must endorse and implement two significant objectives concerning our protection strategy: 1) to protect our nation's critical assets from those who would cause our nation harm, and, 2) to protect the forces that secure our facilities from unnecessary vulnerability. To do any less is to undermine our national security responsibility, which is without question, a core mission of this Department.

Department of Energy
Washington, DC 20585

FEB 09 1999

TO: JOSEPH S. MAHALEY, DIRECTOR
OFFICE OF SECURITY AFFAIRS

FROM: OWEN B. JOHNSON, DEPUTY DIRECTOR
OFFICE OF SAFEGUARDS AND SECURITY

SUBJECT: DRAFT SPECIAL SECURITY TEAM (HAGENBRUGER) REPORT TO THE SECRETARY

My staff and I have completed the review of the subject draft and are attaching numerous specific comments on the report content. Those comments, which are intended to correct factual errors in the Report can help somewhat make the Report of use to the Department as it attempts to determine a path forward for an improved Department overall security operation. Unfortunately, because the Report does not really address the root cause of DOE's security problems there really is no way to achieve what I understood the Secretary's goal to be in this matter by commenting on the Report. The Report simply fails to address the major elements of the security dilemma confronting the DOE, namely how it is organized to execute its security mission–and make no mistake it's unique U.S. Government responsibilities for the security of cradle to grave nuclear materials is a mission–and how it budgets to accomplish that mission.

These are the two most important components of any successful program in either the public or the private sector. How do you manage and how do you budget. Previous reports on the general subject e.g., the Freeze Report, the Shapiro Report and the Mahaley Report of 1997 to the Under Secretary have given clear recommendations which have never been acted on and which in my opinion are key to our continuing difficulties. Issues like how the Design Basis Threat (DBT) is determined and implemented, what the Site Safeguards and Security Plan (SSSP) process is, and how the policy process works etc. are important, but frankly marginal to any real solution to the historic difficulties of solving a chronic condition of uncertain funding, and fragmented dysfunctional security organization. Ironically, the only allusion the Report makes to the funding issue contains a strong endorsement for the method of funding which has been proved a failure, namely indirect funding for security costs. This is a method which guarantees failure regarding adequacy of funding because, by definition indirect costs are a part of overhead, a form of cost which is not specifically earmarked but rather is malleable to ensure some discretion in funding on a priority basis. The Hagengruber Report recognizes this fact by referencing then Deputy Secretary Curtis' "challenge" to drive down indirect costs as a way of reducing Departmental costs overall with the result that "...the robustness of your security program can be continually thinned until...inadequate," (pg.37). In short, the Report glances at a critical issue but doesn't amplify the importance of the issue and doesn't get it right in any case notwithstanding numerous

historical documents such as Freeze which gave a roadmap for systemic improvement. Because such reports were not heeded the Department continues to confront the same major impediment to security success as before.

The Freeze Report and other such reports also addressed the importance of having the Department's main security component(s) organized in such a way as to be complementary, under the management of a Secretarial direct report and funded directly with the Department's security mission. Again, the Special Review doesn't address the issue at all. (There is a one sentence statement in the Introduction section which never receives further amplification and which provides the reader no hint either of what is intended or whether there is a rationale for the statement.) What the Report does look at, the DBT, SSSP, policy process and responsibility for oversight of policy implementation are symptoms of the problems which result from failure to manage the underlying causal deficiencies.

Concluding, the Department's substantive problems in the execution of its security mission are manifested in the continuing inadequacy of its efforts to adopt recommended solutions contained in previous reports on the quality of DOE's security organizational structure. Repeated failure to address those problems over time guarantees continued inadequacy into the future. This Report does not answer the charge to assist the Department in this regard in the least. Further, the numerous factual errors which the attached comments address are also unfortunate and indicative of a writer(s) with inadequate knowledge of the subject matter about which he/they are writing, but in the end those deficiencies are not really critical to the larger issue. This Report is simply not DOE money well spent.

Attachment: As Stated

Enumerated below are specific Office of Safeguards and Security "line-by-line" comments addressing the Hagengruber Report language which this office considers in need of correction. In the interest of efficiency the comments refer to sections of the Report beginning with page one and do not repeat similar corrections necessary in the Executive Summary and the Introduction. Many of the comments we provide result from Report language errors that manifest what can only be described as misunderstanding of DOE policy or policy process. This appears to be due to inadequate discussion of the various issues with NN-51 personnel, following the initial in-briefs

Report Page 1, para 4 - "with integrated security management a higher standard of protection of SNM can be achieved with modest operational cost and impact"
Comment: See comments regarding ISM at page 3. Also, recognize that process changes alone even if they are improvements will not by themselves improve SNM protection.

Report Page 2, para. 1 - "Optimizing the DBT at every site... requires measures without consideration of ...site specific considerations" - see comments re page 11, para 2, at page 3 which indicate how this statement is factually incorrect.

Report Page 4, para. 3 - "NN should be restructured . . to focus on policy. . . "
Comment: SAI - 26 and DOE 470.1 both characterize NN-51s principal role as a policy organization. Its necessary concurrence role on SSSPs is aimed at securing DOE sites compliance with DOE policy requirements. Such a concurrence role is required because NN-51 has no authority (explicitly or implicitly) to direct field changes. A nonconcurrence can of course be ignored by the field manager. If relevant organizations each follow SAI - 26 and existing DOE Order requirements no restructuring as such should be required.

Report Page 8, para.3 - "Safeguards and Security is not a mission."
Comment: Safeguards and Security is a critical mission essential element of the Department. It is a vital part of this Department's National Security mission and is a critical part of one of the five main business lines, as specified in the mission statement of the Department's Strategic Plan and the Secretary's Performance Plan to the President for FY 1998. Pertinent Performance Plan language reads, from Commitment NS3-3, "Ensure and enhance protection of nuclear materials, sensitive information and facilities. . . "

Report Page 9, para. 5 - ". . . the cost of changes to increase standards will be sizeable"
Comment: There is no substantial supporting information for why protection standards changes (if/where necessary) need to be expensive, nor does the description of how the application of some form of integrated security management (ISM) if desirable, would affect such costs. In fact appropriate strategies may actually achieve cost reductions. This is not to say ISM for security might not be useful, simply that no cost effectiveness case is made. Any requirement for increased protection will be limited to a few locations which already provide substantial delay. It is unlikely that additional delay time needs to be a significant cost driver.

Report Pages 10-11 - Discussion of need for shift from a compliance approach to an integrated security management approach
Comment: The discussion of the rationale for a conversion to ISM seems to assume that current safeguards and security implementation is measured through a compliance method which is altogether inaccurate. (DOE moved away from compliance in the 1980s). It fails to recognize for example that a major facility protection planning element is the SSSP and its supporting vulnerability assessments (VA) neither of which is remotely compliance based. The VAs and subsequent SSSPs are expected to be the products of performance testing which is one of the numerous aspects of judging the status of security at a site through numerous performance as opposed to compliance - measures. In general, there is already very little assessment of security by either headquarters or fie'd personnel that would be characterized as compliance based. This brings into question whether the assumption that moving to an ISM for security would actually provide greater protection.

Report Page 11, para. 3 - Design Basis Threat need for localized threat
Design Basis Threat does allow for the application of local threat data. DOE Order 5632.1 C. paragraph 7.b. reads as follows: "The "Design Basis Threat Policy for the Department of Energy Programs and Facilities (U)" shall be used to identify and characterize the range of potential adversary threats to Departmental programs and facilities. Field Elements should review and develop, as appropriate, supplementary local threat policy to take into account site-specific and regional specific threat considerations". The key here is that the national threat is based on a document that is developed by an interagency group, but its implementation is expected to take local conditions into account as well. NN-51 has, however never received a request to adjust the implementation of DBT requirements based on the results of localized (or site-specific) threat analysis.

Report Page 13, para. 4 - "For example, the NN-51 V&V ..."
Comment: The V&V process, agreed to by the Field program offices and NN as part of SAI-26 shared responsibilities is intended to ensure the SSSP is a good document supported by, among other things accurate vulnerability assessments. Often though, the V&Vs, utilizing various assessment tools (e.g., JTS, Alpha) have pointed up deficiencies in the SSSPs. If these deficiencies, usually in the form of inadequate vulnerability assessments go uncorrected it would leave the facility at risk without the Field Manager's or the Secretary's knowledge. Because NN-51 usually facilitates the V&V assessment process when the process does identify deficiencies the consequence unfortunately is the perception that NN-51 is engaged in oversight when the reality is that NN-51 is only one participant in the SSSP V&V process along with the program office and the field office. When that process goes smoothly there seems to be no issue of NN-51's participating role.

Report Page 14, para. 1 & 2 - "Quality Panels"
Comment: We believe the Quality Panels are very effective in helping the policy development process, and generally actively participated in by the field and program offices. All policy, whether emanating from quality panels or revisions to Departmental Orders, is disseminated

through a structured departmental review process. Quality panels often see the need for and recommend policy changes. The quality panel members reach a consensus before many of the policy recommendations are made. It is expected that since the quality panels are represented by the sites, they would support the recommendations and field and program offices review and concur on the proposed changes before they are published.

Report Page 14, para. 3 - "Diversity in weapons and equipment . . ."
This is an important point which was also made in the Mahaley Report. As long as NN has no line funding source it does not have authority to manage equipment expenditures. It can only advocate standardization. But standardization and cost efficiencies are certainly one more argument for a security equipment line funding source, which NN unsuccessfully sought in the FY 2000 budget and will resurrect in its 2001 budget formulation. This point is also made in the Mahaley Report.

Report Page 15 - "Indirect charging of security costs"
The only argument for this notion is that it provides the site manager with great flexibility in the allocation of security expenditures. The huge downside is that security becomes the victim of all other operational exigencies. The Report implies cost efficiencies resulting from indirect charging, but it offers no solid evidence of such efficiency and we know of no evidence.

Report Page 16 - "Design Basis Threat (DBT) Development"
Comment: This confusing paragraph appears to mix performance testing with DBT development, two unrelated phenomena. But with respect to DBT development the Report errs in implying exclusive ownership by NN. It is the product of DIA, CIA, FBI, DOD and NRC input, is based on intelligence community generated factual, credible and validated information using terrorist operations information including equipment and technologies. It results indirectly from the DIA Postulated Threat and, contrary to the Report assumption has involved in its process DOE program offices as well as advance briefings to field office security personnel as well as DOE senior managers. The overall process, contrary to the Report statement, is rigorous and quite formal in the sense that it results from numerous interagency discussions over a series of months. Further, in 1998, NN-51 established the DOE Threat Steering Group to further augment program office involvement. The Group's success is characterized by pending agreed on threat clarifications.

Report Page 17 - "DBT Application flawed"
Comment: If DBT application by field sites is flawed by inflexibility in interpretation of requirements of the DBT that would be a result of failure to utilize the flexibility in DOE policy which provides for appropriate adjustment based on site specific characteristics. (See previous reference to specific language in Order 5632.1.C). Policy explicitly assumes DBT application based on a range of threats, site conditions (SNM types/quantities etc.). Policy explicitly rejects a one-size-fits-all approval. As stated, "field elements should . . . take into account site-specific . . . threat considerations."

Para. 4 - " A sound approach recognizes a spectrum of threats."
Comments: By Congressional direction, the DBT has been independently reviewed for validity, applicability and credibility. The National Security Council's Nuclear Command and Control System conducted the review and Reported in February 1997 that the DBT is a credible threat document and provides a baseline which the DOE should use to develop its protection strategy. In fact, the Report indicated that in some aspects, the threat levels should be increased. How the Report could fail to recognize that "a spectrum of threats" is inherent in the DBT assumptions is puzzling. Early discussion with NN-51 would have corrected this misunderstanding.
In focusing only on the DBT, this Report fails to recognize other sources of security policy, such as DOE Orders. Our security policy fully recognizes that not all sites are equally attractive to potential adversaries and uses the principle of *graded protection* to address this. The principle of graded protection requires that we make distinctions among facilities and among parts of facilities. We require different levels of protection depending on the materials stored at a particular facility and within facilities and apply different security standards to various areas based on the materials they contain. In short, our policy recognizes that there is a spectrum of targets and consequences.
An April 1998 GAO Report (*Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*) pointed out that "DOE uses a graded approach to protect its assets based on risk and vulnerability assessments. Under the graded approach, DOE develops and implements security programs at a level commensurate with the asset's importance or the impact of its loss, destruction or misuse."

Report Page 18 - "DBT and Denial"
Comment: The DBT itself does not require denial or any other single, specific strategy. Department Orders prescribe the protection strategy based upon site assessment, attractiveness of the target and consequences of unauthorized use. The DBT describes the adversary's capabilities and identifies the type of target that would be attractive from various scenarios such as theft, radiological sabotage, property destruction etc. Denial is prescribed in only the gravest of consequence, i.e., nuclear yield and must not be determined by cost. Most sites currently strive to meet denial strategy where applicable and where they understand the necessity for denial based on target type. Contrary to the Report suggestion (paragraph 3) that denial can be defined as interruption before the adversary escapes, in those cases where time lines to a possible nuclear yield are very short (review of which was the original purpose of this study) denial must occur virtually as the adversary arrives at the target.

Comment: The DOE has established a multi-level approach to risk management. Part of this approach is the designation of protection strategies to include: denial, containment, interruption, and recovery, recapture. The two most common planning strategies if denial and interruption within time lines determined by performance testing has failed are containment. However, as part of the "adversary" protection posture at a given site, the ability of the protective force to "interrupt" the adversary plays a critical role. The real issue has been, an inability of the sites to differentiate the types of SNM susceptible to specific manipulation and the required segregation of these materials from the general inventory. This is mostly special access information which

NN has thus far been unable to secure release for some Field Managers. Authors of the Report are completely familiar with this matter. Unfortunately, the review does not address this very important issue.

"DBT / Site Specific"
See previous comments which correct the Report's misunderstanding that the DBT and Departmental Policy are inflexible in implementation.

Report Page. 19, para. 1
Comment: This paragraph also assumes that protection policy means one-size-fits-all when in fact DOE Safeguards and Security Orders provide substantial site-specific flexibility. Through DOE Order 470.1 4. Requirements Section, Deviations which reads in part, "Alternate or equivalent means of providing adequate safeguards and security may be proposed . . ."

Report Page 20, para. 2 - 3 - "SSSP process is ineffective"
Comment: The conclusion that the SSSP process is ineffective is not supported by the remainder of the paragraph and those following paragraphs nor is it correct. The fact that the VAs prepared by the field elements do not always address required elements of the DBT or include the baseline adversary capabilities does not equate to SSSP ineffectiveness. The VAs conducted are starting point that should be used to assist the site to accurately and completely model their sites, assets and operations using other tools such as JTS etc. It should also be understood that adversary characteristics and equipment are constantly evolving over time. This is reflected in what has been observed as being readily available resources and equipment to potential adversaries, however, it must be noted that the most contentious issues cited by field personnel (flyer plates, sniper rifles, assault weapons, light antitank weapons, explosive devices, etc.) have been part of the DBT for many years. ASSESS, JTS and Alpha are helpful tools to provide rigor and increased consistency to the overall V&V process. Ultimately, the SSSP process produces high confidence that the site protective strategy can defeat the DBT and meet DOE protection requirements.

Report Page 20, para. 4 - "IG Study"
Comment: The Office of Safeguards and Security disagreed with the mentioned Report due to factual inaccuracies. The severity of the factual inaccuracies raised serious issues with the validity of the Reports findings and recommendations. The response to the IG reconfirmed that the SSSP guide were not policy documents and was a reconfirmation of earlier correspondence from NN-1 saying ". . . guides are discretionary and field elements may use any format they choose so long as . . . DOE Orders are met."

Report Page 23, para. 3 - "PAPs should be strengthened"
Comment: This paragraph is inaccurate and mis-categorizes the programmatic intent of the PAP. In the preceding paragraph it is noted that PAP is a safety program, here it indicates it is a measure for managing insider adversary issues. While PAP has been assigned a role in the Design Basis Threat (DBT), it is not itself directed at the insider adversary threat (PSAP is better

structured to do that). The Report should look to the basic purpose and structure of the programs, and not simply recommend "strengthening." It might be more productive to build on other bases, especially in the context of the two paragraphs which follow and identify broader areas of concern needing to be addressed. Further, the statement, "These programs are intended to enhance the protection of SNM and Classified information..." is inaccurate. Neither program was intended to protect classified information. They are structured to promote the protection of assembled nuclear devices (PAP), and Category I quantities of SNM (PSAP). The area of protection of security information associated with the maintenance of these programs should be addressed through the information security mechanism. If enhancement of that process is needed, the initiatives of the Office of Counterintelligence might be applicable.

Report Page 25, para. 1 - "NN-50"
Comment: DOE 470.1 paragraph 5, is clear regarding roles and responsibilities. NN is to establish safeguards and security policies, requirements, standards, and guidance for DOE operations, including design basis threat, for use in designing and implementing DOE protection programs, and the Program Offices are to issue program direction that is consistent with the S&S policy. No revision is necessary if all parties stay within the established roles. With respect to a concurrence role for SSSPs the roles of both NN and the program offices should remain unchanged. The Field Manager can ignore a nonconcurrence, but the fact of the nonconcurrence possibility can serve to ensure prudent judgement by the Field Manager as he/she exercises that approval authority.

Report Page 25 - "DBT process change"
Comment: The Report provides no evidence that this proposal has validity. The DBT itself is not challenged, and its implementation is not demonstrated to be unacceptably onerous since, as stated before the DOE Orders explicitly indicate the DOE expects site-specific application. Finally, the entire national security community of the U.S. Government knows of no better known instrument for the DOE to use for its overall protection program planning/implementation.

Appendix I:

Memo from Barbara R. Stone, Director Office of Safeguards and Security Evaluations Office of Independent Oversight and Performance Assurance to: General Eugene E. Habiger, Director Office of Security and Emergency Operations, SO-1

August 30, 1999

With attachment

Department of Energy
Germantown, MD 20874-1290

August 30, 1999

SO-20 Lead Document

A22

MEMORANDUM FOR: General Eugene E. Habiger, Director
Office of Security and Emergency Operations, SO-1

FROM: Barbara R. Stone, OA-10

SUBJECT: Recent Issues Regarding Vulnerability Analyses

During the last several years the Office of Safeguards and Security Evaluations has noted an accumulation of problems pertaining to the conduct of Vulnerability Analyses in support of Site Safeguards and Security Plans (SSSPs). In general, these problems pertain to the identification of adversary pathways and the representation of adversary tactical capabilities. The problems speak to a lack of consistency and rigor in the analytic processes that are used in support of the risk calculations that are central to the SSSP process. We believe that the time has come to address these problems on a Department-wide basis.

Our specific recommendations for resolving these problems, along with a more detailed supporting analysis, is presented in the attached position paper. If you would like to discuss these matters further, please contact me at 3-5895.

Barbara R. Stone

Barbara R. Stone, Director
Office of Safeguards and Security Evaluations
Office of Independent Oversight
and Performance Assurance

Attachment (OUO)

cc w/attachment:
G. Podonsky, OA-1

Office of Independent Oversight and Performance Assurance: Recently Identified Concerns Relating to the Preparation of SSSP/VAs

Introduction – This paper discusses concerns that have been identified during recent inspections with respect to the preparation of Vulnerability Analyses (VAs) in support of Site Safeguards and Security Plans (SSSPs) at various DOE sites. It outlines the nature of these concerns and presents a proposed course of corrective action.

There are two broad categories of SSSP/VA related concerns that have emerged during inspections conducted by the Office of Safeguards and Security Evaluations in the last several years. First, the field has experienced repeated difficulties in obtaining timely approval of SSSPs. This issue has been the subject of much recent attention and is currently being addressed by the SSSP Working Group. It will not be discussed in this paper.

The second—and more serious—concern pertains to the actual content and quality of the VAs that support the current SSSPs. This issue, which calls into question the very foundation of the risk calculations used throughout the Department, has received little attention from safeguards and security managers. It is this concern that forms the subject of this paper. The specific issues are grouped under three headings: (1) Weaknesses in the Depiction of Adversary Pathways; (2) Weaknesses in the Representation of Adversary Tactical Capabilities; and (3) Assumptions Concerning the Need to Analyze Only 'Worst-Case' Pathways. The following sections describe these issues in greater detail and present a proposal for addressing them within the larger framework of creating a more effective VA process.

Weaknesses in the Depiction of Adversary Pathways

Most DOE facilities use the ASSESS analytic tool to identify potential adversary pathways. This is perfectly reasonable. Although the ASSESS tool has its inherent weaknesses, it remains the best currently available method for achieving an objective rating of potential pathways. It is certainly stronger than largely subjective methodologies such as Alpha, which is fundamentally little more than a means of organizing subject matter expert opinion. Unfortunately, some sites are not making the best use of the ASSESS tool to generate solid, defensible pathway analyses. There are three ways in which the use of ASSESS could be significantly improved.

Assigned Detection and/or Delay Values Do Not Accurately Represent Actual Capabilities. ASSESS builds upon a detailed representation of all of the security-related features at a site, including such things as the delay times associated with doors and walls and the effectiveness of intrusion detection and assessment systems. By calculating the relative contribution of each path element in detecting or delaying an adversary, ASSESS is capable of identifying the optimal pathways for an adversary. Obviously, the ability of ASSESS to perform this function depends upon the assignment of numerical values for each protection element that do not distort that element's relative effectiveness. But, despite the fact that there is both reasonable guidance and

a sufficient body of experience within DOE to support appropriate determination of such values, errors often occur. This appears to be partly a function of carelessness—building an accurate ASSESS facility file is laborious, time-consuming work that rarely receives the required amount of resource support. It also appears to be a function of simply adopting the default values contained in the program, without doing the necessary analysis and/or performance testing necessary to justify either the defaults or a user-defined modification. During one recent inspection, a facility was found to have assigned a detection probability for a non-destructive vehicle search—an inherently difficult task—that was identical to the detection value assigned for the detection of individuals traversing a PIDAS with multiple, complementary intrusion detection sensors. Although this was patently absurd, neither the modelers nor subsequent reviewers had challenged the number.

ASSESS Analyses Are Not Kept Up-to-Date. As already emphasized, the preparation of an ASSESS analysis is both labor and time-intensive. Furthermore, since it requires a fairly high level of expertise, facilities have often resorted to outside technical experts to conduct (or, at least, to supplement) the ASSESS preparation effort. And then, at least at some facilities, the effort essentially freezes. During one recent inspection it was noted that the ASSESS-identified adversary pathways used to support the SSSP had been developed several years ago, using a facility configuration that did not reflect significant upgrades in intrusion detection systems. Faced with these upgrades, a real-life adversary would certainly have searched for other pathways, likely the same pathways that an updated ASSESS model would have identified.

ASSESS Insider Analyses Are Disregarded. In addition to calculating pathways for outside adversaries, ASSESS also can calculate probable insider and collusion path strategies. Although these analyses are difficult to complete, the results have generally proven valuable. Recently, however, less and less attention is being given to either updating existing ASSESS insider analyses or to conducting new ones when changes in facility operations indicate. This appears, largely, to be an unintended consequence of Department-wide reliance on PSAP to mitigate the insider threat. In other words, in spite of clear guidance to the contrary, the increasingly common assumption seems to be that "if we place a category of insiders into PSAP, then we don't have to analyze the threat that they represent."

All three of these problems can be related, at least in part, to the unwillingness of sites to make a sustained commitment to keeping VAs completely up-to-date. This, in turn, appears to be related to the perception that SSSPs have no useful purpose and that minimal compliance with the SSSP/VA requirement is all that should be demanded.

Weaknesses in the Representation of Adversary Tactical Capabilities

In the early part of this decade, the probable outcome of engagements between an adversary team and the protective force was usually calculated using the Neutralization module in ASSESS. Over the last five years, most DOE facilities have replaced this with more tactically representational models, first SEES and then JTS (the most recent iteration, JCATS, is just now becoming available). These models, in effect, constitute a kind of electronic performance test. Although they are not inexpensive to conduct, they are considerably less expensive, test for test, than corresponding force-on-force tactical performance tests. Thus, sites have increasingly relied upon these models as the primary element in developing the Probability of Neutralization

numbers that are essential to an overall calculation of protection system effectiveness. In effect, the risk numbers found in most SSSPs today rely very heavily upon the outcome of battles fought on computer screens, with limited numbers of force-on-force tests to supplement the computer-generated results. But neither JTS modeling nor force-on-force testing is effective if adversary capabilities are not adequately represented. Several problems in this area have recently been observed.

There Are Significant Errors in the Database Supporting the JTS Combat Simulation Model. While JTS is capable of providing useful indications of performance effectiveness, this capability depends upon the accuracy of the weapons and munitions performance data incorporated into the model's databases. JTS uses a complex set of databases to model tactical engagements in a near "real-world/real time" manner. The program compares for a given weapons/munitions versus target set a series of probabilities to include:

- The probability that an individual, armed with a particular weapon, would engage the target;
- The probability that, if the target is within the effective range of the weapon/munition, the target would be hit; and
- The probability that a single hit would kill or disable the target.

Within the JTS databases, there are two primary table that are used to support the latter two probabilities, namely Probability of Hit (Ph) and Probability of Kill (Pk). During recent reviews of JTS files used in the DOE community, this office has identified significant errors in these two tables. These errors will either over or under estimate the outcome of specific engagements, leading to questions regarding the reliability of the overall results. In addition to the identified errors, a significant number of readily available weapons and munition types are not included in the database.

Capabilities of Available Adversary Weapons Are Not Being Accurately Represented. In the last year this office has catalogued a long list of readily available adversary weapons and tools that are not being used appropriately by the adversaries depicted in current SSSP/VAs. Among these are tactical smoke, irritant gases, anti-personnel and anti-vehicle explosive devices ("stay-behinds"), grenades, armor-piercing small arms ammunition, and communications disruption devices, to name but the most obvious. It has become "customary" in DOE to limit the use of such weapons and tools, creating the potential for artificially high calculations of protective force effectiveness. This situation is equally common in both JTS calculations and in MILES-based force-on-force testing.

Adversary Tactics Are Poorly Thought-Out. Observed adversary tactics used during JTS simulations and validation and verification force-on-force tests are frequently crude, and often do not rise to the level expected of troops who have completed basic infantry training. During one recent inspection, it was noted that the adversaries depicted in the site's analysis succeeded in gaining control of a target location at the onset of their attack—and then hunkered down in tactically worthless positions that sacrificed the benefit of this initial advantage. Adversaries sometimes take little or no advantage from outside overwatch positions or from the use of

"stay-behinds" to isolate a target location or channel the protective force response. In both performance testing and simulations, this is likely the result of inadequate preparation. Personnel assigned to portray adversaries in modeling and performance testing are generally given only a few days to prepare tactical plans. A special problem with JTS simulations is that, generally, one computer operator is assigned to control the entire adversary team, while three (sometimes more) operators are employed to represent the protective force. This leads to situations where one adversary element is well managed in the simulation, while other elements are neglected and relatively ineffective.

The Shock Value of an Actual Attack is Undervalued. The only element of surprise in a JTS simulation or in a force-on-force test comes when an adversary comes up with some new tactical twist. The most fundamental real-world surprise—the fact that an attack is actually taking place—can never be adequately represented in such activities. Yet vulnerability analyses uniformly assume that, with no prior warning whatsoever, personnel who have spent years conducting routine patrols punctuated by the occasional MILES drill will respond with composure and complete efficiency when faced with an actual attack. This is compounded by the fact that many protective force personnel have never been in an actual combat situation and have never experienced the sudden shock of casualties among colleagues and friends. The adversary in the real world would have no such disadvantage. Having planned the attack and having chosen to carry it out, the adversary team members are, presumably, psychologically prepared to carry it out. And it is reasonable to assume that the members of an adversary team are already inured to bloodshed. Despite this, the typical analysis makes no effort to weight system effectiveness numbers to compensate for this problem.

Weaknesses such as these are partly a function of the structure of DOE security itself. We have a place for managers and personnel with a background in protecting assets, be it former military policemen or products of our own security forces. But we have recruited only a few personnel down through the years whose expertise is in *attacking* facilities. Thus, we tend to think like defenders, not like attackers, even when the task at hand is to realistically represent the capability of the terrorist. A second weakness is the lack of institutional resources dedicated to maintaining an up-to-date picture of adversary tactical and technical capabilities. Currently, no one in DOE outside of the Office of Safeguards and Security Evaluations appears to have a consistent interest in either cultivating the adversary mind-set or an understanding of adversary capabilities.

Assumptions Concerning the Need to Analyze Only 'Worst-Case' Pathways

The most recent format and content guidance for SSSPs indicates that the SSSP only needs to contain detailed descriptions of the 'worst-case' scenario results. This has led to the misconception that the only scenarios that require full-scale analysis are identified worst-case scenarios. Thus, some facilities come up with a set of potential high-risk scenarios, analyze them, develop near and long term mitigation to describe in the SSSP, and then conclude their analysis. This, however, does not square with stated DOE guidance, which required that all potential high and moderate risk scenarios be evaluated and documented, even if only the worst-case scenarios are explicitly discussed in the SSSP. Moreover, a site cannot even determine which scenarios are worst-case, unless all conceivable scenarios are at least considered. Here again, the problem seems to be pressure to do the compliant minimum, instead of applying the resources necessary to do the job right.

Recommended Actions:

The common issue in all of these concerns is the need for greater consistency and rigor in the conduct of VAs. This should be addressed at two levels:

1. Expectations for VA conduct in these areas should be clearly established.

2. Headquarters-level quality control should be rigorously exerted.

To accomplish these tasks, a committee should be formed to establish expectations regarding the issues discussed in this paper, particularly the representation of adversary characteristics. This committee should consist of representatives from those organizations with direct interest in the protection of SNM, including NN, DP, EM, and OA. This same committee, augmented by appropriately qualified technical specialists, should also be made responsible for conducting detailed quality review of all SSSP/VAs.

The combined result of these two activities should be to ensure that (1) the expectations communicated to vulnerability analysts reflect a consistent DOE-wide approach to conducting rigorous analyses and (2) appropriate quality standards are maintained. In this manner we can assure that all risk calculations are made on the same basis, enhancing the ability of senior Departmental managers to make complex-wide risk/benefit decisions.

In addition to these broader policy responses, the Department should also take action to ensure the reliability of its JTS analysis tool by procuring from the U.S. Army a certified database that includes representative weapons/munitions available to both DOE protective forces and potential adversaries. This certified database should be distributed to all sites currently using JTS (and also to sites that have adopted JCATS, the newest JTS variant). The Army Material Systems Analysis Agency (AMSAA) has, as one of its missions, responsibility for developing certified databases for Department of Defense models (such as JTS). The Office of Safeguards and Security Evaluations has already had preliminary discussions with AMSAA's director regarding the provision of such a database. While cost estimates are not yet available, the cost to DOE should be minimal, since the Army has already developed this information for its own use. The primary question is which DOE organization should take the lead in implementing this system-wide enhancement.

Appendix J:

Letter from Timothy P. Cole, President Wackenhut Services Inc. to:
Terry Vaeth, Manager U.S. Department of Energy, Rocky Flats

July 16, 1992

WACKENHUT

SECURITY SYSTEMS AND SERVICES THROUGHOUT THE WORLD

WACKENHUT SERVICES INCORPORATED
1500 SAN REMO AVENUE
CORAL GABLES, FLORIDA 33146-3009
TELEPHONE (305) 666-5656

July 16, 1992

Mr. Terry Vaeth
Manager
U. S. Department of Energy
Rocky Flats
P.O. Box 928
Golden, CO 80402-0928

Dear Mr. Vaeth:

Recent events at the Rocky Flats Plant relative to Protective Force management and operations cause me great concern and I feel compelled to bring them to your attention. I believe the situation has degenerated to the point where intervention by the Field Office Manager is required.

In order that you have a full perspective on my position, I would like to relate how WSI came to Rocky Flats and point out some of the more salient activities that have occurred since. When Mr. Tuck called me on July 25, 1990, asking if we would assume the Protective Force mission at Rocky Flats I replied "absolutely yes and when would you like us to start." He replied "tomorrow if possible." Two days later, I met with Mr. Nelson to discuss takeover and we, in fact, assumed full responsibility for the force on August 1, 1990. We fully recognized the potential downside of assuming responsibility for this operation; especially in light of the serious and very fundamental problems that caused us to be there in the first place. Upon arrival we found a hostile union and resentment from incumbent employees to include virtually all levels of EG&G management. There was little DOE staff to support us in our role as a M&O contractor and we faced a government lack of acceptance which, to a certain degree, still remains.

While I felt the problems would be severe both operationally and organizationally, I was optimistic of our chances as I felt DOE would recognize the herculean task they had given us and adopt a supportive, nurturing management style as a result. The former observation was right on; the latter was not.

During our first few months we were racing to prepare for an upcoming DOE OSE Inspection and Evaluation. Further, the plant mission was undergoing intense scrutiny based on safety and environmental concerns. Those priority issues coupled with fundamental security needs put us in a position of vulnerability from a performance measurement standpoint. There weren't enough hours in the day. The Protective Force supervisory ranks and the number of cleared, trained Security Inspectors were inadequate for accomplishment of the security mission which drove us to bringing in "augmentees" from other DOE locations. As you can imagine, having forty/fifty or more Security

Inspectors from different sites, representing different unions was a management challenge in its own right. All of the issues described above coupled with the historical disregard for the security mission exhibited by our predecessors drove us to aggressively implement fundamental changes within the organization. To bring about what we perceived to be the necessary changes in a stable environment would have been very difficult. To accomplish this in a "hyperactive" environment where negative employee culture must be modified has been exceedingly complicated and demanding. We have repeatedly accepted the jeopardy of attempting to replace/compensate for security system deficiencies with Security Inspectors to our ultimate detriment -- a position in which we still find ourselves. We continue to attempt to perform to ill-defined expectations under conditions where we must work with inadequate/outdated security systems and associated maintenance.

Notwithstanding the difficulties described above, our past two years at Rocky Flats have not been without notable accomplishments. We have successfully completed two DOE OSE Inspection and Evaluations plus numerous reviews and audits. WSI also took the lead in a joint effort to establish the tripartite organization which has accomplished so much in the past two years. We integrated large numbers of augmentees into the existing Protective Force without any safety or organizational damage. These onerous and labor intensive compensatory measures were without equal in DOE's history. WSI developed the enhanced mission requirements that Operation Desert Storm necessitated and accomplished them with professionalism and a sincere pride. You should also be aware of the union disaffiliation activity which occurred during this period. WSI maintained an objective, equitable relationship with both union activities until the issue was decided. Our troops have placed very high in national competitions and acquit themselves well in every respect when called upon.

My attempts to give you a feel for the organizational and operational climates when we assumed responsibility for the Protective Force is for a real purpose. The purpose is not to make excuses, explain away, or otherwise disclaim our performance deficiencies. We have privately and publicly accepted responsibility for all of our actions and stepped up to problems and emphasized corrective actions rather than arguing the issues. I now believe it is time for DOE RFO to accept that same responsibility. I, more than any other, know what is at stake and the potential outcomes of bringing these issues up to you. However, after twenty-one years of direct service to my country and another ten through contractor support I feel I am more than qualified to make management observations relative to our existing relationship. I must tell you very frankly that we have been exposed to "management terrorism" and "organizational sedition" for well over a year. This simply must stop. Positive changes have taken place. We are working hard to accelerate the pace of change, but we all must recognize that changing a culture is measured in years.

The DOE management oversight process at RFO is, in my opinion, heavily slanted toward the negative to include specific "targeting" of people in management as well as individual members of the Protective Force. The distrust, doubt and fear our Security Inspectors have for certain DOE officials is unhealthy and may lead to serious consequences. Rather than constantly assail the attitude of some Security Inspectors toward certain DOE officials, I submit we take an in-depth look at how this situation was created. I believe we will find this is a shared problem. While we have dealt with performance deficiencies when they occur it is now time for us to address how this environment came to be in the first place and how can we remedy it.

The Protective Force has had four General Managers since contract inception. Each has possessed extensive credentials in the safeguards and security field as well as education and general management experience. Further, each was well respected within the DOE S&S community. To accept the fact that all four have not been capable of managing the

Protective Force is illogical and really without merit. However, both WSI and EG&G have attempted to satisfy ill-defined expectations by replacing numerous senior managers. When you consider the mutuality of problems both prime contractors have faced you must pause to consider the commonality of conditions. This management/oversight approach has created such a negative and adversarial environment between us that I do not think it is possible for mutual success under current conditions. We do not face this type or style of management terror at any other facility within the Corporate responsibility. Our performance at these other sites routinely results in performance scores in the high eighties or low nineties.

Something is seriously wrong and I would like to get it fixed. Our Corporate reputation has suffered beyond what equity would suggest. Our personal, professional and financial investments and related corporate commitments to RFO are substantial and will continue. I seek only to establish a balanced, positive evaluation of our performance consistent with the challenges and limitations we face. We only want a level playing field and an opportunity to execute our mission at Rocky Flats in a rational, thoughtful manner that is free from intimidation or inappropriate professional and financial anxieties.

Mr. Vaeth, these are serious issues that have serious consequences. I assure you I have put lots of thought and consideration into this letter. There is attendant jeopardy in taking these issues on, especially in light of the ongoing contract actions. However, our company is founded first and foremost on a high standard of personal and professional integrity. Our ethical conduct and desire to do the very best for any client will never be compromised in the blind pursuit of a contract dollar. My stake in the RFO Protective Force contract is personal. I want our mutual success more than anyone; however, I am unable to reconcile the current oversight conditions. I seek your help in changing them for the better.

Sincerely,

Timothy P. Cole
President

TPC/cmo

Appendix K:

Office of Personnel Management interview with William R. Gillison, General Manager, Wackenhut Services Inc.

between March 6, 1996 and April 10, 1996

William R. Gillison, General Manager, Wackenhut Services, Inc., Building T119B, Rocky Flats Environmental Technology Site, P.O. Box 1719, Broomfield, Co. Interview was held in Building T115B with Marcy Nicks of the Department of Energy in attendance on 3/6/96 and 4/10/96.

Mr. Gillison provided the following information on 3/6/96, 3/7/96, 3/20/96, 4/8/96 and 4/10/96.

Gillison met Jeff Peters in 2/90 when Peters was a Security Inspector and Vice President of the Security Police Officer's (SPOs) union. Both were employees of EG&G at that time. In 8/90, Wackenhut Services Incorporated (WSI) assumed responsibility of the protective force at Rocky Flats. Peters transferred to WSI and Gillison remained with EG&G until 4/92. They had very little contact until 9/90 when Peters was promoted to the position of Manager of Internal Security. Contact from then until 4/92 occurred a couple of times a month at security meetings. In 4/92, Gillison became the General Manager of WSI and Peters was promoted to the position of Director of the Protective Force Operations. Peters' direct supervisor was William Sanders the Acting General Manager of Operations. In 10/93, Sanders was made Director of Training and Gillison became Peters' direct supervisor, sharing the supervisory duties with Jim Gilmer, Deputy General Manager. This period of direct supervision has continued to the present although Peters was reassigned to the Director of Training in mid 1/96.

From 4/92 to mid 1/96, they had daily contact, only exception being from 12/6/95 to 1/17/96 when Peters was on paid Administrative Leave. There was very little contact during that period of time. Since 1/96, contact is a couple of times a week as Peters is now assigned to another building. Their only social contact has occurred at company Christmas parties, one picnic with other work acquaintances and on one occasion, they and others went target shooting in Boulder.

Peters has always been a very good employee who takes his job seriously. Peters has been nationally recognized as a Whistleblower by the Secretary of Energy, Hazel O'Leary a year or two ago. The whistleblowing involved Peters making tape recordings of a very difficult Department of Energy (DOE) Manager of Safety and Security, Rich Levernier. The taping of the conversations and negative comments about Rocky Flats Contractors and RFFO DOE Manager Mark Silverman resulted in Levernier being reassigned to another DOE facility about 18 months ago. Levernier was making life very difficult for WSI as WSI was continually under surveillance, being criticized unfairly and made to look like the WSI was unworthy of any contract bonuses. Peters turned his information over to the Inspector General's office which resulted in an investigation concerning the conduct of Levernier. Gillison was also interviewed about Peters' tapes and WSI's dealings with Levernier.

Gillison protected Peters during this whistleblowing activity and considered himself to also be a Whistleblower, although Gillison never officially declared himself one or received recognition as a Whistleblower. Gillison went along with Peters taping the conversations with Levernier as valuable information was gathered from those tapes.

In about 2/93, Gillison heard WSI Corporate had lost a civil court action when the corporate office was sued by Alesco, the company who was running the Alaska pipeline. Alesco sued WSI for gathering information on a pipeline employee without the employee's knowledge. WSI lost the case. When the outcome of the lawsuit became knowledge, Gillison telephoned WSI Corporate Office to see if Peters' tape recordings of conversations with Levernier could place the company in jeopardy. Gillison was advised that the tapings were not illegal, but to protect the company, Gillison should tell Peters to stop the tapings. Gillison stated at that point in time, there were no laws, rules or regulations from the DOE

K-H managers felt Peters' charges were incredulous and could not understand why Peters reported his concerns to the IG's office after Rocky Flats DOE took responsibility for the high risk SNM. Gillison says Waller is from the school where an attitude of "when in charge, take charge" and stated Waller assumes K-H can take full risk for SNM. Gillison explained that only the DOE Headquarters can take responsibility for high risk. Mark Silverman RFFO DOE can assume moderate risk and K-H can assume low risk. Gillison says Waller was surprised to learn this.

The SNM was moved back into vault room on 11/28/95. The move of the SNM in the first place was against the DOE directives as no security plan and vulnerability analysis (VA) had been done when the move was made on 10/29/95. The security plan was not completed until two or three weeks after the material had been moved to Room 3337. Gilmer signed the plan in about mid 11/95 after Gillison made a statement to Gilmer that WSI staff were being beaten down on the matter. Gillison also reported to WSI Corporate that the SNM was at high risk and it was not WSI's responsibility to assume responsibility for such material. Only the DOE Headquarters can assume responsibility for high risk SNM.

Although no SPOs were on the SNM the last week, Gillison says he did not feel too uncomfortable with the SNM being unprotected by humans as the three Intellitech alarms were still there and if an adversary did approach the material, Gillison felt there could be time for SPOs to respond and keep the material from radiological sabotage. However, Gillison did not approve of the K-H team bypassing requirements to move the material so IAEA Treaty requirements could be met on time.

Gillison recalls having a conversation with Peters about considering himself "chewed out" by Corporate for being disloyal to the company by furnishing testimony in the William Milligan court case. Gillison does not recall this conversation being on 11/28/95, but believes it was a little earlier. Exact date unrecalled. Gillison explained Milligan had been fired by WSI and Milligan subsequently sued the company. Peters supplied a deposition for Milligan's trial that was in Milligan's favor and not the company's. Milligan was a Whistleblower who was terminated from employment because of poor performance. Gillison felt Peters should have told Gillison what his testimony would be and the company would not have pursued litigation to fight Milligan's claims. Gillison stated Peters' deposition was in Milligan's favor. As a result, the company settled out of court with Milligan.

Gillison also stated he saw no connection between Peters being a Whistleblower in the Levernier problem and Milligan's whistleblowing activities. Gillison did state Milligan was on Levernier's "hit list" of WSI employees targeted by Levernier for dismissal and Peters' whistleblowing on Levernier included that list. Gillison believes Levernier had a grudge against Milligan and put Milligan's name on the hit list. Gillison also added, the attitude was a little like WSI experiences with K-H. Meaning K-H is slow in letting WSI know when SNM is being moved and K-H skirts the DOE directives to make the moves on short notice.

Gillison and Peters have philosophical differences regarding the safety and safeguarding of SNM. Peters always thinks of the worst case scenarios and Gillison tends to think of lesser adversarial problems. Gillison is well aware of what could be deemed catastrophic problems, but does not let them rule his decisions as the plant is in a cleanup mode and has to make due with less dollars. By the same token, Gillison stated he is not going to accept lax security where it concerns the health, safety and security of the plant, its employees and the community at large.

Appendix L:

Report to the President on"Status of Safeguards and Security for 1996," Office of Safeguards and Security, Office of Security Affairs, Department of Energy

January 1997

Status of Safeguards and Security for 1996

Office of Safeguards and Security
Office of Security Affairs
January 1997

Department of Energy
Germantown, MD 20874-1290

January 27, 1997

MEMORANDUM FOR DISTRIBUTION LIST

FROM: EDWARD J. MCCALLUM, DIRECTOR
OFFICE OF SAFEGUARDS AND SECURITY

SUBJECT: STATUS OF SAFEGUARDS AND SECURITY

This report provides a comprehensive review of Safeguards and Security activities throughout the Department of Energy complex during 1996 and provides a candid look at the future of the Program. The report is structured to present a Departmental perspective of the Safeguards and Security Program to senior management and all safeguards and security professionals. For the first time the report also contains a section which summarizes safeguards and security participation in National Nuclear Command and Control activities.

During the past year **disturbing trends** continued that resulted in **additional budget reductions**, further **diminishing technical resources**, **reducing mission training** and undermining our ability to protect nuclear weapons, special nuclear materials and other critical assets. This is occurring at a time of increased responsibilities resulting from the international transfer of nuclear materials and dismantling of U.S. nuclear weapons. Although traditional and time proven protection principles are still emphasized, it is becoming **increasingly difficult to adequately protect our nation's nuclear stockpile in the face of inadequate resources, obsolescent systems, aging protection forces and funding uncertainties.** This has increasingly resulted in a "hollow-force" that goes below the "bottom line" and makes it more difficult to fulfill National Security mandates. It is imperative that the Safeguards and Security **downward resource spiral be immediately halted.** Further, nuclear materials must be consolidated to reduce costs or additional resources must be found for protection. Adequate investment is essential to sustain a vital Safeguards and Security Program that continues to support the nation's security, the public health, safety and our environment.

I am confident that the report will be a valuable tool to stimulate open conversation, provide constructive feedback and assist in addressing the continued viability of the Department's Safeguards and Security Program. Collectively, we must continue to strive to maximize the use of our resources necessary to ensure requisite security for the Nation's and the Department's most vital assets.

Attachment

EXECUTIVE SUMMARY

This report summarizes the protective posture for the nation's special nuclear materials stockpile, weapons, and related security interests at both nuclear and non-nuclear facilities for 1996. In doing so, the report reveals a dynamic Safeguards and Security Program that continues to judiciously manage the demands of an expanded and increasingly complex mission despite the damaging effects of declining resources.

The mission of the Safeguards and Security Program is to develop policy, programs and technology to protect Department of Energy (DOE) facilities, nuclear weapons, nuclear materials, classified and sensitive information and critical assets. Of primary importance is the protection and accountability of special nuclear material, nuclear weapons, and classified and sensitive unclassified information associated with the nation's nuclear stockpile. This stockpile consists of nuclear weapons and several hundred metric tons of special nuclear material, to include nuclear weapons undergoing maintenance or dismantlement. It also involves millions of pages of classified information located throughout the country.

As it exists today, the Department is faced with myriad challenges that attest to the criticality of a robust and effective safeguards and security program. In this regard, the principal challenges facing the Department include: (1) today's diverse and unpredictable global security environment; (2) the threat of nuclear proliferation; (3) reliability of nuclear materials control and accountability; (4) long-term storage of special nuclear materials; (5) aging DOE facilities and security systems; (6) declines in Protective Force preparedness; (7) needed improvements in information security capabilities; (8) inadequate funding of the personnel security program; and, (9) the need for adequate staff training and development. When viewed in the context of declining budgets, these challenges and their potential impact to national security are even more crucial.

The Department of Energy's Safeguards and Security Program has vigorously and imaginatively responded to these challenges through the development of adaptable policy and the implementation of innovative cost-saving measures. While the successes enjoyed through these efforts have yielded valuable operational efficiencies, the Department's Safeguards and Security Program is faced with major debilitating obstacles and projected shortfalls that will exacerbate existing resource shortages and severely limit security responsiveness and fulfillment of the safeguards and security mission.

The present mission-to-resource imbalance in the Department's Safeguards and Security Program is dramatically evidenced by the growing disparity between safeguards and security resource requirements identified by Departmental facilities and actual allocations eventually provided by cognizant Program Offices. This growing difference between requirements and allocations has led to a reduction of staffing and other resources at Headquarters and field facilities to a level where important security functions are operating under conditions of "single-point failure." Consequently, when such a condition exists, no reliable backup capability exists should a critical security function be defeated.

The resulting one-deep security structure has seriously weakened critical protection postures and capabilities that, in some cases, can now be more easily evaded or defeated. As an example, the Department's Protective Force strength has been reduced almost 42 percent since 1992, resulting in a "hollow" force that is not only growing older, but is also less equipped to handle today's security challenges. In the past, Protective Forces had been used as a compensatory measure for aging physical security systems. Given the magnitude of the reductions, however, this is no longer the case.

Similarly, aging physical security systems throughout the complex are a growing concern. Safeguards and security systems at some nuclear weapons production sites were designed and installed in the 1960's. These systems no longer provide the necessary level of protection required in today's threat environment.

Problems with the Department's security posture are not limited to physical security measures. With facilities being forced to store larger than expected amounts of special nuclear material for longer periods, the ability of the Department to ensure the accountability of special nuclear material under its possession has become even more acute. Consequently, significant concern exists where surveys reveal that major Departmental facilities hold unmeasured nuclear material inventory, and former processing facilities with deposits have not been adequately characterized.

With respect to information assurance, the Department is faced with an exponential growth of interconnected and stand-alone automated systems processing both classified and sensitive unclassified information. As this interconnectivity continues to expand, through local and complex-wide networks, it no longer becomes necessary to physically enter a facility to acquire, modify, or destroy classified and sensitive information. Therefore, a greater emphasis will be required to provide security for the DOE's automated information systems.

Funding shortfalls continue to plague the program. Since reaching a high of $1.143 billion in Fiscal Year 1991, Program funding is estimated to decrease to approximately $757 million in Fiscal Year 1998. Based on current analysis (*Figure 1*), the projected budget will fall short of requirements by $157 million annually until material is consolidated and major sites closed.

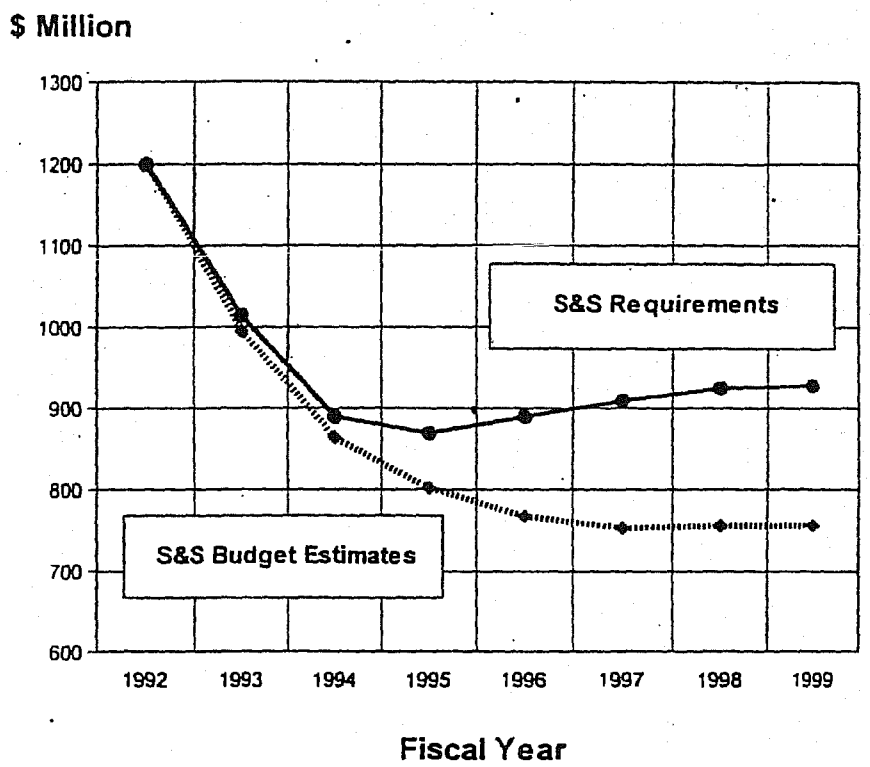
The 1998 funding shortfall, in Safeguards and Security requirements, is $157 million and is composed of such major diverse program elements as:

- physical security upgrades at Los Alamos National Laboratory (designated DOE production facility);
- additional protective force staffing such as special response teams and first responders;
- a special nuclear material storage facility at Savannah River which will meet International Atomic Energy Agency requirements;
- funding to conduct protective force readiness exercises and training to support validation of protection conditions;

- funding to conduct personnel security investigations and reinvestigations for access to classified information and special nuclear material; and,

- preservation of continuing security operations and technology applications to modernize and enhance nuclear material protection, control and accountability.

Figure 1. Crosscut Estimate



The effects of these budget shortfalls are illustrated in *Figure 2* found at the end of the Executive Summary. These figures summarize the status of safeguards and security at both DOE weapon and non-weapon facilities. The ratings assigned have been determined from a combination of results gleaned from the Safeguards and Security Survey Program, site assistance visits, program self-assessments, and Headquarters' analysis of site management and operational performance. The decline of overall Safeguards and Security Program readiness and capability represents a disturbing trend that must be addressed.

While funding for the Safeguards and Security Program has fallen significantly, program requirements have not. In fact, requirements are growing. The Safeguards and Security Program continues to further expand into non-traditional, yet critical, areas involving national security interests. Principal among these new areas is the Department's nonproliferation activities. Safeguards and Security plays a vital role in preparing Departmental facilities subject to the conditions of nuclear nonproliferation and treaty verification agreements, especially those related to International Atomic Energy Agency (IAEA) safeguards activities. This undertaking has moved the Safeguards and Security Program beyond its traditional roles and expanded its mission into another area of national importance.

Requirements are also driven by sources external to the Department. For example, the Department is required to adhere to the provisions of Presidential Decision Directive 39, *U.S. Policy on Counterterrorism* (PDD-39), that reaffirms the use of all appropriate means to deter, respond to, and defeat all terrorist attacks on U.S. territory, people, resources, and facilities whenever they occur. The Directive details the need to deter the acquisition of weapons of mass destruction (nuclear, chemical, and biological) by terrorist groups. Specifically, this policy states, ". . .terrorist acquisition of weapons of mass destruction is not acceptable, and there is no higher priority than preventing acquisition to (sic) such weapons/material or removing that capability from terrorist groups." As with other Presidential and National Security directives, the Department must adhere to the requirements set forth therein.

Notwithstanding the need for more resources to adequately meet its mission requirements, the Safeguards and Security Program continues to develop and implement new approaches that are both efficient and cost effective. As an example, the materials control and accountability program is actively pursuing improvements by increasing emphasis on physical inventory, leveraging new technologies to ensure measurement reliability, exchanging ideas at the working level by conducting improvement working groups, and increasing confidence through improved accounting standards.

With respect to the ever growing need for effective information security measures, the Department is developing and acquiring technologies to enhance information protection, training personnel to meet the demands of higher technology, and conducting strategic planning that fosters the development of partnerships between Government and industry.

These improvements will have marginal impact, however, unless the necessary resources are soon provided. Never has the Department been confronted with a more dynamic and less-predictable global security environment. The near-static, monolithic threat that once compelled five decades of domestic nuclear weapons production has given way to more sophisticated and fragmented threats in various guises; projected through acts of terrorism, crime, and international violence.

To meet this diverse challenge, the Department must commit to a viable Safeguards and Security Program. Failing to honor its mission requirements will not only reduce public trust and Congressional confidence, but more importantly, will endanger the national security and public safety it is obligated by law to maintain. Unless decisive measures are taken to stem the reduction of crucial program resources and capabilities, these voids threaten to become a larger window of vulnerability, which places the Nation's special nuclear materials stockpile, weapons, and critical holdings at an unacceptable level of risk.

Figure 2.

CY 1996 STATUS OF SAFEGUARDS AND SECURITY RATINGS AT DOE WEAPON FACILITIES

FACILITY	FACILITY RATING	PM	PPO	NMC&A	IS	PS
Kansas City Plant (Allied Signal)	SATISFACTORY			N/A		
Los Alamos National Laboratory	SATISFACTORY	↓	↓			
Pantex Plant (Mason & Hanger)	SATISFACTORY					
Sandia National Laboratories - New Mexico	SATISFACTORY					
Transportation Safeguards Division	SATISFACTORY					
Tonopah Test Range (Sandia Corp.)	SATISFACTORY		⇧		⇧	
Nevada Test Site (Bechtel - Nevada)	SATISFACTORY		⇧		⇧	
Lawrence Livermore National Laboratory	MARGINAL ↓	↓				
Sandia National Laboratories - California	SATISFACTORY					
Y-12 Site (LMES)	SATISFACTORY					⇧
Rocky Flats Environmental Technology Site (Kaiser-Hill)	MARGINAL ↓	↓	↓			↓
Consolidated Tritium Facility (WSRC)	SATISFACTORY					

RATINGS AT DOE NON-WEAPON FACILITIES

FACILITY	FACILITY RATING	PM	PPO	NMC&A	IS	PS
ALBUQUERQUE OPERATIONS OFFICE	SATISFACTORY			N/A		
Pinellas Plant (LMSC)	SATISFACTORY			N/A		
CHICAGO OPERATIONS OFFICE	SATISFACTORY			N/A		
Argonne National Laboratory - East	SATISFACTORY					
Argonne National Laboratory - West	SATISFACTORY					
Brookhaven National Laboratory	SATISFACTORY					
New Brunswick Laboratory	SATISFACTORY					
IDAHO OPERATIONS OFFICE	SATISFACTORY			N/A		
Idaho National Engineering Laboratory	SATISFACTORY					

FACILITY	FACILITY RATING	PM	PPO	NMC&A	IS	PS
Idaho Chemical Processing Plant (LITCO)	SATISFACTORY					
NEVADA OPERATIONS OFFICE	SATISFACTORY			N/A		
OAKLAND OPERATIONS OFFICE	SATISFACTORY	⇩		N/A		
OAK RIDGE OPERATIONS OFFICE	SATISFACTORY			N/A		
K-25 Site (LMES)	SATISFACTORY		⇧			⇧
Oak Ridge National Laboratory	SATISFACTORY					
Portsmouth Gaseous Diffusion Plant (LMES)	SATISFACTORY					⇧
OHIO FIELD OFFICE	SATISFACTORY			N/A		
Mound Plant (EG&G Mound)	MARGINAL ⇩	⇩	⇧	⇩		
ROCKY FLATS OFFICE	MARGINAL ⇩	⇩		N/A		
RICHLAND OPERATIONS OFFICE	SATISFACTORY			N/A		
Fast Flux Test Facility (WHC)	SATISFACTORY					
Plutonium Finishing Plant (WHC)	SATISFACTORY					
SAVANNAH RIVER OPERATIONS OFFICE	SATISFACTORY			N/A		
200-F Separations Area (WSRC)	SATISFACTORY			⇧		
200-H Separations Area (WSRC)	SATISFACTORY					
Reactors Area (WSRC)	SATISFACTORY			⇧		
STRATEGIC PETROLEUM RESERVE PROJECT MANAGEMENT OFFICE	SATISFACTORY			N/A	⇧	

- Marginal

- Unsatisfactory

Improvement since last report: ⇧

Decline since last report: ⇩

Appendix M:

"Verification Assessment Report of the Rocky Flats Environmental Technology Site Safeguards and Security Plan," Department of Energy Internal Memo

July 17, 1998

Verification Assessment Report of the Rocky Flats Environmental Technology Site Safeguards and Security Plan (U). July 17, 1998

p-2. (U) References:

(a) SSSP for RFETS. April 1998.

(b) Memorandum for Hank Dalton, Rocky Flats Field Office, from Edward McCallum, Office of Security Affairs. Subject: Review of the Rocky Flats Environmental Technology Site Safeguards and Security Plan. March 21, 1997

(c) Memorandum for Jessie Roberson, Rocky Flats Field Office, from Joseph Mahaley, office of Security Affairs. Subject Site Safeguards and Security Plan (U). September 25, 1997.

(d) Comprehensive Inspection of Rocky Flats Field Office and the Rocky Flats Environmental Technology Site (RFETS (U). May 1998.

(e) Memorandum of transmittal for EM-62 and NN-513.2, from James Steward, Security Director Rocky Flats Field Office. Subject: 1998 RFETS SSSP. June, 1998, with attachments: SSSP Parts I&II. April 1998.

(U) These reference documents are related to each other in the following ways. The SSSP of April 1998, ref. (a) was received by headquarters OSS for verification and concurrence. During the verification process it was determined that there were vulnerabilities at the site that were not identified or addressed in the 1997 SSSP and that SNM was at risk under the then existing conditions. It was also determined that the upgrades proposed in the 1997 SSSP did not reduce the conditional risk to low. As a result of the verification's findings, a memorandum, ref (b), was prepared and issued in March 1997. Subsequently, an additional memorandum, ref c., was prepared and issued for conditional concurrence by OSS in September 1997. This memorandum provided a period of 120 days to correct identified vulnerabilities with the physical security system and the protective force.

(U) An independent Office of Security Evaluation inspection of RFETS was conducted in April and May of 1998 and documented in a May 1998 report, ref (d). This report mad no mention of reference (b) and (c), even in the areas of management of the protection program and protection of special nuclear materials. Therefore it is not known if OSE was aware of the documented OSS concerns.

(U) Both reference (d) and (e) were written after the period of conditional concurrence had expired. Documentation showing that OSS took follow-up action upon expiration of the conditional concurrence was not provided.

(1)

Appendix N:

Letter from David Ridenour, Director Office of Safegurds and Security to:
Ms. Jessie Roberson, Manager, DOE Rocky Flats Office

March 31, 1997; and

Letter from David Ridenour, Director Office of Safegurds and Security to:
Secretary of Energy Federico Pena

April 16, 1997

The following letters were provided to the Government Accountability Project evidencing security deficiencies at the Rocky Flats Plant. The letters were authored by a former Department of Energy Director of Security at Rocky Flats.

David E. Ridenour
6422 Quartz Circle
Arvada, Co 80007

March 31, 1997

Ms. Jessie Roberson, Manager
DOE Rocky Flats Field Office
P.O. Box 928
Golden, CO 80402-0928

Dear Ms. Roberson:

It is with great regret that I tender to you my resignation from Federal service. Although I have served with the Safeguards and Security Division (SSD) for only a short time, it is plain that my Division and my team are being deliberately prevented from effectively carrying out our mission. That mission is to ensure Special Nuclear Material (SNM), classified and restricted data, and unclassified controlled nuclear information are adequately protected from less or compromise.

The placing of SSD under the Assistant Manager for Material Stabilization and Disposition (AMMSD) is a clear conflict of interest. The key production manager (AMMSD) now controls the Safeguards and Security checks on his own operations. This is the fox watching the hen house.

Two rounds of arbitrary staffing reductions, both in the Federal and in the staff support contractor work force have eliminated my Division's capability to effectively perform the contractor Quality Control/Quality Assurance role. Security Operations oversight of the contractor, Kaiser-Hill, is almost nil. Safeguards oversight (Material Control and Accountability) is only marginally better.

Internal Security (clearances) is deficient $1.9 million in FY'97 funding. Processing is at a halt and rechecks are being arbitrarily extended from 5 to 7 years to maintain operations. If the funding shortfall is addressed, my remaining team members will be overwhelmed by the backlog.

Despite the operational staff shortages in the Rocky Flats Field Office, Assistant Managers have created administrative entourages.

Personal egos and bureaucratic empire building, both at Rocky Flats and within the Department of Energy headquarters, have destroyed the dialog necessary to build a current Site Safeguards and Security Plan (SSSP). This plan is critical to demonstrating effective protection of the SNM at Rocky Flats.

In my professional life as a military officer, as a Registered Professional Engineer and as a technologist

with the contractor operating the Department of Energy's Fernald, Ohio site, I never before experienced a major conflict between loyalty to my supervision and duty to my county and to the public.

I feel that conflict today.

Sincerely;
David E. Ridenour
Director, Safeguards & Security

David E. Ridenour, P.E.
6422 Quartz Circle
Arvada, 9080007

April 16, 1997

Hon. Federico Pena
Secretary of Energy
1000 Independence Ave. SW
Washington. DC 20585

Dear Mr. Pena:

It has been a week since I resigned my position as the Director of the Safeguards and Security Division (SSD) at the Department of Energy (DOE) Rocky Flats Field Office (RFFO) on 04/10/97 due to my concern over the operation of the site and my disgust with the treatment my security team and I were expected to endure. To this date, I have had no contact from the Department of Energy as to the acceptance of that resignation. I have therefore consolidated my concerns with DOE's Rocky Flats Field Office, which as a Mayor of Denver, I know you are knowledgeable of, and those concerns are presented in this letter and the enclosed attachments.

As a Professional Engineer, I have a code of conduct to uphold. Under Rule 1 of the Colorado *Rules of Professional Conduct of The State Board of Registration for Professional Engineers and Professional Land Surveyors* which states: "Registrants shall at all times recognize that their primary obligation is to protect the safety, health, property and welfare of the public," I felt compelled to, pursuant to Rule I.1.A. resign on 04/10/97 from my Federal position. The State of Ohio Code makes my obligation to the public even clearer, stating in 4733-35-03 "where the Engineer...faces a situation where the safety, health and welfare of the public is not protected, he shall: Sever his relationship with his employer or client..." Under the cited Colorado code and rule, I am also obligated to notify "such other authority as may be appropriate." In this case, believe that authority is the Secretary of Energy. Massive reductions in both the Federal and staff support contractor work force at RFFO who are charged with Quality Control/Quality Assurance (QC/QA) of the Safeguards and Security operations of the site contractor, Kaiser-Hill, combined with the active hostility of my supervisor, Henry (deleted), AMMSD, and a proliferation of administrative tasks tied me and my team to our desks and made it impossible for SSD to effectively monitor the contractor's performance of Safeguards and Security functions. The impact of not conducting effective QC/QA is to place at unknown/unquantified risk the safety, health, property and welfare of the public, due to the large quantities of Special Nuclear Material (SNM) held in storage and in process lines at the former

Weapons Complex site.

My repeated requests to AMMSD for relief from administrative overload and for additional knowledgeable Security Systems Engineering personnel to cover oversight of $65 million in active security projects (funded by Congress) for the protection of SNM have gone unheeded by senior management. Instead, I was instructed by my direct supervisor, AMMSD, that my mission was to "not negatively impact the contractor" and that I was to "facilitate the contractor winning award fee." I was also instructed to "accommodate the ego" of my immediate supervisor, AMMSD, by senior DOE Rocky Flats management (Keith Kline, RFFO Deputy Manager). This is a major conflict of interest in that SSD, in ensuring that the proper level safeguards and amount of security is provided, may well negatively impact cost and schedule and that may result in no award fee being won by the contractor.

The attached copy of my resignation letter (dated 03/31/97 but delivered 04/10/97) and two background papers provide additional details.

You should know that the Denver office of the DQE Inspector General also has the information in this package. You or your staff may reach me for any questions on these issues at the above address or at (303) 940-3512.

Sincerely;

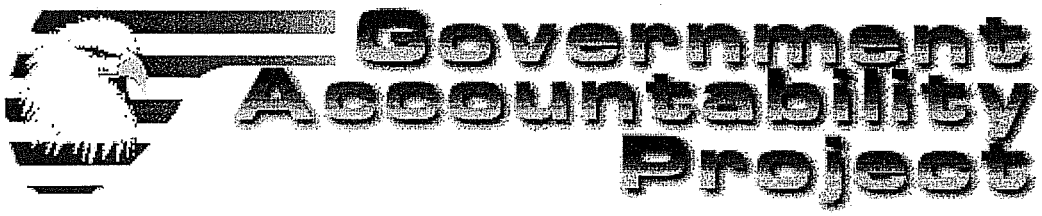
David E. Ridenour,
P.E.

encs.

Appendix O:

Excerpts of Transcript of telephone conversations between Jeffrey Peters, Operational Security Manager, Wackenhut Services, Inc., and Edward J. McCallum, Director Office of Safeguards and Security

May 7 & 8, 1997



Excerpts of Transcript of May 7 & 8 1997

Telephone Conversations

Between Jeff Peters and Ed McCallum

Jeffrey Peters: Former Operational Security Manager, Wackenhut Services, Inc., at the Rocky Flats nuclear site near Denver, Colorado.

Ed McCallum: Director, Office of Safeguards & Security, Department of Energy

Note: The following conversations between Mr. Peters and Mr. McCallum were legally recorded by Mr. Peters from his residence in Colorado. Certain names have been removed to protect privacy or because the conversation was irrelevant or dull. The topic of the conversations focuses on security protection at the government-owned Rocky Flats Environmental Technology Site, a former nuclear weapons production facility near Denver, Colorado. Rocky Flats stores nearly 14 metric tons of weapons-grade plutonium. This transcript is being released to evidence contractor and governmental coverup and wrongdoing, and in support of the claims of Mr. Peters and Mr. Graf, who have contacted various oversight agencies, Congress and the news media in an effort to expose the security deficiencies at Rocky Flats and the ongoing reprisals against those who have dared to raise these concerns. Mark Graf, a Lieutenant with Wackenhut, will be trying his case for discrimination against Wackenhut on April 5, 6 and 7, 1999, in Denver. For more information, follow this link. *In a hurry? Click here for a short version.*

##

[Preliminary attempts at contact deleted]

16 [Ringing]

17 **Ed McCallum:** Hey Jeff.

18 **Jeff Peters:** Hey Ed. How ya been?

19 **Ed McCallum:** (Yells to someone else in background)

20 I'll take that, if it's on the car I'll take

21 that--later on. (Voice in background responds)

22 Later on, tell him I'll call him back. Sorry.

23 Hey long time no, I haven't heard from ya.

24 **Jeff Peters:** Yeah, how ya been?

Jeff Peters: Oh, yeah. I do.

Ed McCallum: I will give -- you've got his number if I -- get hit by a truck before I reach him you oughta' call him if you don't hear from him in the next week.

Jeff Peters: 202-

Ed McCallum: He's, he's writin' a report right now which is pushing for hearings. Now when they do hearings, it's gonna execute me. 'Cause I'm the first name to go in the Department; that's my job as the uh, pressure valve for Congress, so but,but I feel very strongly, I mean, you got Rocky and you also have Livermore in the same condition.

Jeff Peters: I could tell you the situation --

Ed McCallum: And it's going down hill. Um, the annual report I wrote didn't only talk that, it said that we were about $150 million dollars

00022

under-funded, we've lost 42% of our protective forces and 50% of our SWAT --

Jeff Peters: Yes.

Ed McCallum: -- capability. I said that at a time when we've increased our SNM holdings by 70 metric tons.

Jeff Peters: Yes.

Ed McCallum: It doesn't take a brain surgeon to figure this one out.

Jeff Peters: Yeah, I'd like to see your report, 'cause whether, uh, see I've got a lot of documents from the original --

Ed McCallum: I had to leave it lighter than what, in order to get it out unclass I had to lighten things up a lot.

Jeff Peters: Yeah.

Ed McCallum: But it still pissed off DP and EM.

Jeff Peters: Well, sure. Because they're dirty in this. That's what I'm going to say, and I'll say --

Ed McCallum: Let me ask you something on the third Riddenour has not done anything to go public with his letter yet. Is there any news organization, that, that would get into this for (unintelligible).

00023

Jeff Peters: Oh, oh. I could tell you also, that Rick Salinger of Channel 4 here, he's the, I believe it's a CBS local affiliate, they want it real bad. Uh --

Ed McCallum: Do you have a fax machine?

Ed McCallum: Put some HE on top of it and boost it up -- you don't need to take it in the middle of Denver, it's going in the middle of Denver anyway.

Jeff Peters: See.

Ed McCallum: The problem will be down there.

Jeff Peters: Yeah, and now you've got an entire city of a million people plus crapped up -- or take it to New York. That's what I mean. The scenarios are just --

Ed McCallum: See, you don't have to take it off the site based on the what the stuff we've already looked at. You can do it on the site and it'll

00049

be downtown.

Jeff Peters: Yeah, well, they allow you with that new strategy unlimited time in the vault! And there's some scenarios out there that we can't even re-enact when I was there -- you couldn't re-enter the building if you had to. Well, you give the adversary that long with that kind of material, you know the result. That's just --

Ed McCallum: A little mushroom shaped cloud over --

Jeff Peters: [Laughs] Exactly. You don't wanna' -- well, maybe you do wanna' be real close to it. At least it's fast. I think you'd probably rather go fast than the slow residual effects of radiation.

25 letter, it's the fox guarding the hen house. If
00056
1 you're going to be oversight, you should be
2 working for either the Board, the Defense Board,
3 or a direct part of Congress, as far as I'm
4 concerned. Or, like you say, DOD. Somebody
5 outside of the DOE is the whole key here.
6 Because they've shown themselves to be corrupt, I
7 mean, beyond the word.
8 **Ed McCallum:** Oh, yeah.
9 **Jeff Peters:** And -- when it -- again, when it comes
10 back to the results that we're talking about.
11 Again, if it was like you said yesterday,
12 pencils -- if we were making pencils, who cares,
13 really.
14 **Ed McCallum:** Yeah.
15 **Jeff Peters:** But not when you're risking nuclear
16 catastrophe.
17 **Ed McCallum:** Well, that's --
18 **Jeff Peters:** No.
19 **Ed McCallum:** I've said in front of the Deputy
20 Secretary and people at that level, I think the
21 citizens, the employees at the plant, and the
22 citizens of Colorado are at extremely high risk
23 for no reason.
24 **Jeff Peters:** And I'm going to the public, I'm going
25 to tell the media that. And I'm going to tell
00057

Appendix P:

Letter from Glenn S. Podonsky, Office of Independent Oversight to: J. Owendoff, Acting Assistant Secretary for Environmental Management, EM-1 & Jessie Roberson, Manager Rocky Flats Field Office

May 14, 1998

Department of Energy
Germantown, MD 20874-1290

May 14, 1998

MEMORANDUM FOR: J. Owendoff, Acting Assistant Secretary for Environmental Management, EM-1
Jessie M. Roberson, Manager, Rocky Flats Field Office

FROM: Glenn S. Podonsky, EH-2

SUBJECT: Transmittal of Draft Safeguards and Security Comprehensive Inspection Report of the Rocky Flats Field Office/Rocky Flats Environmental Technology Site

The Office of Oversight conducted a comprehensive inspection of the Rocky Flats Field Office (RFFO) and the Rocky Flats Environmental Technology Site (RFETS) from April 27 - May 15, 1998. The inspection was conducted to assess the effectiveness of safeguards and security programs that provide protection for RFETS security interests.

Inspection results revealed that great progress has been made in instituting a sound system to manage RFETS's protection programs. RFFO and Kaiser Hill safeguards and security staff now provide an effective means for line management to fulfill their safeguards and security responsibilities. Nevertheless, the protection program elements measured during this inspection do not indicate that a fully effective program is yet in place. As evidenced by deficiencies identified in some areas of physical security systems, material control and accountability, computer security, and classified matter protection and control, there remain a number of legacy safeguards and security issues to be resolved. In addition, new issues have arisen. Additional management attention and emphasis will be required to address these issues and to maintain adequate levels of protection for SNM and classified/sensitive information. Such attention becomes particularly important in light of potentially conflicting operational priorities and in the event that current projected facility closure deadlines cannot be met.

The following ratings were assigned:

Safeguards and Security Management Programs:	Needs Improvement
[redacted]	[redacted]ce
Protection of Information:	Needs Improvement

Consistent with DOE Order 5630.12A, Safeguards and Security Inspection and Assessment Program, please provide to my office by May 29, 1998, any interim corrective actions taken and/or planned to correct the identified deficiencies.

By the same date and separate memorandum, please provide any comments on the factual accuracy of the draft report to this office so that corrections can be incorporated as appropriate. Please refer any questions to me (301 903-3777), or Barbara R. Stone, Director, Office of Security Evaluations (301 903-5895).

Barbara R. Stone for

Glenn S. Podonsky
Deputy Assistant Secretary for Oversight
Environment, Safety and Health

Attachment:
Draft Inspection Report (S/NSI)

cc w/attachment:
P. Brush, Acting EH-1
T. Todd, FM-1
A. Durham, HR-1
E. Curran, CN-1
R. Gottemoeller, NN-1
J. Mahaley, NN-50

Appendix Q:

"Comprehensive Inspection of Rocky Flats Filed [sic] Office and the Rocky Flats Environmental Technology Site (U)," Department of Energy Internal Memo

May 1998

Comprehensive Inspection of Rocky Flats Filed Office and the Rocky Flats Environmental Technology Site (U), May 1998.

p-2. (U) The purpose of the inspection was to assess the effectiveness of protection afforded various RFETS security interests and to report the results of that evaluation to appropriate DOE management. Large scale performance tests were conducted using Department of Defense (DoD) assets to play the role of the adversary force – apart of the Secretary of Energy's initiative to improve safeguards and security at the Department's critical facilities.

p-8 (U) Protection program management has been a long standing weakness at Rocky Flats. SE rated the topic Unsatisfactory in 1991, and Marginal in 1992 and 1994. While the 1996 SE inspection of RFETS was not rated, weaknesses in protection program management were evident. RFFO security surveys and K-H self-assessment have also rated protection program management less than satisfactory. In general, these ratings have reflected not only weaknesses in the RFETS safeguards and security staffs, but also a lack of support for safeguards and security by RFETS line managers, the actions of Headquarters offices, and some safeguards and security policy weaknesses. A consistent trend prior to 1996 was that at the time of each of inspection, a number of newly implemented plans were expected (by RFETS) to greatly improve the safeguards and security program, but these plans had not sufficiently matured for SE to evaluate their worth. In each case, subsequent evaluations showed that these plans had not been fully implemented or had proven effective.

p-10 (U) The second issue affects the SSSP at RFETS. EM and DP in a July 30, 1997 memorandum, have jointly directed their sites to accept only part of the most recent Design Basis Threat and to employ the consequence values provided in the 1989 SSSP Planning Guide rather than the 1996 SSSP Format and Content Guide. Interviews disclosed that this memorandum is applicable to the 1998 update of the RFETS SSSP. This joint guidance reduces the threat that RFETS is required to respond to, reduce the consequence values to be used in calculating risk of theft of Category II SNM, and eliminated the consideration of on-site consequence for radiological sabotage. Further, ion promulgating this guidance EM and DP have assumed the role of setting DOE safeguards and security policy – a role assigned to NN by DOE order. Interviews with NN personnel responsible for the DBT Policy were unaware that the EM and DP memorandum was still in force.

"...Protection is adequate by a narrow margin.".

"Overall, the RFETS protection program is finely balanced between success and failure."

(1)

p-5 (U) OSE force on force scenario 4 (ref.(d) p-63, similar in nature to scenario 2 resulted in 15 protective force casualties. This casualty total exceeds the margin of prudence for protective force effectiveness necessary in an actual armed conflict. Therefore, scenario 4 is a qualified loss.

(U) OSE force on force scenarios 1 and 3 were not worst case scenarios. The protection effectiveness of any site's plant protection operations is not judged against just any scenario. Rather, it is judged against those scenarios that credible stress the system in the worst case. For example, five poorly prepared and trained adversaries with no element of surprise do not represent the design basis threat scenario. While the OSE rationale for conducting some of the force enforce performance testing using less than worst case scenarios is unknown, the tests may have meaningful data for purposed other that validating the protection effectiveness.

(U) In addition to the scenario issues described above, the OSE inspection found:

- All four scenarios, based on surprise, were initiated prematurely. "Lack of surprise, favored the protective force," ref (d) p-56.
- "Some protective force members clearly had difficulty distinguishing fried from foe" ref (d) p-66.
- "On at least one occasion, and possible on additional occasions, protective force members intentionally fired at unarmed individual who exhibited no indication of being adversaries or of posing a threat" ref (d) p-66.
- "The protective force was not fully prepared to effectively deal with some of the tactics and weapons used by the adversaries in these scenarios" ref (d) p-66.

p-8 (U) The protection effectiveness and determination of risk is measured against worst case scenarios not lesser cases. The set of scenarios considered in the 1997 and 1998 SSSPs was extensive and reduced to the set of worst case scenarios. This lack of focus on worst case scenarios was also evident in the force on force testing performed during the OSE inspection. Two of the OSE scenarios (scenarios 1 and scenario 3) were either lesser cases that scenarios 2 and 4 or were tested against facilities that were more difficult to attack or escape from. If the plant protection operations cannot defeat the worst case threat and scenario(s), then the assets are at risk.

p-10 (U) Several issues create the basic problems which are inhibiting the correction of the continued high risk at RFETS. These issues are: (1) the lack of development of worst case scenarios and plant protection operation upgrades which address the vulnerabilities from a systematic top-down method, and (2) the inability of the SSSP configuration control to adequately address pointed observations and issues developed by other responsible organizations.

Appendix R:

Testimony of Peter D. H. Stockton, DOE Special Assistant, U.S. District Court, Colorado, Civil Action No. 97-WM-2191, U.S., ex rel., David Ridenour et al. v. Kaiser-Hill Company

July 2001

This testimony was witnessed and cleared by a Department of Energy classifier to ensure that no classified information was revealed.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 97-WM-2191

UNITED STATES OF AMERICA, ex rel., DAVID RIDENOUR, et al.

Plaintiffs,

v.

KAISER-HILL COMPANY, L.L.C., et al.

Defendants.

RECOMMENDATION OF UNITED STATES MAGISTRATE JUDGE

Patricia A. Coan, United States Magistrate Judge

This is a qui tam action under the False Claims Act. The matter before the court is the United States' Motion to Dismiss [filed August 21, 2000]. An Order of Reference under 28 U.S.C. §636(b)(1)(A) and (B) referred this case to the undersigned magistrate judge on April 6, 2000 to issue recommendations on dispositive motions.

I.

The False Claims Act ("FCA" or "Act"), 31 U.S.C. §3729 and §3730, as amended by the False Claims Amendments Act, Pub.L. 99-562, 100 Stat. 3153 (1986), empowers the United States ("Government") or a private person to bring a civil action against a person or company who knowingly presents a false claim to the Government for payment, in violation of 31 U.S.C. §3729(a). 31 U.S.C. §3730(a) and (b)(1). The private citizen who brings an action under §3730(b)(1), the "relator," sues on behalf of himself and the United

The United States Exhibits T, as in Tom; M, as in Mary; H, U, G2, G3, and G4, K, and L have been admitted.

Kaiser-Hill's Exhibit 3 has been admitted.

So I think we left off the relators -- with the relators' last witness, so we need another witness on the relators' side.

PETER STOCKTON,

called as a witness on behalf of the plaintiffs-relators, having been first duly sworn, was examined and testified as follows:

THE COURT: Please take a seat and state your name. Your name, please.

THE WITNESS: What? Oh. Peter Stockton.

THE COURT: You may inquire.

DIRECT EXAMINATION

BY MS. BROWN:

Q. Good morning, Mr. Stockton.

A. Good morning.

Q. Would you briefly tell the Court your educational background.

A. You have to speak up because I'm marginally deaf.

Q. Would you briefly --

misled about the fence. I can't tell you why. Now --

UNIDENTIFIED FEMALE SPEAKER: I'm going to object --

MR. WILLIAMSON: Objection, Your Honor. How am I supposed to cross this witness? This is a classified issue that he's now discussing that he's been misled --

THE WITNESS: No, it's not a classified issued. We've just talked about this.

MS. BROWN: I would suggest letting the witness finish his answer, if your question is how you're going to cross-examine him, to sigh what the answer is.

THE COURT: Right. And the relationship to DOE, just the event and then what happened as a result of the event.

MS. BROWN: Which is what the question was.

Q. (By Ms. Brown) Continue, Mr. --

A. The second issue involved material outside of an authorized area that was in process and there were no compensatory measures taken. We were told at first that this -- this was not going on. We finally -- after a period of time, they admitted that it went on for a minimal amount of time, maybe two hours a week. Then after about four hours of going round and round with them, they finally admitted that it went on five days a week,

eight hours a day. And as a result of this, the securities are to send a team to -- at Richardson's direction to Rocky Flats. The team was down here off and on about six months getting the thing straightened out.

Q. If I might, Mr. Stockton, to just --

MS. ZIRKELBACH: Just -- excuse me. I'll have to move to strike that answer for the reasons that we've been articulating. I can't cross-examine him about it. I can't say, what was the problem -- the alleged problem with the fence, how were you misled by it. I can't ask him where this material supposedly existed, what compensatory measures were -- he was told existed but in fact didn't, what other compensatory measures could have been implemented, et cetera.

So now we've got this evidence in that has to do with these two alleged deficiencies and I can't do anything with it, and I don't think that's really fair to the defendants.

THE COURT: I'm going to allow the answer as background to the relators' theory that there was some sort of cover-up which relates to the dismissal and allow it only for that purpose.

MS. BROWN: Thank you, Your Honor. May I continue?

Appendix S:

Letter from Representative John D. Dingell, Ranking Member, House Commerce Committee to: former Senator Warren Rudman, President's Foreign Intelligence Advisory Board

March 24, 1999; and

Statement of Representative John D. Dingell at the Joint Hearing of the Commerce Committee Energy and Power Subcommittee & the Science Committee Energy and Environment Subcommittee on Restructuring the Department of Energy

July 13, 1999

Text only of letters sent from the Commerce Committee Democrats.

March 24, 1999

The Honorable Warren Rudman
President's Foreign Intelligence Advisory Board
Room 340, Old Executive Office Building
Washington, D.C. 20502

Dear Warren:

First, let me congratulate you on your recent appointment to lead the bipartisan review of security threats to the U.S. nuclear weapons laboratories over the last twenty years. I am hopeful that your review will finally focus appropriate attention on a very serious and longstanding problem that has been ignored, mismanaged, and/or covered up during several Administrations. Unfortunately, your effort is only the latest in a long line of reviews undertaken by, among others, the General Accounting Office (GAO), the Department of Energy (DOE) and its Inspector General, the U.S. Nuclear Command and Control System Support Staff, and various Congressional committees, the results of which have been uniformly ignored by the responsible officials.

I am also writing to offer you my assistance as you undertake this review. During my 14-year tenure as chairman, the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce conducted several classified and unclassified inquiries into this matter. (This letter discusses the unclassified portion of our work.) We found a disturbing pattern of security weaknesses in the contractor-run national weapons laboratories, along with extraordinarily lax oversight by the Department of Energy (DOE). As you may already know, these problems included: laboratories refusing to implement basic security precautions; DOE Secretaries and other officials ignoring repeated warnings of security problems; and bureaucratic obfuscation of the problems that meant that even the National Security Council and the President received inaccurate, misleading information. Although our main focus initially was terrorism and physical security, our concerns soon broadened to encompass other significant security deficiencies and the system's management problems.

The Subcommittee, on a bipartisan basis, sought continuously to bring these problems to light, and to fix the underlying weaknesses, such as the lack of independent security oversight, that allowed problems to persist. This work required a sustained effort over several years, work made more difficult because of the recalcitrance of the contractors running the national laboratories. You should expect significant difficulties in arriving at a full understanding of the problems, particularly if, given your tight deadline, you are forced to rely on those contractors and government officials responsible for managing the laboratories over the last twenty years.

The Subcommittee's work on this matter began in 1981 in response to efforts to undermine independent review of security threats. The Department of Energy's Assistant Secretary of Energy for Defense Programs had become concerned in 1979 about the level of security at the weapons laboratories. As recommended by the General Accounting Office (GAO) in 1977, and also the Inspector General, he established an independent, inter-agency group that reported directly to him on the adequacy of safeguards at these facilities. This program employed some of the best experts in the country in terrorism, sabotage, protection of classified material and related activities. This group found that the safeguards at the most critical facilities – which included Los Alamos – were in shambles while, at the same time, DOE's Office of Safeguards and Security was giving the facilities a clean bill of health.

However, in 1981, when a new Administration took over, the Assistant Secretary was replaced

by a high-ranking official from Los Alamos National Laboratory who immediately shut down the independent assessments program. In 1982, in a classified report to the Subcommittee, GAO strongly recommended (in part because DOE was submitting misleading reports to the National Security Council) the reinstitution of an independent assessment program which would report directly to the Under Secretary of the DOE. Two hearings by the Subcommittee in 1982 and 1983 focused on the organizational problems at DOE and the GAO recommendation. In 1983, the Committee adopted, with strong bipartisan support, an amendment to the DOE Defense Authorization bill establishing an independent Office of Safeguards Evaluation reporting directly to the Secretary. Unfortunately, the bill never received floor consideration.

Attempts by the Subcommittee and others in 1983-84 to establish an independent evaluations office within DOE were turned down by the Secretary and the Assistant Secretary for Defense Programs, who wanted the evaluations program under his control. Independence was critical because, during the Subcommittee's work, top officials misled the Subcommittee and harassed a DOE whistleblower. In 1984, the Subcommittee held a hearing on the Department's attempts to strip the employee's security clearance and issued a report. The Department rewarded the harassers with promotions, bonuses and medals. In 1984, the Department also terminated an investigation by its Inspector General into management adequacy in the safeguards and security program.

The Subcommittee also attempted to alert President Reagan to its concerns. In 1984, however, DOE officials told the President there was nothing to be concerned about. In January 1986, prior to his briefing by DOE on the status of safeguards and security, I wrote a letter to President Reagan listing general problem areas. These included: credibility of the inspection and evaluation program; inadequately trained guard forces; inadequate protection against insider threats; inability to track and recover special nuclear materials and weapons if they were stolen; inadequate protection of classified information; inverse reward and punishment system for the contractors; and lack of funding for safeguards and security upgrades. (A copy of that letter is enclosed.) In response, based on information provided by the national laboratories and DOE officials, Secretary of Energy Herrington wrote of "significant progress" and "improvements," and Admiral Poindexter said he was "impressed with the progress being made."

The Subcommittee continued its work during President Bush's Administration. Among other matters, it looked at inadequate personnel security clearance practices at the laboratories where it was immediately clear that there were inadequate resources to do an effective job. That situation has not changed to this day. The Subcommittee also began to review the foreign visitors program -- as did Senator Glenn, then chair of the Senate Governmental Affairs Committee -- and the mysterious shutdown of an investigation into drug problems and property controls at Lawrence Livermore Laboratory

At the same time, Secretary Watkins' Safeguards and Security Task Force recommended establishing independent oversight functions which would report directly to the Under Secretary. Once again, the recommendation was not implemented, although Secretary Watkins did move the Office of Security Evaluation out from under Defense Programs.

In 1991, the Subcommittee also reviewed the role the Department may have played in allowing Iraq to augment its nuclear capability. In May of 1989, DOE employees attempted to alert Secretary Watkins to the fact that Iraq was shopping for strategic nuclear technologies. They were not allowed to brief the Secretary. But in August of 1989, three Iraqi scientists attended the "Ninth Symposium (International) on Detonation" sponsored by the three weapons labs, the Army, Navy, and the Air Force. It was described by a DOE official as the place to be "if you were a potential nuclear weapons proliferant." At the time, DOE didn't even have a nonproliferation policy, and Secretary Watkins was not briefed on the Iraqi threat until May of 1990.

In 1991 and 1992, the Subcommittee received six GAO reports critical of DOE's safeguards and security efforts. These covered weaknesses in correcting discovered deficiencies, incomplete safeguards and security plans, weak internal controls, unreliable data on remedial efforts, inadequate accountability for classified documents, and security force weaknesses. Two other GAO reports noted that even basic control measures for non-classified property were not in place at the Lawrence Livermore National Laboratory, nor was DOE oversight adequate.

Subcommittee staff met with Secretary O'Leary and her senior staff in 1993 to outline these concerns. At the time of the Republican takeover of the House in January 1995, when my chairmanship ended, the problems had not gone away, and recent GAO reports find little, if any, improvements. In March of 1998, the U.S. Nuclear Command and Control System Support Staff, an independent, federal-level organization chartered by Presidential Directive to assess and monitor all equipment, facilities, communications, personnel and procedures used by the federal government in support of nuclear weapons operations, recommended once again a high-level, independent office to review safeguards and security at DOE.

Many of us in the Congress have tried for years to address the chronic problems at DOE's national laboratories. You now have the opportunity to take an independent, comprehensive, and bipartisan look at these security weaknesses. Independence from those who have failed to solve these problems – which includes officials at DOE and representatives of the laboratory contractors who implement and establish policies at the labs as if they are academic researchers, not the guardians of our weapons secrets – is essential for your review to accomplish more than the prior reviews. Similarly, the independence of any future evaluations office will be essential to any lasting progress.

Your review will not be easy work, but I stand ready to help.

With every good wish.

Sincerely,

JOHN D. DINGELL
RANKING MEMBER

Enclosure

cc:
The Honorable Tom Bliley, Chairman
Committee on Commerce

The Honorable Bill Richardson, Secretary
U.S. Department of Energy

Statement of
the Honorable John D. Dingell
at the Joint Hearing
of the
Commerce Committee Energy and Power Subcommittee
& the Science Committee Energy and Environment Subcommittee
on Restructuring the Department of Energy

July 13, 1999

I want to thank the Chairmen for holding this hearing today. The gravity of this issue is underscored by our Committees joining together on a bipartisan basis to try to address the very serious security and management problems at the Department of Energy. This is a subject with which I am all too familiar. The problems we are discussing today are the very same ones that this Committee has been trying to correct for well over a decade: the lack of security at our weapons facilities, problems in security clearances, the handling of classified information, and the foreign visitors program.

The recent report by Senator Warren Rudman and the President's Foreign Intelligence Advisory Board unfortunately confirms that the Department of Energy, as currently organized, cannot adequately protect our nation's most prized nuclear secrets. It documents security lapses over the past several decades in a clear and comprehensive fashion. No one familiar with DOE disagrees that the current management structure needs to be vastly reformed to ensure it meets the highest standards of accountability.

For precisely these reasons, I am gravely concerned about recent proposals to elevate the Department's dysfunctional weapons bureaucracy to the status of an almost completely autonomous agency. Chairman Bliley, many of my Democratic and Republican colleagues, and I share concerns about current legislative efforts to establish such an agency in charge of nuclear weapons, for the reasons described in the Rudman Report. We are concerned that the same bureaucrats, who have refused to implement President Clinton's recent security order and who resisted reform efforts by both the Bush and Clinton Administrations, would be running this agency, with even greater latitude and far less oversight than is currently in place.

Allowing these proposals to become law would be tantamount to using gasoline to extinguish a fire. In every investigation concerning problems at the DOE weapons facilities and laboratories, the individuals responsible for the operation of defense programs consistently and repeatedly denied the problems, punished the whistle blowers, and covered up the problems to their superiors and Congress. Proposals to set up a fully or semi-autonomous agency would only reinforce this pattern of behavior by insulating these programs from outside scrutiny and accountability. The only beneficiaries of such a proposal would be the weapons bureaucracy at DOE. This would indeed be a remarkable act of political *jujitsu* where the very institutions responsible for the security problems at DOE would emerge from scandal not merely intact, but even more powerful and autonomous than before.

These proposals also "solve" far more than the security problems raised by the Rudman report. They have become magnets for all manner of unrelated concerns. If we want to solve security problems, then that's what we should do. A separate security agency within DOE may make sense, but a separate weapons bureaucracy will make new problems and compound old ones.

One particularly dangerous, extraneous idea is to give the new agency the power to implement and oversee regulations relating to health, safety, and environmental protection. This is utter foolishness and it threatens the well being of communities that host these facilities, because in the absence of oversight, history has showed us that these weapons facilities will flout environment, health and safety regulations and then cover up their misdeeds.

For example, in a 10 year period, beginning in 1974, the Department of Energy disposed of some of its radioactive and chemically contaminated waste by spreading it on the ground at its Piketon, Ohio facility and then rototilling it into the soil.

In 1984, when a malfunction at another DOE facility caused radioactive dust to be released into the air, the response at the facility was to recalibrate the warning system so that the releases would no longer trigger an alarm.

These are only two examples, but they are part of a pattern well known by those who have lived near DOE's Hanford, Rocky Flats, Savannah River or other sites in the days when these programs were shielded from oversight by the Department's environment, health and safety officials.

This danger is also recognized by Senator Rudman who appeared before the full Commerce Committee just a few weeks ago and said in no uncertain terms that he opposed giving this new agency the environment, health and safety functions currently vested in other parts of the Department.

I very much want to work with my colleagues on both sides of the aisle, on these committees and others, to truly address the problems at the Department of Energy. But these are longstanding problems that cannot be addressed with simple solutions. The addition of a new agency or undersecretary may be a fine place to begin, if it is done correctly, but we can never hope to solve these problems without addressing fundamental problems in the DOE culture and the Department's relationships with its contractors. Unfortunately, the proposals to date are not even inept simple solutions. They are dangerous proposals that threaten to undue all the good work done by our Committees and the Bush and Clinton Administrations to make DOE a safer place for its workers and those who host its facilities.

Prepared by the Democratic staff of the Commerce Committee
2322 Rayburn House Office Building, Washington, DC 20515
Select Feedback to let us know what you think.

Back to the Commerce Committee Democrats Home Page

Appendix T:

"Debate Widens Over Most Effective Way to Secure Energy Department's Los Alamos Nuclear Site," John J. Fialka, *Wall Street Journal*

March 15, 2000

Debate Widens Over Most Effective Way to Secure Energy Department's Los Alamos Nuclear Site

By JOHN J. FIALKA
Staff Reporter of THE WALL STREET JOURNAL

LOS ALAMOS, N.M.—In the midnight darkness of April 12, 1997, a secret war game was played out in a canyon here that illustrated the weakness of one of the most heavily guarded places at this nuclear-weapons laboratory.

A small team of elite Army Special Forces commandos, playing the role of terrorists, surprised and quickly overwhelmed the lab's guard force. Running among the dozen buildings in the compound—protected by guard towers, a high fence topped with razor wire and electronic motion detectors—the invaders reached the simulated objective of the game: enough nuclear material to make an atom bomb.

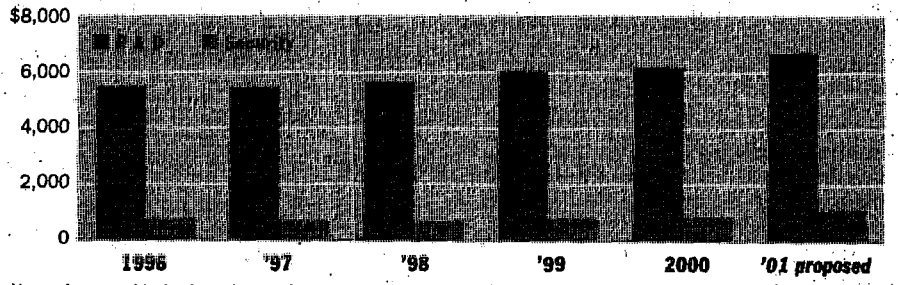
While public attention has been focused on allegations of spying of nuclear-weapons secrets from Los Alamos, the exercise provides a vivid example of a lesser-known security nightmare. There is a growing internal debate over how to protect the Department of Energy lab's aging facilities against the theft of its rich stock of atomic-bomb materials.

In the 1997 test, the final line of defense in the facility, known as Technical Area 18, were the canisters containing portable amounts of plutonium and highly enriched uranium that are regularly handled here. They were purposely made too heavy for an attacker to run off with. The "terrorists" ran off with some anyway, wheeling the material into the woods using equipment the defenders hadn't anticipated—a garden cart.

Though the Energy Department says it has moved to shore up safeguards, the exercise that some agency security planners soberly refer to as "Garden Cart" is a reminder of the challenges.

Nuclear Security

Department of Energy Research and Development budget and Safeguards and Security budget, in millions of dollars



NOTE: Agencywide budget figures for safeguards and security before 2001 are estimated because they were not centrally kept until this year.

Source: DOE

The department spends $700 million a year for security, but the job of defending some of the agency's most sensitive installations is becoming more risky and expensive as Cold War-era buildings age and as urban sprawl makes facilities more accessible. A public road now runs alongside TA-18, which was picked for its remoteness in 1944. The road must be closed each time technicians hold dangerous "criticality" experiments using remote controls to generate radiation from chain reactions.

The 1997 mock invasion succeeded despite months of guard training and dozens of computerized battle simulations showing that newly beefed-up defenders of the facility would win. "The exercise had a very bad outcome, and they learned," says Houston "Terry" Hawkins, the lab official who oversees TA-18 and antiterrorist-related activities.

Gen. Eugene Habiger, the Energy Department's new director of security operations, has visited TA-18 twice and finds it "very difficult to defend" because it sits on the floor of a canyon surrounded by high, unguarded foothills. After a department analysis showed the security requirements of TA-18 absorbed $18 million a year to protect $3 million to $5 million of research, Gen. Habiger began pushing a two-year-old plan to move TA-18 to a fortress-like complex in Nevada. (The lab maintains research and security costs at TA-18 are about the same: $12 million each.)

The department spent $100 million to build the Nevada complex, called the Device Assembly Facility, in the early 1990s as a secure place for the final assembly of nuclear weapons to be tested at the site. Since the U.S. abandoned such testing in 1992, the complex sits largely unused. Gen. Habiger and other security planners argue that its state-of-the-art defenses and its flat, remote location—where outsiders can be seen coming for miles—would make the job of protecting TA-18 less stressful and much cheaper.

But the department is still weighing the move. "There are very critical programs in that facility," says Ernest Moniz, undersecretary of energy. "We just can't afford to turn them off for a few years." Also, the TA-18's skilled technicians are among the handful of people in the world who know how to handle nuclear weapons materials safely, and some aren't anxious to move.

Mr. Hawkins adds that if a nuclear weapon is damaged in transit or if a terrorist group brandishes a nuclear weapon, the U.S. response teams will be guided by the technicians here. The exact configuration of uranium or plutonium used in nuclear weapons determines whether it is safe to handle.

To figure out how a weapon disfigured in an accident or a makeshift terrorist weapon should be dealt with, the experts in TA-18 would use their assortment of different-size pieces of the sensitive metals to model it. "When you get the wrong shape, that thing goes tick-tick-tick-tick-tick," explains Mr. Hawkins, referring to a Geiger counter. "We want to make sure that doesn't happen." In scientific terms, putting the metals in the wrong shape initiates a chain reaction that could emit a lethal burst of radiation to people nearby. The experts here call it "going critical."

Meantime, DOE officials say more recent exercises show the security loopholes here have been plugged. This has been done largely by adding more guards, some of whom can be seen patrolling in armor-plated Humvees topped with .50-caliber machine guns. "You can never have enough security," says Brig. Gen. Thomas Gioconda, acting head of the department's defense-related programs, "but you also have to run a program."

Security exercises are governed by what Gen. Gioconda and others describe as "the threat," a secret level of preparedness that is periodically reassessed. "The threat" was markedly upgraded during the early 1990s when Soviet weapons and mercenaries began to reach terrorist groups.

To assure that its guard forces could cope, DOE began using Army Special Forces units as simulated attackers, plus an Army method of war gaming that tends to deter cheating. It uses lasers, mounted on rifles and other weapons that register "kills" on special receivers worn by soldiers.

Referees remove "killed" soldiers from the fray. They enforce safety precautions to assure that guards and attackers remove real ammunition from their weapons before the "force-on-force" exercises begin. A tragedy occurred here in December 1995, according to Scott Gibbs, a laboratory program director, when a guard forgot to remove his ammunition and shot another guard, playing the role of attacker.

The 1997 exercise came after another reassessment of the threat, he says. Because more powerful weapons used by attackers could quickly eliminate guards in watch towers, the laboratory decided to abandon the towers and depend on highly mobile teams of guards to respond to an attack.

The Garden Cart attackers, however, used snipers hidden in the hills to "kill" the first guards who arrived. Because they happened to be the commanders of the guard force, the rest of the force was thrown into disarray. Many of them also were "killed" as they arrived in small groups down a narrow road leading into TA-18. "[The Special Forces] took them out piecemeal as they came in," says one participant in the game, whose account wasn't challenged by DOE or lab officials.

Despite the mock security breach, Glenn Podonsky, director of the DOE's office of independent oversight, notes that, in reality, no U.S. nuclear facility has been attacked in more than 50 years. "The fact of the matter is that it's never occurred, and I can only conclude that is because we are a very difficult target."

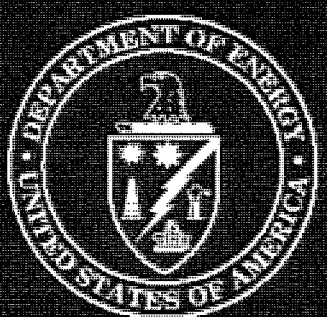
Appendix U:

"Summary Report on Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self-Assessments at Los Alamos National Laboratory," U.S. Department of Energy Office of Inspector General

May 2000

DOE/IG-0471

INSPECTION REPORT



U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF INSPECTIONS

SUMMARY REPORT ON INSPECTION OF ALLEGATIONS RELATING TO THE ALBUQUERQUE OPERATIONS OFFICE SECURITY SURVEY PROCESS AND THE SECURITY OPERATIONS' SELF-ASSESSMENTS AT LOS ALAMOS NATIONAL LABORATORY

MAY 2000

Department of Energy
Washington, DC 20585

May 30, 2000

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (signed)
Inspector General

SUBJECT: INFORMATION: Summary Report on "Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self-Assessments at Los Alamos National Laboratory"

BACKGROUND

The Office of Inspector General received allegations regarding the conduct of security reviews at the Department of Energy's (DOE) Los Alamos National Laboratory (LANL). Specifically, it was alleged that DOE Albuquerque Operations Office (Albuquerque) management changed the ratings of annual Security Surveys of LANL security operations after members of the Albuquerque Security Survey team completed the survey. It was also alleged that LANL Security Operations Division personnel were pressured by their managers to change or mitigate findings in LANL Self-Assessment reports.

RESULTS OF INSPECTION

Regarding the Albuquerque Security Surveys of LANL Security Operations, we found that:

- Albuquerque management changed ratings for the 1998 and 1999 surveys without providing a documented rationale for the changes;
- Albuquerque management did not fully address concerns about a compromise of force-on-force exercise during the 1998 Albuquerque Security Survey at LANL; and
- The 1997 and some 1998 Albuquerque Security Survey work papers were destroyed contrary to Albuquerque policy on the destruction of records. As a result, there was no complete record to show how ratings were developed by the survey teams.

Regarding the LANL Security Operations' Self-Assessments reports, we found that:

- Approximately 30 percent of the LANL Security Operations Division personnel interviewed, who had been involved in the conduct of self-assessments, believed they had been pressured to change or "mitigate" security self-assessments;

- Some security self-assessments required by LANL procedures were not being conducted; and

- DOE's Los Alamos Area Office security staff was not performing all of the oversight responsibilities associated with the LANL Security Operations Division programs.

We concluded that the processes used to develop the Albuquerque security surveys of the LANL security operations and the LANL self-assessments were inadequate. As a result, there are legitimate concerns that the overall security condition at LANL, specifically for Fiscal Years 1998 and 1999, was not being accurately reported.

We provided management with a number of recommendations that, if implemented, would improve the effectiveness of Albuquerque security surveys and LANL self-assessments.

MANAGEMENT REACTION

Albuquerque management stated that the facts presented and the conclusions reached were accurate, and that the recommendations were appropriate. Albuquerque management stated that they would take corrective action.

Due to the concerns identified during our inspection, we recommended that the Department review these operations at other facilities. Specifically, we requested that the Director, Office of Security and Emergency Operations evaluate self-assessment programs at other DOE facilities to determine if they have been fully implemented and adequately represent security conditions. The Director agreed to this recommendation.

Attachment

cc: Deputy Secretary
Under Secretary
Acting Under Secretary for Nuclear Security/Administrator for Nuclear Security
Director, Office of Security and Emergency Operations
Manager, Albuquerque Operations Office

SUMMARY REPORT ON INSPECTION OF ALLEGATIONS RELATING TO THE ALBUQUERQUE OPERATIONS OFFICE SECURITY SURVEY PROCESS AND THE SECURITY OPERATIONS' SELF-ASSESSMENTS AT LOS ALAMOS NATIONAL LABORATORY

TABLE OF CONTENTS

Overview

Introduction and Objectives

The Office of the Inspector General received information from two complainants relating to security reviews at the Department of Energy's (DOE) Los Alamos National Laboratory (LANL). LANL is operated by the University of California under contract with DOE. One complainant alleged that managers of DOE's Albuquerque Operations Office (Albuquerque) Safeguards and Security Division, changed the ratings of periodic (annual) Security Surveys of LANL security operations after members of the Albuquerque Security Survey team completed the survey. Specifically, it was alleged that the Security Division managers upgraded survey ratings that were "Marginal" or "Unsatisfactory" as a result of "deals struck" between Albuquerque and LANL management officials. The second complainant alleged that LANL Security Operations Division personnel were pressured by their managers to change or mitigate self-assessment findings in LANL Self-Assessment reports. Both complainants alleged that the Albuquerque Security Survey reports at LANL and the LANL Self-Assessment reports did not clearly reflect the overall security conditions found by the survey field reviewers.

The objectives of our inspection were to determine: 1) if Albuquerque Security managers changed Albuquerque Security Survey ratings of LANL Security Operations; 2) if there was a basis for these changes; and, 3) if LANL Security Operations Division management had pressured its staff to alter self-assessment reports. This inspection did not include an evaluation of the overall security conditions at LANL.

During the course of this inspection, a number of individuals requested confidentiality. They indicated they feared retaliation for disclosing information to the Office of Inspector General (OIG).

Observations and Conclusions

We concluded that the processes used to develop the Albuquerque Security Surveys of the LANL Security Operations and the LANL Self-Assessments have raised legitimate concerns that the overall security condition at LANL was not being accurately reported.

Details of Findings

Details of Findings

In order to ensure compliance with DOE requirements,[1] the Albuquerque Safeguards and Security Division conducts annual security surveys of LANL Security Operations. The topical areas evaluated during these surveys include: Program Management, Protection Program Operations, Information Security, Nuclear Materials Control and Accountability, and Personnel Security. Each topical area also has several sub-topical areas. The Albuquerque Operations Office assigns ratings of "unsatisfactory," "marginal," or "satisfactory" based on conditions existing at the end of survey activities. A complete listing of the topical and sub-topical areas is provided at Appendix C.

Changes to Security Survey Ratings

Our inspection found that Albuquerque management changed ratings for the 1998 and 1999 Albuquerque Security Surveys of LANL Security Operations after the Survey Teams had assigned them. During the 1998 Albuquerque Security Survey at LANL, Albuquerque management upgraded several topic area survey ratings, and most importantly, the overall composite rating.[2] The OIG was told that had Albuquerque management not upgraded the topical and sub-topical ratings in the Nuclear Materials Control and Accountability topical area, and had management allowed the inclusion of a compromised force-on-force exercise, the overall composite LANL Security Survey rating would have been "Unsatisfactory."[3]

During the 1999 Albuquerque Security Survey at LANL, the overall composite rating was downgraded from "Satisfactory" to "Marginal" as were two sub-topical ratings and one topical rating.[4] The Survey Team initially rated LANL as "Satisfactory" based on the results of the 1999 Albuquerque Security Survey at LANL. However, during a final review, Albuquerque management determined that because the "23rd Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities," dated Jan 1997/Dec 1998, contained an issue concerning storage of classified parts, a "Satisfactory" rating

[1] The DOE requirements are specifically addressed at Appendix B.

[2] The 1998 rating changes are detailed at Appendix C. It should be noted that three of the seven ratings upgraded by Albuquerque management were the same as those ratings initially recommended by the Team Lead but subsequently downgraded by the "murder board."

[3] According to DOE Order 470.1, when a Survey has a composite rating of "Unsatisfactory" and the rating indicates a significant vulnerability, the Operations Office Manager shall coordinate with the cognizant Program Secretarial Officer within 24 hours to: 1) take action to shutdown/suspend operations of the facility or activity, pending remedial action, or 2) apprise the cognizant Secretarial Officer and the Office of Safeguards and Security of the rationale for continuing this critical operation and identify immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

[4] The 1999 rating changes are detailed at Appendix D. Team Lead ratings were not found for the 1999 survey.

would be the wrong message to send to the contractor. Therefore, the composite rating was downgraded from "Satisfactory" to "Marginal." Albuquerque management said that the composite ratings needed to closely reflect the results of other DOE reviews that had recently been conducted at LANL.

Management Rationale for Rating Changes

Although we found no evidence to support allegations of collusion or "deal making" between Albuquerque and LANL regarding the changes to the survey ratings, we did find that the survey reports did not contain any record of the rationale used by Albuquerque management for changing survey ratings. Albuquerque managers said that although Security Specialists conduct the surveys and propose recommended ratings for the sub-topic and topic areas, Albuquerque managers reserve "the right to take a look at what the survey team has developed" and decide what "message" should be sent to the contractor. Albuquerque management said that the rating process was "subjective" and that ratings remain "fluid" until a final report is issued. Contrary to the process identified in the Albuquerque Security Survey Procedural Guide, the Albuquerque managers said that they view it as a mistake to have the Security Specialists assign ratings because they do not have the overall LANL security program perspective prior to assigning final ratings and issuing the final security survey report. Further, in pursuing this matter, we found no other source which could provide the documented basis to support the Albuquerque management position concerning rating assignments or changes.

1999 Albuquerque Survey Team

The Albuquerque security survey team that conducted the 1999 Security Survey at LANL was composed of some inspectors and support service personnel who had never been assigned to a survey team previously and several who had not attended survey team training. Albuquerque management said that the 1999 Survey Team was short on staff because they had difficulty hiring qualified people to fill positions that had been vacated by retirements and other turnover. Two survey team members and two previous Survey Team Leads said they had questioned Albuquerque management about the appropriateness of the 1999 survey team's experience and the sufficiency of the number of inspectors staffed to conduct the 1999 survey.

Compromise of Force-on-Force Exercise[5]

The OIG also found that Albuquerque management did not fully assess concerns about a compromise of a force-on-force exercise during the 1998 Albuquerque Security Survey at LANL. The OIG

[5] A force-on-force exercise is conducted as a performance evaluation to assess the capability of the safeguards and security system to meet performance objectives in response to an outside group referred to as an Adversary Force.

found that Albuquerque management refused to allow the survey team to include a finding concerning a compromise of a force-on-force exercise in the survey report, and did so without adequately investigating the alleged compromise. A Security Force-on-Force Exercise Specialist told us there were major concerns raised regarding the Guard Force response, that the exercise had not gone well, and that the concerns had been appropriately raised to Albuquerque management. Albuquerque management said they had been made aware of the concerns, however, there was no evidence of "cheating" and that "the losers always complain that the winner cheated." A Security Specialist said that, had the compromise of the force-on-force exercise been included in the 1998 Albuquerque Security Survey report, the composite rating would have been "unsatisfactory." Instead, LANL was given a "marginal" rating.

Destruction of Records

During our inspection we noted that the 1997 and some 1998 Albuquerque Security Survey work papers were destroyed contrary to Albuquerque's policy on the destruction of records. The OIG also noted that some 1998 and 1999 work papers were either missing, not organized, or did not contain adequate summarization to support the ratings in the survey reports. As a result, there was no complete record to show how the survey teams developed the ratings.

LANL Self-Assessments

Since the inception of the LANL security self-assessment process[6] in 1996, LANL has had a history of not meeting all of its established self-assessment requirements. Specifically, the LANL Fiscal Years 1997 and 1998 Tier III Self-Assessment End-of-Year Reports indicate that some required Tier I and II self-assessments were not completed and that the process was not consistently implemented.[7] During our inspection, LANL officials confirmed weaknesses in the Tier I and Tier II self-assessment processes. The OIG found that in one LANL division, Tier I reviews were not being completed because the Tier I security responsibilities were assigned on a part-time basis and other responsibilities held a higher priority. In another LANL division, the OIG found that there had been no Tier II self-assessments completed since March 1998 because staffing was not adequate given other priority work.

[6] The LANL self-assessment process is described at Appendix B.
[7] At the time of our report, the LANL FY-99 Tier III Self-Assessment End-of-Year Report had not been issued.

In addition to finding that some self-assessments were not conducted, the OIG also found an instance where a self-assessment report was written without a self-assessment review being conducted. The OIG was provided a copy of a Tier II Self-Assessment Report that was generated in 1999 to support a Tier II review that was never performed. The OIG was told that this report, prepared at the direction of a LANL manager, was provided to an Albuquerque Security Survey Team to represent a completed Tier II review. The LANL manager who was identified as directing the preparation of the report denied having knowledge of any such report being prepared.

Pressure to Change Or Mitigate Issues

Regarding LANL Self-Assessments, the OIG found that 8 of the 28 LANL Security Operations Division personnel interviewed (approximately 30 percent) who had conducted self-assessments believed they had been pressured to change or "mitigate" security self-assessments. Several of these individuals said LANL management appeared to be more concerned about making LANL and the Security Operations Division "look good" than reporting the actual security condition at LANL. The OIG was informed of two instances where LANL management became so upset with issues[8] raised by the initially assigned reviewers, that management reassigned other reviewers who subsequently determined that there were no issues to be raised and that the organizations were satisfactory.

In addition, the OIG was provided information which showed that LANL management downgraded 40 issues and four concerns initially identified in a self-assessment draft report to six concerns and six observations which appeared in the final report. When interviewed, a LANL manager said that the reviewer had raised some issues that could not be validated, other issues that were unsupportable, and that there appeared to be a personality conflict between the reviewer and the organization being reviewed.[9]

A senior LANL manager indicated that, given the number of self-assessment findings identified since 1995, there was no concerted effort to avoid or mitigate findings.

[8] LANL has developed their own definition for issues, concerns and observations. Issues are deficiencies discovered during an internal self-assessment that require a corrective action plan. Concerns and observations are suggestions that may require improvement and may be mentioned in the text of a report, but they do not require a corrective action plan.

[9] It should be noted that the reviewer had conducted self-assessments in the same organization for three years prior to this review and had no difficulties in reporting issues developed during the prior self-assessments.

Los Alamos Area Office Oversight

The OIG determined that DOE's Los Alamos Area Office (LAAO) security staff was not performing all of the oversight responsibilities associated with the LANL Security Operations Division programs. Several DOE personnel told us that LAAO security was understaffed and did not have the technical expertise required to conduct all their oversight responsibilities. An Albuquerque manager confirmed that LAAO is understaffed and that the present staff has not had the necessary training to conduct the tasks required by their assignments. The manager told us there has been a reduction in full time equivalent positions at LAAO, and Albuquerque has not been able to replace staff that retire or leave for other positions. The Albuquerque manager said the two staff members that remain at LAAO's Office of Security have the responsibility for oversight but they do not have the technical expertise in all areas for which they are responsible. As a result, the manager said Albuquerque has taken responsibility for the security areas for which the LAAO staff does not have the technical expertise. It should be noted that our review did not independently evaluate the staffing levels and experience of the LAAO staff.

Energy's Office of Independent Oversight and Performance Assurance

The Department of Energy's Office of Independent Oversight and Performance Assurance reviewed LANL security operations during 1999 and issued a report on August 27, 1999, titled, "Independent Safeguards and Security Inspection of Los Alamos National Laboratory." The OIG is providing our findings to the Office of Independent Oversight and Performance Assurance for its consideration.

Recommendations

Recommendations

We recommend that the Manager, Albuquerque Operations Office:

1. Ensure that the supporting rationale for changing survey ratings after they have been assigned by the Survey Team is documented, and that the justification and the rationale for the factors responsible for the composite facility rating are included in the survey report.

2. Ensure that Security Survey Team Personnel possess the requisite expertise and skill necessary to perform the survey and that team members have sufficient experience in the topical areas being reviewed.

3. Update the Albuquerque Security Survey Procedural Guide to comply with the Albuquerque Records Information Destruction Schedule with regard to the destruction of all survey and inspection files.

4. Ensure that LANL's self-assessment program is fully implemented at all three-tier levels.

5. Review and assess staffing levels for security personnel at the Los Alamos Area Office, and ensure that the Area Office has adequate staff with the necessary technical expertise to carry out its security oversight responsibilities.

The OIG recommends the Director, Office of Security and Emergency Operations:

6. Evaluate self-assessment programs at other facilities to determine if these programs have been fully implemented and adequately represent the actual security conditions at the facilities.

Management Reaction and Inspector Comments

Management Reaction

In their response to the draft report, Albuquerque management stated that the facts presented and the conclusions reached were accurate, and that the recommendations were appropriate. Albuquerque management stated that they would take corrective action.

The Director, Office of Security and Emergency Operations agreed to evaluate self-assessment programs at DOE facilities, given the concerns identified during the inspection.

Inspector Comments

The actions planned and taken by the DOE Office of Security and Emergency Operations and the Albuquerque Operations Office were responsive to the recommendations.

Appendix A

Scope and Methodology

The OIG conducted this inspection at Los Alamos National Laboratory (LANL), Los Alamos Area Office (LAAO), and the Albuquerque Operations Office (Albuquerque) from April through November 1999. To accomplish our review objectives, the OIG:

- Reviewed DOE O 470.1, "Safeguards and Security Program," and DOE O 471.2A, "Information Security Program;"
- Reviewed the Albuquerque Security Survey Procedural Guide;
- Interviewed Albuquerque, LAAO, and LANL personnel;
- Reviewed documentation relating to security surveys and self-assessments;
- Reviewed the Albuquerque Management Review Division report titled "Manipulation of Security Survey Results" dated July 9, 1999;
- Reviewed the House Select Committee Report referred to as the "Cox Report" dated January 1999; and the President's Foreign Intelligence Advisory Board's report dated June 1999;
- Reviewed self-assessment reports issued by the LANL Security Operations Division and Security Survey reports issued by the Albuquerque Operations Office; and
- Reviewed the Office of Independent Oversight and Performance Assurance's Independent Safeguards and Security Inspection of LANL dated August 27, 1999.

This inspection involved a review of the Albuquerque Security Surveys of LANL Security Operations and LANL's Self-Assessment Program for Fiscal Years 1997, 1998, and 1999.

This inspection was conducted in accordance with "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency.

Appendix B

DOE Survey Requirements

The Department has mandated a "Safeguards and Security Program" through the issuance of DOE Order 470.1, SAFEGUARDS AND SECURITY PROGRAM. The purpose of this order is to ensure appropriate levels of security protection consistent with DOE standards to prevent unacceptable, adverse impacts to national security.

DOE Order 470.1 establishes that the responsible Operations Office assign ratings of "unsatisfactory," "marginal," or "satisfactory" based on conditions existing at the end of survey activities; and that survey reports include a justification and rationale for the overall composite facility rating. The order specifically states that these ratings are not to be based upon future or planned corrective actions. Additionally, the order establishes that the survey team personnel who conduct the Security Surveys are to possess qualifications, experience, and training (basic survey and team leader training) sufficient to accomplish effective and thorough surveys.

Albuquerque Security Survey Requirements

To assist in Albuquerque security survey reviews, the Albuquerque Safeguards and Security Division developed a Security Survey Procedural Guide dated May 22, 1997, which identifies the responsibilities of the Survey Team Lead, the Assistant Survey Team Lead, and the survey team members during each phase of the survey. This Guide outlines the survey team process. Specifically, the guide states that the DOE Team Lead is to conduct a "murder board" during which Topic Team Leads[10] support rating rationale/justification and assign final ratings. Survey team members also provide comments and clarifications for ratings assigned. The finalized information is then given to the report coordinator for inclusion in the survey report.

Self-Assessment Requirements

DOE Order 470.1, Chapter X, SELF-ASSESSMENT PROGRAM, establishes the requirement for self-assessment programs at contractor facilities. It requires that self-assessment programs be conducted and documented for all cleared facilities and that the self-assessments be performed between the security surveys, which are conducted by the responsible Operations Office.

The LANL Safeguards and Security Self-Assessment Program is also mandated by the terms of the Department's contract with the University of California, contract modification No. W-7405-ENG-36. This contact modification requires that "... the University will conduct an ongoing self-assessment process including self-

[10] A "Topic Team Lead" is the individual assigned to head the team that reviews one of the five topic areas as identified in Appendix C.

assessments performed at the Laboratory as the principal means by which to evaluate compliance with the performance measures ... against which [the] University's overall performance of obligations under the contract will be determined."

The University of California, in compliance with contract requirements, has implemented a self-assessment program that is defined in a LANL Safeguards and Security Assurance Manual dated June 1996. This manual establishes a three tiered self-assessment process with a primary objective of ensuring the effective and efficient implementation of the LANL Safeguards and Security program.

The formalized safeguards and security self-assessment program includes a plan for each applicable topical and sub-topical area. The self-assessment process consists of a three-tier process. At Tier I, each LANL Division is required to conduct a self-assessment within the division. This is accomplished by the organizational safeguards and security officer, utilizing a checklist format, covering areas such as computer security, information security, property protection, and Nuclear Material Control and Accountability. At Tier II, each section within the LANL Security Division is required to conduct a self-assessment in their functional area(s). At Tier III, a LANL self-assessment is conducted by a team of Subject Matter Experts (SMEs) under the direction of LANL Security Division Program Integration Group.

Appendix C

1998 Security Survey Rating Changes[11]

Program Topic Areas:	Team Leader	Murder board	Final Report
Program Management			
Program Management and Administration	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Program Planning	Satisfactory	Satisfactory	Satisfactory
Personnel Development and Training	Satisfactory	Satisfactory	Satisfactory
Facility Approval and Registration of Activities	Satisfactory	Satisfactory	Satisfactory
Foreign Ownership, Control, or Influence	Satisfactory	Satisfactory	Satisfactory
Safeguards and Security Plans	Unsatisfactory	Unsatisfactory	Unsatisfactory
Surveys and Self Assessment	Satisfactory	Satisfactory	Satisfactory
Resolution of Findings	**Satisfactory**	**Marginal**	**Satisfactory**
Incident Reporting and Management	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Protection Program Operations			
Physical Security	Marginal	Marginal	Marginal
Security Systems	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Protective Force	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Security Badges, Credentials and Shields	Satisfactory	Satisfactory	Satisfactory
Transportation Security	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Information Security			
Classified Guidance	Satisfactory	Satisfactory	Satisfactory
Classified Matter Protection and Control	**Satisfactory**	**Marginal**	**Marginal**
Special Access Programs and Intelligence Information	Satisfactory	Satisfactory	Satisfactory
Classified Automated Information Systems Security	Satisfactory	Satisfactory	Satisfactory
Technical Surveillance Countermeasures	Satisfactory	Satisfactory	Satisfactory
Operations Security	Satisfactory	Satisfactory	Satisfactory
Unclassified AISS (Optional)	Unsatisfactory	Unsatisfactory	Unsatisfactory
Protected Distribution System (Optional)	Satisfactory	Satisfactory	Satisfactory
Communications Security (COMSEC) (Optional	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	Marginal	Marginal	Marginal
Nuclear Materials Control and Accountability			
Basic Requirements	**Marginal**	**Unsatisfactory**	**Marginal**
Material Accounting	Unsatisfactory	Unsatisfactory	Unsatisfactory
Material Control	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
OVERALL RATING	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Personnel Security			
Access Authorization (Personnel Clearance)	Satisfactory	Satisfactory	Satisfactory
Security Education Briefings and Awareness	Satisfactory	Satisfactory	Satisfactory
Control of Visits	Satisfactory	Satisfactory	Satisfactory
Unclassified visits and Assign by Foreign Nationals	**Satisfactory**	**Marginal**	**Satisfactory**
Personnel Assurance Program	Satisfactory	Satisfactory	Satisfactory
Personnel Security Assurance Program	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory	Satisfactory
1998 Composite Rating	**Unsatisfactory**	**Unsatisfactory**	**Marginal**

Items in **Bold** indicate changes in ratings.

[11] There is no documentation for the 1999 Security Survey that provides a similar Team Leader rating breakdown.

Appendix D

1999 Security Survey Rating Changes

Program Areas:	Murder board	Final Report
Program Management		
Program Management and Administration	Satisfactory	Satisfactory
Program Planning	Satisfactory	Satisfactory
Personnel Development and Training	Satisfactory	Satisfactory
Facility Approval and Registration of Activities	Marginal	Marginal
Foreign Ownership, Control, or Influence	Satisfactory	Satisfactory
Safeguards and Security Plans	Satisfactory	Satisfactory
Surveys and Self Assessment	Satisfactory	Satisfactory
Resolution of Findings	Satisfactory	Satisfactory
Incident Reporting and Management	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory
Protection Program Operations		
Physical Security	Satisfactory	Satisfactory
Security Systems	Satisfactory	Satisfactory
Protective Force	Satisfactory	Satisfactory
Security Badges, Credentials and Shields	Satisfactory	Satisfactory
Transportation Security	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory
Information Security		
Classified Guidance	Satisfactory	Satisfactory
Classified Matter Protection and Control	**Satisfactory**	**Marginal**
Special Access Programs and Intelligence Information	Satisfactory	Satisfactory
Classified Automated Information Systems Security	Satisfactory	Satisfactory
Technical Surveillance Countermeasures	Satisfactory	Satisfactory
Operations Security	Satisfactory	Satisfactory
Unclassified AISS (Optional)	Satisfactory	Satisfactory
Protected Distribution System (Optional)	Satisfactory	Satisfactory
Communications Security (COMSEC) (Optional)	Satisfactory	Satisfactory
OVERALL RATING	**Satisfactory**	**Marginal**
Nuclear Materials Control and Accountability		
Basic Requirements	Satisfactory	Satisfactory
Material Accounting	Marginal	Marginal
Material Control	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory
Personnel Security		
Access Authorization (Personnel Clearance)	Satisfactory	Satisfactory
Security Education Briefings and Awareness	**Satisfactory**	**Marginal**
Control of Visits	Satisfactory	Satisfactory
Unclassified Visits and Assignments by Foreign Nationals	Satisfactory	Satisfactory
Personnel Assurance Program	Satisfactory	Satisfactory
Personnel Security Assurance Program	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory
1999 Composite Rating	**Satisfactory**	**Marginal**

Items in **Bold** indicate changes in ratings.

Appendix V:

Memo from General Thomas F. Gioconda, Acting Deputy Administrator for Defense Programs to: the Secretary of Energy Bill Richardson

March 2000

Department of Energy
Washington, DC 20585

MEMORANDUM FOR THE SECRETARY

THROUGH: T. J. Glauthier
Deputy Secretary

Ernst J. Moniz
Under Secretary

FROM: THOMAS F. GIOCONDA
Brigadier General, USAF
Acting Deputy Administrator
for Defense Programs

SUBJECT: ACTION: APPROVAL OF DEPARTMENTAL POSITION REGARDING TECHNICAL AREA 18 AT LOS ALAMOS NATIONAL LABORATORY

BACKGROUND: In November 1999, Deputy Secretary T. J. Glauthier commissioned a multi-Program Office team to examine alternatives for conducting nuclear criticality activities currently performed at Technical Area 18 at Los Alamos National Laboratory (Los Alamos). The Team was co-chaired by Peter Stockton and Jon MacLaren (Office of Defense Programs) and included members from Offices of Security and Emergency Operations; Nonproliferation and National Security; Environmental Management; Science; Nuclear Energy, Science, and Technology; Materials Disposition; Civilian Radioactive Waste Management; and Environment, Safety and Health. The Team also considered other related missions at Technical Area 18, including nuclear nonproliferation and emergency response.

The Team was tasked to develop a recommendation supported by a proposed transition plan that would ensure continuity of criticality training and the retention of critical staff to manage and operate these facilities. After reviewing several proposals utilizing weighted evaluation criteria, the Team reached consensus on a recommendation to conduct further evaluations on two siting options:

- constructing a new underground facility adjacent to Los Alamos Technical Area 55, and
- modifying the Device Assembly Facility at Nevada Test Site.

Included in these additional evaluations is the requirement to conduct preliminary facility designs and National Environmental Policy Act reviews. These alternatives would be evaluated against the baseline case of continuing national security activities at Los Alamos Technical Area 18. A summary of the cost and schedules for each of these options is attached.

After review of the Team's recommended approach, each Secretarial Officer or designee took the following position:

Defense Programs	Technical Area 18, Los Alamos
Environmental Management	Device Assembly Facility, Nevada
Environment, Safety and Health	Device Assembly Facility, Nevada
Materials Disposition	
Nonproliferation and National Security	Device Assembly Facility, Nevada
Nuclear Energy, Science and Technology	Fuel Manufacturing Facility, Argonne National Laboratory West
Civilian Radioactive Waste Management	Technical Area 55, Los Alamos
Science	Technical Area 55, Los Alamos
Office of Secretary	Device Assembly Facility, Nevada
Security and Emergency Operations	Technical Area 55, Los Alamos

SENSITIVITIES:

There is significant level of programmatic and financial uncertainty in the siting options that were presented by the Team as well as the baseline case. All three options involve 10-year life cycle costs estimated at $500 to $600 million, including capital funding on the order of $100 million over the next 6 to 7 years. While all options strive to maintain the criticality capability, options other than remaining at Technical Area 18 may require that activities be temporarily suspended in a phased approach as equipment and materials are relocated and made operational at the new location. In addition, options that would relocate Technical Area 18 will require additional National Environmental Policy Act review prior to initiating facility modification or construction activities. This environmental review is anticipated to take 12 to 15 months at a cost of $2.5 million.

As the Lead Program Secretarial Officer for Los Alamos National Laboratory and the Nevada Test Site, Defense Programs has additional concerns regarding the two options presented by the Team. Utilization of the Device Assembly Facility for this mission presents unresolved program compatibility issues with the facility's primary missions of underground test readiness and responding to a damaged nuclear weapon. Additionally, Defense Programs' limited capital

funding is already allocated to higher priority Stockpile Stewardship projects.

After carefully considering the recommendation presented by the Team as well as positions provided by the Managers of Albuquerque and Nevada Operations Office and the Directors of Los Alamos and Sandia National Laboratories, Defense Programs recommends that the Department retain its current mission and activities at Technical Area 18. Defense Programs will continue to pursue improvements to reduce operational and security costs and also validate proposed security and infrastructure upgrades.

The Office of Security and Emergency Operations has verbalized concerns in the past regarding the ability of TA-18 to effectively address future changes to the design basis threat and may provide a separate position to the Secretary during the March 15, 2000, meeting that recommends moving out of TA-18 in an expedited manner.

Since many departmental organizations utilize Technical Area 18 to conduct national security activities, Defense Programs sought to gain consensus regarding this position. This memorandum was coordinated with affected Program Secretarial Offices.

POLICY ISSUES: None.

RECOMMENDATION: That you concur in retaining current activities at Los Alamos Technical Area 18 with appropriate security and infrastructure upgrades.

APPROVE: _____

DISAPPROVE: _____

DATE: _____

CONCURRENCES:
Office of Civilian Radioactive Waste Management
Office of Environment, Safety and Health
Office of Environmental Management
Office of Materials Disposition
Office of Nonproliferation and National Security
Office of Nuclear Energy, Science, and Technology
Office of Science
Office of Security and Emergency Operations

ATTACHMENT 1
Cost and Schedule Estimates for Option Study Alternatives

Option	Estimated Capital Cost ($M)	Estimated Other Project Cost ($M)	Estimated Completion Time (Years)	Estimated 10-year Lifecycle Cost ($M)
Los Alamos National Laboratory Technical Area 18	60	30	7	600
Nevada Test Site Device Assembly Facility	24	57	6	500
Los Alamos National Laboratory Technical Area 55	63	27	7	500

DP-24:MacLaren:S-1 Memo 3-7-00.doc:3/9/00

Distribution:

so: addressee
1bcc: ES
1bcc: ECS
3bcc: DASMASM
1bcc: DP-24 Rdr
1bcc: T. Bishop, DP-24
1bcc: J. MacLaren, DP-24
1bcc: R. Dintaman, DP-17
1bcc: O. Goktepe, SC-80
1bcc: M. Hutmaker, NE-40
1bcc: J. Psaras, EM-21
1bcc: R. Pearson, MD-3
1bcc: W. Lake, RW-44
1bcc: D. Spears, NN-20
1bcc: J. Weidner, SO-40
1bcc: F. Chen, EH-22
1bcc: E. Livingston, S
1bcc: C. Leasure, LANL
1bcc: E. Mullen, LANL
1bcc: C. Cruz, AL/NPD
1bcc: J. Tillman, AL/NCPO

DP IDRMS#: 2000-00517
DUE DATE: 3/10/00

DP-24 Correspondence Reviewer and Date: _____
DP-20 GTN Correspondence Reviewer and Date: _____
DP-20 FORS Correspondence Reviewer and Date: _____

DP-24	DP-24	DP-20.1	DP-20	DP-17	DP-17	DP-10
MacLaren 3/ /00	Dunsworth 3/ /00	Rhoades 3/ /00	Beck 3/ /00	Dintaman 3/ /00	Miotla 3/ /00	Crandall 3/ /00
DP-1	EH-1	EM-1	MD-1	NE-1	NN-1	RW-1
Gioconda 3/ /00	Michaels 3/ /00	Huntoon 3/ /00	Holgate 3/ /00	Magwood 3/ /00	Gottemoeller 3/ /00	Itkin 3/ /00
SC-1	SO-1	US	DS	S		
Decker 3/ /00	Habiger 3/ /00	Moniz 3/ /00	Glauthier 3/ /00	Richardson 3/ /00		

Appendix W:

Letter from Ronald E. Timm President, RETA Security to: General Eugene Habiger
Director, Office of Security & Emergency operations, SO-1

January 5, 2000

PERSONAL AND CONFIDENTIAL

January 5, 2000

General Eugene Habiger
Director, Office of Security & Emergency Operations, SO-1
U.S. Department of Energy
Washington, DC

Subject: Lying and Retaliation in the SO-20 Department.

It is with the utmost regret that I write this letter. There are two points I need to make. The two issues are: the first and most pressing issue is that of a number of people in the Department that are lying in the reporting of the actual status of security at our most important nuclear sites; the second issue concerns the illegal retaliation of these people against those trying to correct these security problems..

RETA Security, Inc. is part of the prime contract to provide support to Department SO-21 under contract DE-AC01-98NN50323. We have provided the key person services of Senior Engineer as well as Program Analyst since 1994. In that time we have provided services to both the Policy and Field Operations Branches. In 1997 we were assigned an additional task through the then NN-51 to support a QA effort through Richard Levernier for review of all 11 SSSPs for protection of Class A nuclear facilities. As part of that effort we worked with Mr. Levernier to develop a QA process that involved evaluation of the Parts I & II of the SSSP, the JTS simulations, and provide input for the on-site systems reviews.

In 1997, one of the first reviews we undertook was that of RFETS. In March of that year we documented high risk at this site. JTS simulations in April confirmed the assertion. Over the period of time since 1997 until November of this year literally no changes were made to improve the security at this site. We have found similar major problems at TSD in 1998, and LANL in 1999. There have been lesser problems at LLNL, SNLA, and Pantex. In all of these instances we have provided extensive analyses and documentation to support these findings. In all instances we were asked to make sure that the results were "bullet proof." We did.

In the spring of 1999 we were assigned to support the efforts of Mr. Peter Stockton on behalf of the Secretary of Energy. In that role we provided technical assistance in the preparation and documentation of nine issue papers that identified major security issues. Many of these issues are related to our efforts since 1997. We understand that you have been briefed on their content.

In the spring of this year we assembled over 90 official documents that tracked the history of problems at RFETS to include congressional requests for information, conditional concurrence by SO-20, OA inspections, etc. These documents show a systematic pattern of lying and misinterpretation of facts. For instance, in the fall of 1997 Joe Mahaley conditionally concurred with the 1997 SSSP if certain protective force actions were addressed within 120 days. None of the issues were addressed until November 1999. In 1998 OA ran a worst case force on force at

RFETS which the site failed. The Inspection report said security was acceptable because three lesser tests were okay. The department has a policy for risk that is numerical value and defined adjectivally as either low, moderate or high. There is no designation as "acceptable." In the summer of 1999 Don Solich prepared a briefing paper for you that indicated no major problems at RFETS even though he was well briefed on the QA results.

In the fall of 1998 we did an extensive review of TSD. These findings were documented in January 1999 and briefed to Joe Mahaley and his staff through Johnson, Ford and Solich. At the initial briefing to Mahaley he said that he needed a day to think about results for TSD that clearly showed high risk. In the summer of that year, with nothing have been done about risk, Mahaley observed force on force testing at Ft. Hood. Based on this review he was prepared to offer SSSP concurrence. In the fall Stockton uncovered "cheating" at this test. To date Mahaley has done nothing to address the high risk. The TSD issue has been continually pointed out to Johnson, Ford, and Solich as a series of memos from Rich Levernier. We have documented over 15 briefings and correspondence on this issue.

In November of 1999 we did a review of LANL, TA-55 and found major problems with the ability of the protective force to deal with worst case scenarios. The results were documented to management to include, Johnson, Ford, and Solich. At the briefing, a HQ contractor asserted that the current SSSP did not in fact represents the current force profile and strength and that it had been greatly improved since seven days earlier. Therefore, the SSSP should be concurred with. This means that the SSSP did not have a VAR asserting any risk other than high. Never in my experience have I seen a situation were no documents supported risk, but that this line of management was prepared to recommend approval because "that is what the General wants."

Since the spring of this year I feel that we have become victims of a systematic retaliation and retribution effort by management in SO-20 to discredit our work and reduce our role in the QA effort needed for concurrence decisions by you. Joe Mahaley, Toby Johnson, Jim Ford, Don Solich, and Sam Calahan are currently engaged in obfuscating issues, and in some instances, lying to keep issues of high risk to national assets from being brought to your attention. Further, this systematic retaliation and retribution effort affects other personnel who were either part of the SSSP reviews, or assisted Peter Stockton. These persons include Marshall Combs, Larry Wilcher, Rich Levernier, Jack Pope, and other personnel from my company.

Currently there is a restructuring of the SSSP being undertaken. We have been systematically denied from participating in this effort by management. Requests by Rich Levernier for us to participate have been denied by Johnson, Ford, and Solich. When we have reviewed some of the documents from this and the DBT effort, we have found a systematic pattern of "dumbing" down the SSSP process. For example, the new SSSP proposes using 1989 values of consequence for loss of assets. The 1989 values were found to be flawed in 1993. They not only result in risk being less conservative by 13% or more, but they require no protection for Cat II SNM. Sam Calahan knows this, but has ignored the issue. Also the QA process is being completely subverted so that SSSP development becomes a joint Field/HQ function with no credible "hold" points for independent QA review functions. The DBT is examining the use of a truck bomb to

cause radiological sabotage. This in spite of the fact that the NRC has expressly addressed the truck bomb and radiological sabotage. We know of at least one site that has vehicle barriers in the wrong location near a large inventory of Pu next to and up wind of a major metropolitan area.

The QA tools developed by Rich Levernier were attacked by Jim Ford. Ford asked for field comments about the QA process. Surprisingly the conclusion was that the QA process was not needed. The comments provided by the field whose SSSP were in question were basically sophomoric and self serving. The CTA model from course CTA-241 for advanced VA analysis was dropped by Sam Calahan in spite of class reviews that extolled its virtues. This model was an alternate to check VA results. With no checks and balances, the SSSP process is further "dumbed down."

After the initial Stockton support, he asked for our help on the consolidation issue. We have extensive experience in this area. Peter was told by Mahaley that RETA was too expensive and that our rate was $300 per hour. This is patently untrue. Our rates for my services are half of that, and others from our company are less than that. Not only that, but these rates have been accepted in contract negotiations with me designated as a key person. Ford and Johnson have also repeated this tale in public forums. I find this very unprofessional, besides being untrue. What this smacks of is denying Mr. Stockton resources he may need to accomplish his work in a timely and efficient manner. Further, it imputes our capabilities.

Since the spring of 1999 our use in support of QA efforts have had a steady decline. The rate of decline is symptomatic of all of the items identified above. The specter of retaliation and retribution is not one that we are corporately comfortable in dealing with. We work at the pleasure of any of our clients. When we have been ethically or professionally compromised we have left that client. We believe that the role that Secretary Richardson and you have signed up to to protect assets of societal importance is necessary, and therefore we have prepared this letter as a last resort. We believe this is not a "he said she said" issue, but based on documented evidence.

As you consider this letter I would invite you to contact what I consider impartial sources that will attest to our professional competence and ethical conduct. Two such persons are: Thomas Gradle, Director of Security, Chicago Operations, and Cliff Druit (BG, ret).

If you would like to meet with me personally, review the documents, or issues I would be pleased to make myself available at your convenience.

Sincerely yours,

Ronald E. Timm,
President
(630)257-3520

Appendix X:

Letter from Maureen McCarthy and Ellen Livingston to: Secretary of Energy Bill Richardson

November 21, 2000

November 21, 2000

Note to: Secretary Richardson

Through: T.J. Glauthier
Ernie Moniz
John Gordon

From: Maureen McCarthy and Ellen Livingston

Subject: Status of Safety, Physical Security, and Environmental Reviews at Los Alamos National Laboratory

As discussed, we owe you an update on safety and physical security issues at Los Alamos National Laboratory (LANL) and, in particular, Technical Area 18 (TA-18). A summary of recent issues -- and recommended actions -- has been developed with the input of affected offices and is provided below.

Revised Schedule for Environmental Impact Statement for TA-18

Last year, you tasked a group to review options (including schedules) for relocating the programs conducted at TA-18, and actions needed to maintain an appropriate level of security until the relocation effort was completed. The group was chaired by the Office of Defense Programs and Peter Stockton -- and included representatives from LANL and the offices of Defense Programs, Security, Environmental Management, General Counsel, and Environment, Safety and Health.

As a result of that review, you directed the Office of Defense Programs last April to prepare an Environmental Impact Statement (EIS) to evaluate the transfer of projects and equipment at TA-18 to another location by 2004; although LANL was identified as a preferred site, other DOE sites also were to be considered.

The EIS and Record of Decision were to be completed by mid-January 2001. The schedule was published in a Federal Register notice on May 2, 2000, and public scoping hearings were subsequently held.

In late May, the Office of Defense Programs indicated in a memorandum to you (Attachment 1) that adequate funds could not be provided to continue the TA-18 studies, and that a revised schedule for conducting the work would be provided upon the program's receipt of additional funding. In a memorandum dated June 29 (Attachment 2), you directed the Office of Defense Programs to continue work on the EIS to support the issuance of a Record of Decision (ROD) by January 15, 2001, and to fund the effort by redirecting funds already available to the program. The program, however, subsequently reported that it would be unable to complete the work

needed to issue an ROD in January 2001, and indicated plans to complete the work on the following schedule:

	Original Schedule:	**Revised DP Schedule:**
TA-18 data obtained	June 1, 2000	Ongoing
Issue Draft EIS for Comment	August 25, 2000	April 2001
Hold Public Hearings	September 19-28, 2000	May 2001
Comment Period Ends	October 9, 2000	June 2001
Issue Final EIS (Fed. Reg. Notice)	December 15, 2000	August 2001
Record of Decision	January 15, 2001	September 2001

The Office of Defense Programs has indicated that the revised schedule cannot be accelerated at this point because of the need to complete technical studies -- and conceptual designs of new facilities -- required for the Record of Decision. Additional information is provided in the attached draft memorandum (Attachment 3).

Recommendation:

While the overall schedule for completing the final EIS cannot be greatly accelerated at this point, we can work with the Office of Defense Programs to issue a Federal Register in mid-December outlining the revised EIS schedule, the specific reasons for the delay, and a continued preference for relocating the TA-18 missions at LANL.

Approve: _____

Disapprove: _____

Safety Issues:

The Office of Environment, Safety, and Health plans by the end of the year to recommend to the Director of the NNSA a citation against the University of California for a series of nuclear safety violations. The violations include the failure of maintenance workers to follow safe operating procedures at TA-55, and, as a result, being exposed to levels of plutonium that exceeded DOE standards; and conduct-of-operation failures at TA-18 involving 3 reactors. The TA-18 events included the operation of nuclear facilities outside the limits and controls established by the facility's authorization basis safety documents. One event in December 1999 involving a reactor being started up and operating for one minute at levels that exceeded LANL's experimental plan, and another issue involved continued operation of a critical assembly -- or reactor -- after LANL had received credible analysis that a hydrogen explosive hazard could be generated during operations.

Upon issuance of any citation, the University of California would be required to develop a corrective action plan for DOE approval. To ensure adequate consideration of the safety

violations, the Office of Defense Programs plans to direct the DOE contracting office to specifically consider these violations in the annual rating review of contractor performance.

Recommendation: That the Office of Defense Programs forward the contracting officer's draft contractor-performance evaluation and fee determination to John Gordon and to you for review before it is approved and finalized.

Approve: _____

Disapprove: _____

Physical Security:

Several physical security issues have occurred at TA-18 over the last several months. In September 2000, a reactor at TA-18 had a power failure -- with the resulting failure of automatic security locking systems on the reactor vault (the vault was then manually locked). Although subsequent reviews revealed that all other security measures surrounding the vault were operable and effective, the loss of the automatic locking system was thoroughly investigated in order to prevent a reoccurrence.

In October 2000, Glenn Podonsky's office conducted an assessment of TA-18 security capabilities. The team identified a number of improvements but also several significant weaknesses -- most notably in the level of response training, and in the security forces' understanding of appropriate response procedures. The problems that were noted can be fixed by changes in strategy without the need for the site to incur significant additional costs. The Office of Defense Programs has submitted an initial corrective action plan to Glenn Podonsky this month. While the personal commitment of John Browne to expeditiously complete these ongoing improvements has been obtained, the following recommended actions will ensure an effective, short-term fix for addressing these security issues if implemented immediately.

Recommendations:

- That the Office of Defense Programs direct the University of California to take immediate, specific compensatory measures (and have the University of California provide confirmation by December 1, 2000, that the compensatory measures have been taken);
- That the Office of Defense Programs forward a final corrective action plan to John Gordon and you by the end of December 2000; and
- That Glenn Podonsky's office conduct a follow-up validation that compensatory measures are in place by the second week of January 2001, and conduct a comprehensive re-inspection in the Spring of 2001.

Approve: _____

Disapprove:_____

cc: G. Falle, S-1
M. Crecdon, DP-1
T. Gioconda, DP-2
G. Podonsky, OA-1
E. Habiger, SO-1
J. McBroom, SO-40
D. Michaels, EH-1
R.Christopher, EH-10
S. Adamovitz, EH-10

Appendix Y:

Letter from General John A. Gordon, Administrator National Nuclear Security Administration to: Dr. John Browne, Director Los Alamos National Lab

November 22, 2000

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

November 22, 2000

OFFICE OF THE ADMINISTRATOR

Dr. John C. Browne
Director
Los Alamos National Laboratory
P.O. Box 1663
Mail Stop A100
Los Alamos, New Mexico 87545

Dear Dr. Browne:

As we discussed yesterday, I have been briefed on a series of significant and unresolved security issues at Los Alamos National Laboratory (LANL) and, in particular, Technical Area 18 (TA-18). The failure of the University of California to submit a suitable corrective action plan and to correct in a timely manner the deficiencies cited in an October 2000 assessment of TA-18 security capabilities is unacceptable. As you know, the assessment identified a number of improvements but also several significant weaknesses -- most notably in the security strategy, the level of response training, and in the security forces' understanding of appropriate response procedures. The problems that were noted can be fixed by changes in strategy without the need for the site to incur significant additional costs.

who said ?

While your office submitted an initial corrective action plan this month, I have indicated to you that we continue to have serious concerns with the pace and scope of the corrective actions. As a result, I am directing the following actions.

First, the University of California must implement immediate, specific compensatory measures and certify to me by December 1, 2000, that the compensatory measures have been taken. The Department's Office of Independent Oversight and Performance Assurance will immediately conduct a follow-up validation to ensure that compensatory measures are in place. That office also will conduct a comprehensive re-inspection in the Spring of 2001.

555P

As referenced in the November 21, 2000, memorandum from Deputy Administrator Madelyn Creedon to Mr. Richard Glass (and also copied to you), appropriate compensatory measures must be in place by December 1, 2000, and a second set of measures in place by December 31, 2000. Moreover, the draft corrective action plan must be updated to reflect timely future actions. If any of these actions do not occur, all activities at TA-18 will be immediately

suspended until the actions have been taken and verified. In addition, we will consider these issues and reserve the right to take additional actions under the terms of the Department's contract with the University of California, including actions that may be required to hold appropriate managers accountable for all aspects of operations at TA-18.

I appreciate your immediate attention to this matter.

Sincerely,

John A. Gordon
Administrator

cc: Dr. Richard C. Atkinson, President, University of California
Secretary of Energy Bill Richardson
Deputy Secretary T.J. Glauthier
Ms. Madelyn Creedon, Deputy Administrator, NNSA
Mr. Richard Glass, Manager, Albuquerque Operations Office, U.S. Department of Energy
Mr. David Guerule, Manager, Los Alamos Area Office, U.S. Department of Energy

Appendix Z:

"Weaponry: Availability of Military .50 Caliber Ammunition,"
General Accounting Office Report # OSI-99-14R

June 30, 1999

GAO

United States
General Accounting Office
Washington, D.C. 20548

Office of Special Investigations

B-282665

June 30, 1999

The Honorable Henry A. Waxman
Ranking Minority Member
Committee on Government Reform
House of Representatives

The Honorable Rod R. Blagojevich
House of Representatives

Subject: Weaponry: Availability of Military .50 Caliber Ammunition

As requested, enclosed with this letter is a copy of a briefing that OSI gave to representatives of the House Committee on Government Reform on May 21, 1999. At that time, we briefed those present on the results of our review, which Ranking Minority Member Waxman had requested, concerning how military .50 caliber ammunition, including armor-piercing and armor-piercing incendiary ammunition, becomes available for civilian purchase. This included the process by which the U.S. Department of Defense disposed of the .50 caliber ammunition for demilitarization, the initial process used by the contractor that demilitarized the ammunition, and that contractor's manufacturing and marketing practices for the demilitarized ammunition.

We will make copies of this letter available to others on request. If you have any questions, please contact Assistant Director Ron Malfi at (202) 512-6722.

Robert H. Hast
Acting Assistant Comptroller General
for Special Investigations

Enclosure

167395

Enclosure I

BRIEFING PAPER
.50 Caliber Military Surplus Ammunition

For the House Committee on Government Reform

♦ INTERVIEWS

Talon Manufacturing Company, Paw Paw, West Virginia

Department of Defense, Industrial Operations Command, Rock Island, IL

♦ QUESTION

How does military .50 caliber ammunition, including armor-piercing (AP) and armor-piercing incendiary (API), become available for civilians to purchase?

♦ SUMMARY OF SIGNIFICANT FINDINGS

Talon Manufacturing Company, headquartered in Paw Paw, West Virginia, holds an exclusive contract with DOD to demilitarize (demil) small arms ammunition, defined as .50 caliber and below. Ammunition leaving the DOD account is classified in three categories: unserviceable, excess, or obsolete. No small arms ammunition goes directly from DOD to the civilian market. The ammunition is shipped in bulk to Talon from various military storage depots. DOD pays Talon $1 per ton for the ammunition that it will demil.

In the case of .50 caliber ammunition, Talon separates the round and discards the primer. The remaining components can then be (1) sold for scrap, (2) used to manufacture reconditioned ammunition (with a new primer), or (3) sold on the civilian market for customers who reload their own ammunition using the brass casing, projectile, and propellant (gunpowder) components. The reconditioned ammunition sold by Talon for purchase by civilians has essentially the same ballistic characteristics as the original military round. It is widely referred to as "military surplus" ammunition.

DOD provides Talon with five types of .50 caliber ammunition: ball, armor-piercing (AP), armor-piercing incendiary (API), armor-piercing incendiary tracer (APIT) and ball tracer. These rounds are all sold on the civilian market.

♦ HIGHLIGHTS OF FINDINGS

DOD Process Used to Demilitarize Small Arms Ammunition

DOD, Industrial Operations Command, Rock Island, Illinois, provided the following information:

- DOD has awarded Talon Manufacturing Company an exclusive contract to demil small arms ammunition, defined as .50 caliber and below.
- The term "military surplus" ammunition is a misnomer, since DOD does not sell ammunition directly to the civilian market.
- Ammunition leaving the DOD account can be classified in three categories: unserviceable, excess, or obsolete.
  - Unserviceable ammunition is transferred to a storage depot and reported on the B5A Demil Account.
  - Excess ammunition is offered to other branches of the military or to other federal agencies. It can also be offered to foreign military agencies. If there is no interest in the excess ammunition, it is then transferred to a storage depot and reported on the B5A Demil Account.
  - Obsolete ammunition can be offered to foreign military agencies. If there is no interest in the obsolete ammunition, it is then transferred to a storage depot and reported on the B5A Demil Account.
- Ammunition reported on the B5A Demil Account is shipped in bulk from a storage depot to Talon.
- DOD pays Talon $1 per ton for the ammunition.

Talon - Initial Processing of Military .50 Caliber Ammunition

- Demil ammunition of all calibers is delivered in bulk to a Talon plant in Herdon, West Virginia. Talon is paid by the ton and does not keep track of the number of rounds it receives from DOD.
- The primer is removed and discarded. The projectile is then separated from the brass casing. The propellant (gunpowder) is removed and saved. The brass casing is inspected and polished. The projectile is inspected.
- Ninety-eight percent of the .50 caliber rounds are used for scrap. The gunpowder is used to create a mixture called "slurry," which is sold as an explosive for use in road construction. The brass casings and projectiles are melted.
- Two percent of the .50 caliber rounds are used to produce reconditioned ammunition or components sold for reloading of ammunition.

Talon – Manufacturing and Marketing of .50 Caliber Ammunition

- The components of the .50 caliber round—propellant, brass casings, and projectiles—are shipped from the Talon plant in Herdon to the plant in Paw Paw, where a new primer is used with the components to manufacture reconditioned ammunition.
- The reconditioned ammunition has essentially the same ballistic characteristics as the original military round. It is widely referred to as "military surplus" ammunition.
- .50 caliber ammunition is sold to both U.S. and foreign military customers and on the civilian market. Talon sells ammunition only to legitimate businesses. Its biggest customers for .50 caliber rounds are Cascade Ammo in Oregon, Claflin Cartridge Company in Illinois, and Wideners Reloading in Tennessee. Wideners buys brass casings and projectiles for resale to civilian customers who reload their own ammunition.
- Talon receives five types of .50 caliber rounds from DOD, which can be identified by the tip of the projectile: (1) ball – no color; (2) AP – black; (3) API – silver; (4) APIT – silver and red; and (5) ball tracer – brown or dark orange.
- These rounds are all sold on the civilian market. The most popular means of packaging the .50 caliber ammunition is belted in 100 round strips (4 API rounds and 1 APIT round with the sequence repeated). It is shipped in the original U.S. military "ammo" can. The belted rounds are intended for machine guns, but the rounds can be used in either bolt-action or semiautomatic rifles by detaching a round from the belt.
- Talon reported that during the one-year period ending March 1999, it sold approximately 419,000 .50 caliber rounds, broken down as follows:

    - 200,000 rounds AP sold to Brazilian Military
    - 3,000 rounds API sold to Colombian Military
    - 35,000 rounds ball sold to U.S. Military
    - 110,000 rounds API and APIT (4 to 1 belted) sold to the commercial civilian market
    - 56,000 rounds ball and ball tracer (4 to 1 belted) sold to the commercial civilian market
    - 15,000 rounds ball tracer and APIT (4 to 1 belted) sold to the commercial civilian market

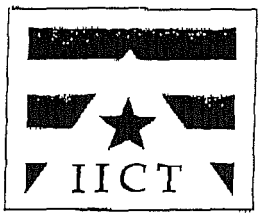
The only other armor-piercing type ammunition Talon receives from DOD is a 7.62 caliber AP round. According to Talon, because this caliber ammunition can be used in handguns as well as rifles, civilian possession is banned under federal law. Talon sells 7.62 AP ammunition only to military customers.

(600541)

Appendix AA:

"Improvised Explosive Devices (IEDs) and Other Criminal and Terrorist Devices: A Basic Reference Manual," Director of Central Intelligence, Interagency Intelligence Committee on Terrorism

September 2000



The Director of Central Intelligence
Interagency Intelligence Committee on Terrorism
Community Counterterrorism Board

Improvised Explosive Devices (IEDs) and Other Criminal and Terrorist Devices

A Basic Reference Manual

September 2000

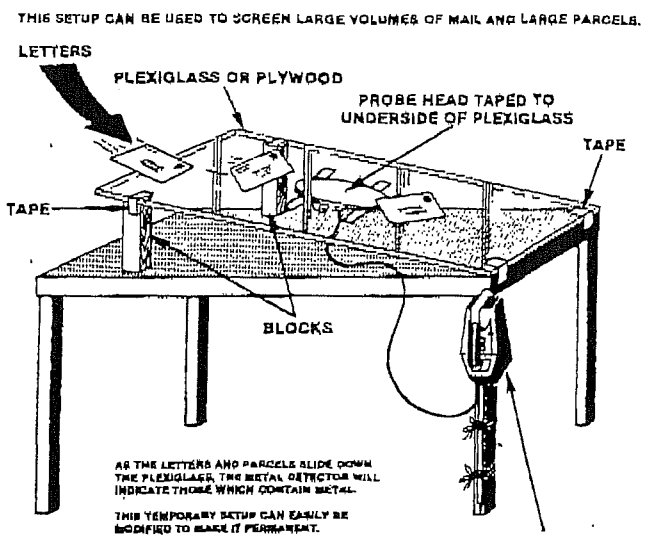


FIGURE 3.3-5. GOLD MOUNTAIN METAL DETECTOR (AVAILABLE FROM A/SY/T)

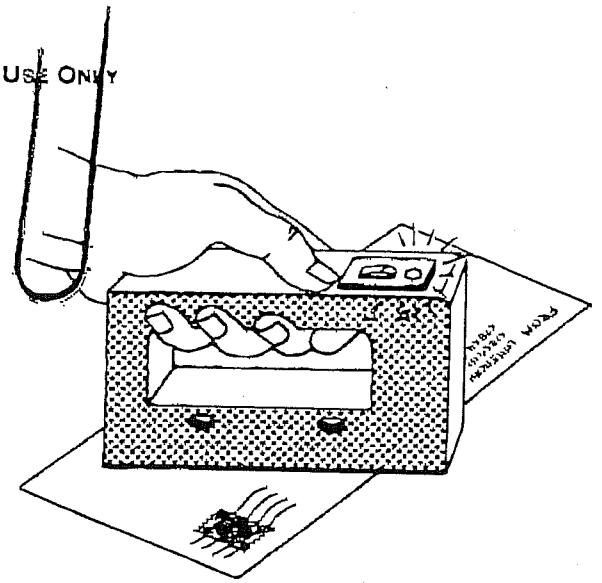


FIGURE 3.3-6. HAND-HELD METAL DETECTOR.

3.4 VEHICULAR BOMBS

The car or truck bomb is an expedient blast weapon. Its main characteristic is use of an explosive device that is large in size and lethal to structures at a long distance. These devices may be made of any explosive. Availability is usually the determining factor.

The use of ammonium nitrate and fuel oil was noted earlier. Because it is so easy to obtain, it is sometimes the material of choice in large, crude bombs. By arranging the containers carefully and using multiple initiation sites, either with detonating cord or with extra detonators, a crude blast focusing effect could be produced. The best defense against these devices is strict security and large safety distances.

Starting in 1983 U.S. interests have been attacked by terrorists and criminals with large vehicle bombs. Substantial loss of life has resulted. The vehicle drivers in some cases have been suicide bombers. An overview of these bombings follows:

- Beirut, Lebanon: U.S. Embassy, 18 April 1983 (estimate – 2000 lb.)
- Beirut, Lebanon: U.S.M.C. – Marine Amphibious Unit (Airport Bombing) 23 October 1983 (est. 12,000 to 20,000 TNT equivalent)
- Dhahran, Saudi Arabia: Khobar Towers U.S.A.F. billeting apartment complex, 25 June, 1996
- Kuwait: U.S. and French Embassy, 12 December 1983 (estimated 4000 lbs. TNT equivalent)
- World Trade Center Bombing, New York, NY, 26 February 1993.
- Alfred P. Murrah Federal Building, Oklahoma City, OK, April 1995
- American Embassy Bombings – Africa

  a. Nairobi, Kenya, 7 August 1998 (estimated 1000 to 1500 lbs. of explosive)
  b. Dar es Salaam, Tanzania, 7 August 1998 (estimated 1000 to 1500 lbs. of explosive)

These massive vehicular bombs have illustrated the need for substantial vehicle access denial systems to afford a buffer area between the bomb vehicle and the building or facility requiring protection. Facilities already possessing a wall and gate system have the basic essentials to ensure some distance. These may be fortified depending upon threat assessment or augmented by emplacing a barrier or maze system at access control points as illustrated in Figure 3.4-1. Mazes will slow but not stop a vehicle.

In many instances it is impossible to provide adequate buffer distance (50 to 100 m), as the building is fronted by sidewalk or street, with no wall, little or no compound, or other separating zone. In these cases it may be feasible to gain cooperation of the host government to control those streets immediately adjacent to the facility. It is recognized that this is often a difficult situation to remedy.

Substantial differences in accessibility requirements between domestic and overseas facilities will continue to be challenging in the control of vehicles. The Government has recognized the vulnerability of buildings. The problem will continue to be a combination of funding to

hydrolysis rate of most chemical agents is slow, and adequate acid catalysis is rarely observed. Alkaline hydrolysis is initiated by the nucleophilic attack of the hydroxide ion on the phosphorus atoms found in VX and the G agents.

The hydrolysis rate is dependent on the chemical structure and reaction conditions such as pH, temperature, the kind of solvent used, and the presence of catalytic reagents. The rate increases sharply at pH values higher than 8 and increases by a factor of four for every 10 C rise in temperature.

Several of the hydrolytic chemicals are effective in detoxifying chemical warfare agents; unfortunately, many of these (e.g., NaOH) are unacceptably damaging to the skin. Alkaline pH hypochlorite hydrolyzes VX and the G agents quite well.

7.10 RADIOLOGICAL DISPERSAL DEVICES (RDD)

7.10.1 INTRODUCTION AND BACKGROUND

An RDD is a device that is intended to disperse radioactive material. This is not the same as a nuclear weapon, which is a device that releases nuclear energy in an explosive manner as a result of a nuclear chain reaction involving the fission or fusion of atomic nuclei. The damage from an explosive RDD will be related to the amount of explosive material used, and will not approach that of a nuclear explosion.

An RDD will be designed to cause fear, injury, and possible lead to levels of contamination that will require large amounts of money to clean up, or even deny use of the location to people for many years. In the minds of uninformed people, a nuclear device and a radiological device may be the same, even though they are not.

CIA Director John Deutch made precisely that point in March 1996 Senate testimony. A terrorist organization, he noted, "does not necessarily need fissile material – which is more difficult to acquire – for its purposes.... But, non-fissile radioactive materials dispersed by conventional explosive or even released accidentally could cause damage to property and the environment, and cause social, political, and economic disruption."

A nuclear blast will produce residual nuclear radiation from the radioactive materials produced during the blast. These materials emit gamma rays, alpha particles, beta particles, and neutrons. These materials are similar to those used in an RDD.

It must be remembered that everyone is exposed to radiation all of the time. Natural sources are cosmic radiation and terrestrial radiation. A 5 hour air flight will expose a passenger to about 65 microsieverts. Terrestrial radiation accounts for about three quarters of the natural radiation exposure, best known is probably radon and its decay products. In addition everyone is exposed to man-made sources, the best known of which are those related to medical sources, although consumer products such as smoke detectors (Americium-241) and luminous dials (Tritium or Promethium-147) also contribute to exposure.

In order to build an RDD, the perpetrator would need to acquire radioactive material. Modern fiction, and some alarmists, have postulated that spent nuclear fuel (nuclear waste) from a civilian reactor could be used by terrorists. However this waste is so radioactive that it is impossible to handle without extensive protection, and would in all likelihood be fatal to the would-be bomb maker.

More likely sources are the local hospitals, universities, and laboratories who use equipment with radiological sources. Construction companies and steel fabricators also use equipment with radioactive sources. In such cases the handling of the more powerful source and RDD will require extensive shielding and skill.

There has been a case where suspected terrorist use of material has been reported. In late 1995, a Chechen guerrilla leader informed a Russian television network that radioactive material had been hidden around Moscow. The TV people found a 32-kilogram container that held a small amount of radioactive material in a plastic bag in a Moscow park.

Prolonged, unprotected contact with radioactive material can be fatal, depending on the activity level of the material.

7.10.2 DETECTION

Note: **Radiation is invisible, and the effects are delayed, possible by years. It can be detected and measured only with the use of instruments. The use and interpretation of these instruments requires training.**

Detection of radiation can only be made using instruments built for that purpose.

7.10.2.1 ENVIRONMENTAL MONITORING. Environmental monitoring of airborne particulates is performed using high volume, high efficiency filter or impact air samplers. The particulate samples are then evaluated using standard survey meters. For personal exposure the normal instru-

ments are pocket ionization chambers, thermoluminescent dosimeters (TLDs) and film dosimeters.

- CDV-700 Survey meter. This meter has a detection range of 0-50 mR/hr and is most useful in a decontamination area. It is designed to measure gamma radiation and, with the probe window open, it will detect high energy beta. Note: It may saturate in areas of high radiation.
- CDV-715 Survey Meter. This meter has a higher range from 0-500 R/hr. As such it would be used in an area of unknown radiation, and can be used in tandem with the CDV-700. It detects only gamma radiation.
- CDV-718 Survey Meter. This meter has a range from 0 to 10,000 R/hr and has a digital readout. The advantage of this instrument is that it can be set to alarm when either a preset dose rate or accumulated dose has been reached
- Eberline RO-20 Survey meter. This meter has a range from 0-50 R/hr. This meter measures gamma radiation, or with the window open it can measure beta.
- Ludlum Model 3 with 44-9 GM Pancake Probe. The range is 0-300 mR/hr and is most useful for checking for contamination at the contamination control point for people leaving a contaminated area and passing through decon. This meter detects alpha, beta and gamma. Be careful not to contaminate the probe.

  Ludlum Model 19 Micro R Meter. This meter detects 0 to 5000 microR/hr, and is useful for finding small sources or radiation.

he use of all of this equipment requires training.

.10.3 RESPONSE

he cornerstone for radiation protection philosophy is LARA - AS LOW AS REASONABLY ACHEIVABLE. his refers to the dose, or exposure, received by responders and people affected by the event.

here are three general guidelines for controlling exposure to ionizing radiation - minimizing exposure time, aximizing distance from the radiation source and shielding from the radiation source.

The dose received is a function of time x dose rate.

Exposure rate is reduced in proportion to the square of the distance from the source. Therefore doubling distance reduces exposure by a factor of four.

Shielding can stop beta and alpha radiation, and it can reduce gamma and neutron radiation. Shielding can include vehicles, buildings, and other objects and materials.

These factors must be uppermost in the mind of responders - they mean remove or shield people from the source. If responders must enter the hot zone, for a rescue, for example, they should plan the action in order to be in and out as quickly as possible, and to use all possible shielding.

People entering the hot zone must wear anti-contamination clothing. This will include:

- one piece clothing,
- hood,
- boots,
- gloves,
- mask, and
- a personal dosimeter which must be worn.

Remember the anti-contamination clothing does not protect from gamma or neutron radiation. A person's accumulated dose level must be monitored at all times.

> In the event of a sudden emergency some form of breathing filter – even a wet handkerchief – can afford significant protection. Inhaled contaminants can remain in the body, and particle that remain in the lungs will continue to emit radiation.

7.10.4 EXPOSURE

The EPA publishes Protective Action Guides that designate the projected radiation dose to an individual and what specific protective actions should be implemented to avoid such dosages. These are designed for use in radiological accidents, not terrorist incidents, however they designate that a maximum recommended exposure for a lifesaving operation is 25 rem. Doses in high radiation levels must be continually monitored.

7.10.5 CONTAMINATION

In the case of an RDD, the radioactive material will be dispersed by passive or active means into the air. This contamination will be the source of the radiation. A person exposed to radiation, but not actually touching the substance emitting the radiation, will not be contaminated. A person who is contaminated will be exposed to radiation.

Contamination can be further spread by people or animals walking across contaminated surfaces and collecting contaminated dirt on their shoes or feet, or on the wheels of vehicles. It must also be remembered that all water and food exposed to the radioactive material could become contaminated; if consumed, this could lead to internal contamination, which will expose internal organs to radiation until the contamination passes from the body. Contaminated plants and animals cannot be consumed.

Control zones must be established to prevent unauthorized access to contaminated areas, these should be established as soon as possible after the event and maintained until the area has been decontaminated.

A hot zone is normally established at the 1-2 mR/hr line. All individuals, materials and equipment leaving the hot zone must be monitored and decontaminated before going into the clean zone. This is done in the warm zone, which is established around the hot zone. All items, such as contaminated clothing, must be safely bagged and secured in the decon area.

Surface contamination can be removed from people and equipment by washing. Everyone and everything must be checked after decontamination has been performed. Do not forget the soles of feet!

The zones should be established by trained personnel only.

7.11.6 HEALTH EFFECTS

7.11.6.1 ACUTE EFFECTS. An acute exposure of 450 R over a very short period of time would lead to a 50% mortality rate for the exposed people, within one month, without medical treatment. Acute radiation exposure over 100 R within a short period of time can lead to acute radiation sickness. The likelihood of death depends upon the individual. Depending on the dose, acute radiation sickness symptoms can include the following:

- Changes in the blood cells
- Vascular changes
- Skin irritation
- Gastrointestinal effects
- Radiation sickness – diarrhea, nausea, vomiting, high fever
- Hair loss
- Burns.

Clinical Symptoms. Table 7.11-1 lists clinical symptoms for three dose rates for specific times after exposure.

7.11.7 TREATMENT

Skilled medical treatment is required. Symptoms such as burns may be treated in a standard fashion.

TABLE 7.11-1. CLINICAL SYMPTOMS FOR RADIATION DOSES

Time after Exposure	Sublethal Dose (100 - 200 rem)	Lethal Dose (250 - 450 rem)	Supralethal Dose (>650 rem)
24 hours	Nausea and some vomiting within hours.	Nausea, vomiting, paleness within minutes or hours.	Nausea, vomiting, extreme paleness within minutes. Shock, unconsciousness, diarrhea, abdominal pain and cramps, fever, severe skin irritation, burns or blisters, insomnia, restlessness.

Appendix BB:

"DOE Probes New Security Lapse And Accident at Los Alamos Lab,"
John J. Fialka, *Wall Street Journal*

December 11, 2000

THE WALL STREET JOURNAL.

DOE Probes New Security Lapse And Accident at Los Alamos Lab

By John J. Fialka
Staff Reporter of The Wall Street Journal

12/11/2000
The Wall Street Journal
A4

WASHINGTON -- Energy Department investigators are probing a new security lapse and a severe plutonium-poisoning accident at the Los Alamos, N.M., weapons lab: near-duplicates of problems that the facility supposedly fixed months ago.

The security problem surfaced during a secret Energy Department-run test of the security at **TA-18**, one of the lab's most heavily guarded complexes. A team of Energy Department personnel staged an attack on the night of Oct. 5, overwhelmed the beefed-up guard force and took possession of a considerable quantity of nuclear-weapons-grade enriched uranium.

The exercise resembled one that sparked an uproar among department officials in April 1997 when an attack force overwhelmed the guards and, using a garden cart, made off with simulated nuclear-weapons material.

The plutonium accident occurred March 16 and involved two teams of technicians working on a glove box -- a device that lets technicians safely handle weapons-grade plutonium by extending gloved arms into a protected box.

The teams failed to alert each other about an electrical problem. When a technician tried to fix the box by pulling on a tube, a highly radioactive and toxic gas containing plutonium contaminated the room. Eight workers were poisoned, four of them seriously.

John C. Browne, director of Los Alamos, which is managed by the University of California, insisted that the laboratory has greatly upgraded both its security and its safety programs in recent years. Work days lost from safety problems at the lab, he said, have declined sharply in five years. "Sometimes this [improved safety] gets lost in the morass of problems. You're always looking at where you can get better," he said.

After the garden-cart incident, the lab spent more than $8 million to retrain its private guards at **TA-18**, a series of small, concrete buildings located in an isolated valley. They were given heavier weapons, including armored cars, and the complex was updated with a new fence and a variety of high-tech sensors, Dr. Browne said.

Attackers in the so-called force-on-force exercise used lasers attached to unloaded weapons and sensors to mimic the firefight and keep track of who shot whom. In the latest attack, lab

masks. "In this exercise, they found it difficult to communicate, even though they'd been trained," Dr. Browne said.

But, "they were not trained on that scenario, if at all," said Gen. John A. Gordon, administrator of the Energy Department's newly constituted National Nuclear Security Administration and a retired Air Force general. He wrote a letter to Dr. Browne calling the test results "unacceptable." He later said he "wanted to make sure nobody misunderstood: that I consider this a very important facility. If there are deficiencies, I want them corrected quickly and correctly. They've assured us they've done that and we're following up on that."

The probes come at a sensitive time for the University of California, which has run the nation's two main weapons labs since the dawn of the atomic age and is in final negotiations with the department on a $10 billion contract to run them through 2005.

The latest failure comes months after Energy Department officials suggested the facility be moved to a more defensible location. In his letter, Gen. Gordon warned Dr. Browne that unless security was upgraded by the end of this month, he would shut down the facility. **TA-18** is used to model and study nuclear weapons that might be used in a terrorist attack.

"I take this very seriously," Dr. Browne said in an interview. "The image is that we were asleep at the wheel, but I don't think we are."

Referring to the plutonium poisoning, Dr. David Michaels, assistant Energy secretary for environment, safety and health, said, "This was one of the worst plutonium exposures we've ever recorded." The new investigation is focusing on the fact that the same glove box and the same technician were involved in a similar, but less serious accident in November 1998. "Our feeling is that the lessons of the first one weren't addressed," Dr. Michaels said.

The Energy Department is expected to release a report on the incident this week that could impose fines on those involved, which could be subtracted from performance fees under its current contract. Next month, the department will launch a third probe, a comprehensive review of all safety practices at the lab, the nation's largest nuclear-weapons research facility with a $1.2 billion budget and 7,000 employees.

Dr. Browne, a physicist, has directed the lab since 1997. This has been a roller-coaster year for him, including the much-publicized, but aborted spy case involving a lab scientist, Wen Ho Lee; a major forest fire in the Los Alamos area and a still-mysterious case of computer-disk drives containing nuclear-weapons secrets that disappeared and then suddenly reappeared.

Ahead remains the question of who will run the labs in the future. Scientists at the laboratory strongly favor retention of the University of California, rather than several large defense contractors who have shown interest in taking over the labs' management contract. So far, the department has focused on negotiating an extension of the contract, set to expire in 2002, for three more years -- if security and management controls can be improved.

It is unclear where a new presidential administration might take these negotiations. Among other universities that have expressed some interest in running the labs is the University of Texas.

Appendix CC:

Overheads from Integrated Cyber Security Initiative

August 29 & 30, 2000

Meeting Purpose & Goals

- Opportunity to talk about issues, options, and alternatives
- Accelerate near term enhancements
- Recommendations and near-term strategies for
  - Media-less implementation / enclosures
  - Identification of sensitive/high value information types
  - Reducing number of classified systems and system administrators
  - Validation of need-to-know decisions
- Status of phase 2 encryption initiative

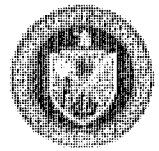
Meeting Objectives

- Identify short/near-term issues (must integrate with long term)
- Recommended courses of action
- Expected outcome (risk assessment)
- Applicability (labs/plants/both??)
- Policy impacts
- Recommended schedule (quick,near-term, long-term)
- Develop cost estimates
- Consider impact of multiple LPSOs
- Cost benefit analysis
- Roles and responsibilities

Media-Less Workstation

- Steps to implement media-less workstation recommendation
  - Prioritize assets
  - Develop standard approach or common operating environment
    - DP-11 convene working group
    - Draft complete by 9/15
  - Implement as funding is made available
  - Develop plan for migration to new policy
    - Sites report number of systems, estimated costs, and target completion date to DP-11 by 9/11
    - Implement for highest priority information types first

ICSI Media-Less Workstations (continued)



- Priority 1 Information Assets
  - Sigma 14 data
  - Sigma 15 data
  - Special Access Programs
  - Top Secret data
  - Weapons test data collection
- Priority 2 Information Assets
  - Sigmas 1 and 2 data
- Priority 3 Information Assets
  - Other sigmas
  - SNSI
  - CNSI

Longer-term issues for ICSI planning and design

- Hiring more system administrators
- Standards for system administrator certification
- PKI
- Separation of roles
- Malicious codes
- Classified via FIS
- Need to be able to communicate and share information; some sites are not aware of numerous incidents because they are classified

Next Step

- Complete documentation of accomplishments, recommendations, policies
- Group review of documentation
- Presentation of recommendations to DP-1
  - Funding decision
- Implement funded recommendations

Meeting Results

- Explain what has been accomplished
- Identify activities to start, continue, or enhance
- Identify new or modified policies
- Recommendation for media-less systems

ICSI Explanation of Accomplishments

- Develop report and briefing on accomplishments since April 1999
  - Policy
  - Labs
  - Plants
- NTK accomplishments needed to be communicated better
- Input due to DP-11 by 9/11
- Draft report to group by 9/18

Activities to Start/Continue/Enhance

- Automated configuration management
- Automated log analysis
- Off host log analysis
- Intrusion detection
- Review number of systems approved for classified processing
  - Current information to DP-11 by 9/15
  - Complete review within next 60 days
- Review accounts on multi-user systems
  - Review results to DP-11 within next 60 days
- Red team review

Activities to Start/Continue/Enhance

- Anomalous use detection
- Switched networks (yellow)
- Port locking
- Modem detection
- Honey pots
- Automated intrusion detection response
- Credential review (yellow)

Policies

- Email scanning
  - Options
    - Policy that will preserve ability to monitor email
    - Policy that says we don't think this is cost effective
    - Counterintelligence doing traffic analysis (looking for classified in common email)
  - Approach
    - Leverage CN EMAC
    - Provide capability to conduct selected email scanning
- Archive scanning
  - Experience indicates minimal results for expended resources
  - Approach
    - Stop scanning of archives

Policies (continued)

- Media-less Workstations
  - Default workstation configuration for classified data processing is media-less
  - Exceptions must be documented
  - Exceptions must be approved by Designated Approving Authority
  - Policy must be part of defense-in-depth solution

- Laptops for Classified Data Processing
  - Default - Classified data processing on laptops is NOT allowed
  - Exceptions must be documented
  - Exceptions must be approved by Designated Approving Authority
  - DP work with labs and plants to develop migration plan

Appendix DD:

Letter from Peter D. H. Stockton, former DOE Special Assistant to: Senator Richard Shelby

September 13, 2001

Peter D.H. Stockton
40332 Mt. Gilead Rd.
Leesburg, VA 20175
(703)589-1718

September 13, 2001

Senator Richard Shelby
Hart Senate Office Building Rm. 110
Washington, DC 20510

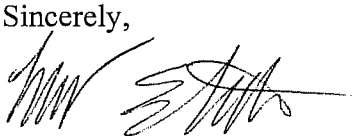
Dear Senator Shelby,

As you will recall, in March shortly after leaving Department of Energy (DOE), I met with you, Senator Wyden, and the Senate Intelligence Committee staff to discuss the problems with security at the DOE nuclear weapons facilities. Three other DOE and Department of Defense (DOD) security experts accompanied me to the briefing who not only run performance tests at the nuclear facilities, but also analyze the adequacy of the security at these sites. As I mentioned at the briefing, there are eleven current and former DOE and DOD security experts who are willing to testify before Congress because they feel so strongly about the matter - but otherwise do not want to be identified for fear of retaliation. Our briefing to you focused on the startling fact that DOE nuclear facilities' guard forces lose well over 50% of the credible force on force performance tests - mock terrorist attacks - a clear indicator that a number of facilities cannot protect special nuclear materials, weapons, and highly classified information from theft or sabotage.

You advised that the Senate Intelligence Committee could not investigate the issue because of jurisdictional problems, therefore, you suggested we also brief the Senate Armed Services Committee and the Senate Government Affairs Committee who have clear jurisdiction over the weapons program. Although I followed up on your suggestions, the range of responses was almost comical: the staff director of one committee didn't want to embarrass his political party although it was impressed upon him that this was clearly not a partisan issue; another key staffer understood the problem but didn't want to pursue it; and the staff director at another committee professed interest, but never followed up. I met with committee staff under both Republican and Democratic control, but to no avail.

Over the last several months we have written an unclassified report based on unclassified sources that will shortly be released by the Project On Government Oversight (POGO). I believe this report will inform the Congress as to the problem of security at DOE, including a series of recommendations to solve the problems. It is important for the Congress to focus on this problem now, particularly in light of the growing sophistication of the terrorist threat as recently demonstrated. I hope that you and your Committee will reconsider your ability to get involved in this issue, given that it is so obviously vital to the health and safety of our public.

Sincerely,



Peter D.H. Stockton

Appendix EE:

"Draft Statement of Facts, Nuclear Security: Improvements Needed in DOE's Safeguards and Security Oversight," General Accounting Office Draft Report

December 14, 1999

United States General Accounting Office

GAO

Draft Statement of Facts

December 14, 1999

NUCLEAR SECURITY

Improvements Needed in DOE's Safeguards and Security Oversight

Notice:
This draft is restricted to official use.

BACKGROUND

DOE has numerous contractor-operated facilities and laboratories that carry out various DOE programs and missions. They conduct some of the nation's most sensitive activities, including designing, producing, and maintaining the nation's nuclear weapons; conducting efforts for other military or national security applications; and performing research and development in advanced technologies for potential defense and commercial applications. Because of these sensitive activities, these facilities, especially the laboratories, are targets of foreign espionage efforts.

Security concerns and problems have existed at many of these facilities since they were created. Recent years have been no different. In 1997, DOE's Office of Security Affairs issued a report that rated safeguards and security at some facilities and laboratories as marginal and identified problem areas that included physical security and accountability for special nuclear material.[1] In March 1999, there were allegations that a scientist at the Los Alamos National Laboratory transferred huge amounts of secret data from a computer system, thereby compromising virtually every nuclear weapon in the United States' arsenal. In April 1999, computer networks at the laboratories were shut down because of concerns about inadequate security. During that same month, we testified on numerous long-standing safeguards and security problems, including ineffective controls over foreign visitors, weaknesses in efforts to control and protect classified and sensitive information, lax physical security controls, ineffective management of personnel security clearance programs, and weaknesses in tracking and controlling nuclear materials.[2]

DOE is responsible for administering a security program that effectively protects against theft, sabotage, espionage, terrorism and other risks to national security. DOE has policies and procedures to protect its facilities, classified documents, data stored in computers, nuclear materials, nuclear weapons, and nuclear weapons components. To ensure that these policies and procedures are followed and implemented, DOE has two primary oversight organizations, the Office of Safeguards and Security Evaluations (OSSE) and the field operations offices. These offices play a critical role

[1] Status of Safeguards and Security for 1996 (Jan. 27, 1997).
[2] Department of Energy: Key Factors Underlying Security Problems at DOE Facilities, (GAO/T-RCED-99-159, Apr. 20, 1999).

in the early detection of safeguards and security problems and can play a major role in the timely resolution of those problems.

DOE's operations offices are the line organizations accountable for oversight of the laboratories' safeguards and security activities. This is because the operations offices are responsible for managing the contracts for the operation of DOE's facilities and for ensuring that DOE's policies, procedures, and requirements are followed. The operations offices are required to conduct an annual survey of the adequacy of the operating contractors' safeguards and security programs. DOE's Albuquerque Operations Office is responsible for the Los Alamos National Laboratory and has safeguards and security staff at a Los Alamos Area Office to provide on-site management and oversight. DOE's Oakland Operations Office is responsible for the Lawrence Livermore National Laboratory and has safeguards and security staff located at the Laboratory to provide a day-to-day presence.

OSSE provides oversight of laboratory safeguards and security activities from DOE headquarters. OSSE is an "independent" oversight organization that is separate from line management structure and conducts safeguards and security inspections of DOE facilities and issues reports.[3] OSSE has existed in various forms since 1982. Previously named the Office of Security Evaluations, this Office was originally organized under DOE's Office of the Assistant Secretary for Defense Programs. In 1991, the Office of Security Evaluations was moved to DOE's Office of the Assistant Secretary for Environment, Safety, and Health. In 1999, the Office of Security Evaluations was renamed the Office of Safeguards and Security Evaluations and was moved to the Office of Independent Oversight and Performance Assurance, which reports directly to the Secretary of Energy.

Additional organizations have provided safeguard and security oversight as the need has occurred. For example, DOE's Office of Counter Intelligence conducts evaluations of counter intelligence activities at DOE's facilities and DOE's operating contractors at the laboratories conduct annual self-assessments of the quality of their safeguards and security programs. In addition, the

[3] Findings in OSSE reports have been referred to as "issues" in some OSSE reports. In this report we will refer to all OSSE findings as findings. OSSE has also used different terms for the reviews it conducts, including inspections, evaluations, and profiles. In this report we will refer to all OSSE reviews as inspections.

contractors also have internal audit organizations that review aspects of the safeguards and security programs. GAO and DOE's Office of Inspector General also evaluate selected safeguards and security activities. Finally, outside organizations have also reviewed the laboratories' safeguards and security activities.[4] However, OSSE and the operations offices are the only DOE organizations responsible for continuing oversight of safeguards and security activities at the laboratories.

DOE LACKS A COMPREHENSIVE TRACKING SYSTEM FOR SAFEGUARDS AND SECURITY FINDINGS

DOE and the contractors that operate the Los Alamos National Laboratory and the Lawrence Livermore National Laboratory use a number of information systems to track safeguards and security findings that have been made by DOE oversight organizations. DOE headquarters maintains the Safeguards and Security Information Management System and the contractors that operate Los Alamos National Laboratory and the Lawrence Livermore National Laboratory maintain their own information systems. These systems, however, do not include information on all safeguards and security findings, are not accessible by all necessary personnel, and/or are not capable of interfacing with each other.

Not one of the information systems maintained by DOE and the laboratories contains information on all safeguards and security findings at the laboratories. DOE's Safeguards and Security Information Management System contained information on all OSSE and operation office survey safeguards and security findings and corrective action plans until 1995. From 1995 to 1999, information on OSSE findings and related corrective action plans was not included in the system. Because OSSE did not highlight or number findings in its reports, staff responsible for correcting safeguards and security could not identify the findings and enter them into the information systems. In 1999, OSSE changed its inspection report format to more clearly identify its findings and OSSE's findings are now being included in the Safeguards and Security Information Management System. The Safeguards and Security Information Management System has never included information related to findings made

[4] In January 1999, a special security review team issued an Internal Report to the Secretary, Special Security Review. Also, in January 1999, a House of Representatives Select Committee issued a report that dealt with security at DOE's facilities entitled U.S. National Security and Military/Commercial Concerns With the People's Republic of China.

by organizations other than OSSE and the operations office, such as GAO, DOE's Office of the Inspector General, and DOE's Office of Counter Intelligence.

At both Los Alamos National Laboratory and Lawrence Livermore National Laboratory, the operating contractors maintain their own comprehensive computerized information systems. These systems contain findings and corrective action information for OSSE findings (from 1995 to 1999, the OSSE findings that the laboratories could identify were included in their systems), operations office survey findings, findings from self–assessments performed by the contractors or internal audits, and findings from any other source that the contractor is aware of. However, the laboratories' information systems include only those findings related to their laboratory and do not include findings for other DOE facilities. In addition, these systems are not compatible with the Safeguards and Security Information Management System and information from one system cannot be compared or downloaded between systems. Maintaining duplicate and/or overlapping systems that are not compatible with each other increases costs and decreases efficiency.

In addition to not including all findings, the Safeguards and Security Information Management System is not readily available to all DOE and contractor personnel that need to access information on safeguards and security findings. The Safeguards and Security Information Management System is available to safeguards and security staff at DOE headquarters and to operations office personnel. DOE area office staff and personnel working for the laboratories' operating contractor who work on safeguards and security issues do not have direct access to the Safeguards and Security Information Management System and must request information through one of the organizations that does have direct access. Laboratory officials believe that access to a centralized, comprehensive system would facilitate tracking corrective actions and would enable the laboratories to use information from other facilities to improve their safeguards and security programs. For example, such a system could aid in the identification of the most cost effective actions to correct safeguards and security problems or could be the basis for trend analyses across laboratories. Information about problems at one facility could also allow managers at other facilities to avoid similar problems.

OSSE officials informed us that they saw a need for a comprehensive safeguards and security information system. They informed us that while they did not intend to develop or maintain such a

system, they were holding discussions with the Office of Security and Emergency Operations about the possibility of creating a central safeguards and security information system.[5]

IMPROVEMENTS NEEDED IN CORRECTING AND CLOSING FINDINGS

When the DOE operations office or OSSE report a finding that raises a significant security vulnerability, the contractor must immediately take any necessary compensatory action to eliminate any risks. Analysis of operations office's survey findings and development of the corrective action plans to permanently correct the findings must be completed within 15 or 30 days (depending on the facility's overall safeguards and security rating assigned) and must be approved by the operations office. As part of the development of the corrective action plan, the laboratory must conduct risk assessment, root cause analysis, and cost-benefit analysis. The operations office must validate and verify that the survey findings have been corrected and certify closure of the finding. We found that the laboratories were not always conducting the required analyses or providing a justification of why the analyses were not conducted. In addition, OSSE has not been involved in development, validation and verification, and closure of its findings.

Need for More Formal Corrective Action Analyses

DOE Order 0 470.1 requires that corrective actions developed for operations office's survey findings be based on documented risk assessment, root cause analysis, and cost-benefit analysis. Risk assessment is essential to determine the risk associated with an identified deficiency in prioritizing its correction. Root cause analysis ensures determination of the fundamental and contributing causes of a deficiency. Cost-benefit analysis is important in determining whether correcting a security risk is worth the cost of corrective action. Risk assessments, cost benefit analyses, and root cause analyses are not always appropriate. However, the corrective action plan process should include a formal determination of whether these analyses are appropriate.

---

[5] The Secretary of Energy established the Office of Security and Emergency Operations in May 1999 to consolidate the management of several security programs, including safeguards and security policymaking.

We reviewed 15 findings related to safeguards and security problems at the Los Alamos National Laboratory and 13 findings related to safeguards and security problems at the Lawrence Livermore National Laboratory. Most of the findings we reviewed have been corrected and closed and at the Lawrence Livermore National Laboratory risk assessments, root cause analyses, and cost benefit analyses had been performed as required.[6] However, we found that at the Los Alamos National Laboratory, not all the required analyses had been performed during the corrective action process.

Of the 15 findings at the Los Alamos National Laboratory, 10 were findings from Albuquerque Operations Office surveys and 5 were from OSSE inspections. These findings were developed from 1994 through 1999. Los Alamos National Laboratory safeguards and security staff did not perform root cause analyses for 5 of the 15 findings. A root cause analysis was not conducted for one finding because the finding was closed while the Albuquerque Operation Office was conducting the survey. For the other four findings, laboratory safeguards and security officials said that root cause analyses were not conducted because the findings occurred before the laboratory required that root cause analysis be documented.

Formal risk assessments (or justifications for not doing formal risk assessments) were not completed for any of the 15 Los Alamos National Laboratory findings that we reviewed. Los Alamos National Laboratory safeguards and security officials told us that formal risk assessments are not conducted because the laboratory does not require this to be done. They said that risk assessments have been conducted informally immediately upon learning that a safeguards and security problem has been discovered, but these assessments are not documented. If classified information or nuclear material is at risk, their first priority is to ensure that adequate compensatory measures are put into place.

---

[6] Safeguards and security staff at the Lawrence Livermore National Laboratory did not perform risk assessment, root cause analyses, and cost-benefit analyses for three of the findings we reviewed because they were findings contained in OSSE's 1997 Site Profile and laboratory staff believed that the issues raised were not formal findings and corrective action plans were not required. In addition, a cost benefit analysis was not performed for one Oakland survey finding that involved the use of certain kind of lock on a room that contained classified printers. Laboratory safeguards and security staff conducted a risk assessment and a root cause analysis for this finding; but did not conduct a cost benefit analysis because the printer room had been eliminated shortly after completion of the survey and the finding was no longer applicable

Cost-benefit analyses were also not completed for any of the 15 Los Alamos National Laboratory findings that we reviewed. Los Alamos National Laboratory safeguards and security officials told us that they did not perform any cost-benefit analyses for these findings because the majority of the findings involve compliance with DOE regulations and must be corrected. While formal cost-benefit analyses (or formal justifications why cost-benefit analyses were not necessary) were not performed, the safeguards and security officials said that cost-benefit of a corrective action plan is considered for all findings.

An example of how these analyses can benefit the corrective action process involves a 1999 OSSE finding that appeared to require replacement of doors to special nuclear material vaults at the Lawrence Livermore National Laboratory. DOE requires that the doors and walls to a vault containing special nuclear material provide the same protection from unauthorized entry. For this finding, Lawrence Livermore National Laboratory officials conducted root cause, cost benefit, and risk analyses and determined that the new vault doors would cost about $200,000 and installation of the doors would cost an additional $1 million, without providing a significant increase in security. As a result, instead of proceeding with the upgrade to close the finding, in November 1999 Lawrence Livermore National Laboratory officials requested a variance from the DOE requirement.

OSSE Does Not Validate Or Certify Closure of Its Findings

DOE's operations offices follow a process for closure of their survey findings that involves them in the development, validation, verification of the corrective action and closure of the finding. OSSE has not followed a similar process for its safeguards and security findings. Once OSSE identified a safeguards and security finding, OSSE maintained little or no involvement in its correction. For the OSSE findings that the laboratories were able to identify in the OSSE reports, the laboratories worked with the operations offices to develop corrective action plans and close the finding. However, the laboratories were not able to identify all findings that OSSE believes it made. For example, in 1998 OSSE issued a site profile report for the Lawrence Livermore National Laboratory that it believed contained eight findings. Of those eight findings, six were identified by the laboratory when it reviewed the report. The two findings identified by OSSE and not by the

laboratory concerned protective force and personnel security issues. In addition, the laboratory identified what it thought was a finding concerning materials control and accountability issues. However, this was not one of the eight findings that OSSE made. For those findings that OSSE made but were not identified by the laboratories, no corrective action plan was completed and, since the finding was never identified it was never closed. There is no assurance that such findings were corrected until OSSE returned for the next inspection.

There are no DOE requirements for OSSE's involvement in corrective action. However, by not being involved in the corrective action, OSSE was not able to ensure that the safeguards and security finding was understood, adequately corrected, and closed. In addition, by not being involved in the corrective action process, for those findings that the laboratories were not able to identify, OSSE was not aware that the finding was not being corrected. In most cases, OSSE officials were not aware of the status of the finding until they returned to the laboratory for another inspection several years later.

In its 1999 inspections at Los Alamos National Laboratory and Lawrence Livermore National Laboratory, OSSE changed its processes. The inspection report clearly identified and numbered (for use in the Safeguards and Security Information Management System) the findings. In addition, OSSE worked with the laboratories in developing a corrective action plan, and approved those plans when they were satisfactorily completed. OSSE does not, however, plan to formally validate and certify closure of the findings. The operations offices will continue to validate and certify closure of the OSSE findings. The changes in OSSE's involvement in the corrective action process is the result of the Secretary of Energy's initiatives to strengthen DOE headquarters' management of all safeguards and security issues.

SAFEGUARDS AND SECURITY RATINGS PRESENT CONFLICTING RESULTS

During a single year, the Los Alamos National Laboratory and Lawrence Livermore National Laboratory receive ratings on their safeguards and security performance from several sources that can range from "unsatisfactory" to "far exceeds expectations". Ratings are included in some inspections conducted by OSSE and in the surveys conducted by the operations offices. The contractors also receive an annual contract performance rating for safeguards and security from DOE that determines the size of the contractor's performance award. Finally, DOE is required to provide the President with an annual report on the status of safeguards and security at DOE's facilities. Safeguards and security ratings have the potential to provide managers and policy-makers with a "report card" on the status of safeguards and security and a given facility and throughout the complex. In recent years, however, ratings have provided conflicting information on the status of safeguards and security or, in cases where the ratings were not reported, provided no information on the status of safeguards and security.

Conflicting Ratings

Over the past 5 years, Los Alamos National Laboratory and Lawrence Livermore National Laboratory each received 15 safeguards and security ratings in OSSE reports, Albuquerque Operations Office surveys, DOE contract performance ratings, and reports to the president. The following two tables shows these ratings for the Los Alamos and the Lawrence Livermore national laboratories.

Table 1: Safeguards and Security Ratings for Los Alamos National Laboratory From 1994 through 1999.

Year	OSSE	Operations Office	Contract Performance	Report to the President
1994	No rating given	Marginal	Exceeds expectations	Marginal
1995	Inspection not conducted	Satisfactory	Far exceeds expectations	Satisfactory
1996	Inspection not conducted	Survey not conducted	Far exceeds expectations	Satisfactory
1997	No rating given	Marginal	Meets Expectations	Report not issued
1998	No rating given	Marginal	Excellent	Marginal
1999	Satisfactory	Marginal	To be determined	To be determined

Table 2: Safeguards and Security Ratings for Lawrence Livermore National Laboratory From 1994 through 1999.

Year	OSSE	Operations Office	Contract Performance	Report to the President
1994	Inspection not conducted	Survey not conducted	Excellent	Satisfactory
1995	Inspection not conducted	Satisfactory	Far exceeds expectations	Satisfactory
1996	Inspection not conducted	Satisfactory	Far exceeds expectations	Marginal
1997	No rating given	Satisfactory	Far exceeds Expectations	Report not issued
1998	No rating given	Marginal	Good	Marginal
1999	Marginal	Marginal	To be determined	To be determined

As shown in these tables, the ratings assigned to safeguards and security can vary widely during a given year. For example, at Lawrence Livermore National Laboratory in 1996, the Oakland Operations Office safeguards and security survey rated the laboratory as "satisfactory", the safeguards and security contract performance rating was "far exceeds expectations", and the annual report to the President assigned a "marginal" rating. A similar situation occurred at the Los Alamos

National Laboratory in 1998. In that year both the Albuquerque Operations Office safeguards and security survey and the annual report to the President rated the laboratory as "marginal" while the safeguards and security contract performance rating was "excellent".

There are several reasons why this disparity occurs. One reason is that the criteria for the ratings are not the same. In their surveys, the operations offices use DOE policies, procedures, requirements, and orders designed to protect classified information and material to measure the laboratories' safeguards and security performance. The ratings assigned for contract performance are based on a different set of criteria, which are negotiated between DOE and the contractors operating the laboratories. In the past, the contract performance criteria have often been process oriented. For example, 1998 performance criteria in the Los Alamos National Laboratory contract included the percent of corrective action plans completed on time, the number of self-assessments completed, and the percentage of time nuclear material is in its stated location and is correctly identified. The contract performance criteria specified that safeguards and security ratings from OSSE and the Albuquerque Operations Office were not to be factored in the performance award. In contrast, OSSE and operations office inspections and surveys are based on criteria designed to determine the capability of the laboratory to protect classified information and nuclear material.

To some extent, another reason for the disparity in the rating can be the timing of the inspection or survey. For example, in 1999, Albuquerque Operations Office conducted its annual survey of the Los Alamos National Laboratory in April 1999. This survey rated safeguards and security at the laboratory as "marginal". OSSE conducted its 1999 inspection of safeguards and security at the Los Alamos National Laboratory in July 1999 and rated Los Alamos' safeguards and security as "satisfactory", noting significant improvements in the program since the operations office's survey. A third explanation for the disparate safeguards and security ratings can be the scope of the reviews conducted. For example, in 1996 the Report to the President rated the Lawrence Livermore National Laboratory "marginal" while the Oakland Operations Office rated them "satisfactory". However, the scope of the Report to the President included only program management and protective program operations while the Oakland Operations Office Survey included all five major safeguards and security topical areas.

While several factors may explain the disparate ratings, the wide variance in the ratings in a single year raises questions about the credibility of the rating process. The ratings could also provide government managers and policy-makers with distorted views of the status of safeguards and security at the laboratories and could allow developing problems to be overlooked. A logical assumption for a manager or policy-maker would be that if an operating contractor is receiving ratings of "far exceeds expectations" and near maximum contract performance awards for safeguards and security, then the safeguards and security program must be doing a good job of meeting requirements to protect classified information and material. However, review of a survey for the same laboratory, for the same year, would reveal a marginal rating with numerous findings of noncompliance with safeguards and security policies and requirements.

DOE is working to correct this situation and the ratings given for contract performance and inspections and surveys may not be as disparate in future years. Seventy-five percent of the safeguards and security contract performance rating for Los Alamos National Laboratory and Lawrence Livermore National Laboratory for 2000 will be based on inspection and survey ratings. The remaining 25 percent of the contract performance rating will be based on the laboratories' ability to produce corrective action plans within the designated timeframes.

The criteria included in the 2000 contract for the Los Alamos National Laboratory and the Lawrence Livermore National Laboratory are unique to these laboratories and can be different from the criteria used at other DOE facilities. For example, the 2000 contract for DOE's Sandia National Laboratory allows for consideration of OSSE ratings in the performance rating, but does not specify that it has to be considered. In addition, the contract performance criteria for the Sandia National Laboratory contains process oriented criteria such as the completion of corrective action plan milestones and the percentage of security guards that can pass firearms proficiency tests. Contract performance criteria for DOE's Pantex and Kansas City facilities allow consideration of safeguard and security survey ratings, but do not specify its weighted importance.

Evaluations of Safeguards and Security Activities
Were Not Consistently Performed

As shown in tables 1 and 2, only the contract performance ratings were completed in each of the past 5 years for Los Alamos National Laboratory and Lawrence Livermore National Laboratory. OSSE inspection ratings were not assigned for Los Alamos National Laboratory and the Lawrence Livermore National laboratory in 1994, 1995, 1996, 1997, and 1998. Albuquerque Operations Office did not assign a rating for safeguards and security for the Los Alamos National Laboratory in 1996, and the Oakland Operations Office did not assign a safeguards and security rating for Lawrence Livermore National Laboratory in 1994. Finally, the Report to the President was not issued in 1997; instead issuing a combined 1997/1998 report.

The Director of OSSE informed us that inspections were not conducted annually from 1994 through 1998 because Secretarial interest in the safeguards and security area waned and staff allocated for safeguards and security inspections was reduced. According to Albuquerque Operations Office safeguards and security officials, the 1996 annual safeguards and security survey was not conducted because in 1994 OSSE had performed an extensive inspection and the problems noted in that inspection were being corrected. DOE headquarters safeguards and security officials concurred in cancellation of the survey. Oakland Operations Office safeguards and security officials informed us that the 1994 safeguards and security survey was not conducted because OSSE had done a comprehensive inspection in late 1993. According to DOE officials, the annual Report to the President was not issued in 1997 because there was indecision about which DOE organization should write the report.

Appendix FF:

Dear Colleague letter from Representative Curt Weldon

June 22, 1999

CONGRESSMAN CURT WELDON

7th District Pennsylvania

June 22, 1999

Protect DOE Whistleblower Against Retaliation

Dear Colleague,

I am writing to enlist your support on behalf of Lt. Col. Edward J. McCallum, the dedicated Department of Energy employee who fought for years to improve the safety and security of our nation's nuclear laboratories -- and is now being targeted as a result. Lt. Col. McCallum has been DOE's Director of Safeguards and Security for ten years, and a Department employee for twenty-five years. Throughout the past decade, this former Green Beret officer attempted numerous times to alert the Administration to grievous lapses in security which left our nation's nuclear facilities vulnerable to foreign espionage and terrorist attack. Officials at the highest levels, including three Secretaries of Energy and White House personnel, consistently ignored Lt. Col. McCallum's warnings, placing our national security in jeopardy.

Now that the Cox-Dicks Committee has revealed the details confirming one of the most extensive and successful campaigns of nuclear espionage against this country, we are paying the price for the Department's disregard of Lt. Col. McCallum's assessments. Astoundingly, the Administration is now attempting to demonstrate "accountability" in the aftermath of the Cox report by firing Lt. Col. McCallum -- one of the few responsible individuals who could have helped it prevent the stealing of nuclear secrets. Wary that Lt. Col. McCallum will focus attention on the Administration's failure to heed his warnings, the DOE has lodged unsupported charges against him and placed him on administrative leave. This "shoot the messenger" approach is not only grossly irresponsible, but it suggests that the Administration is more committed to preventing further criticism of its programs than working to make credible reforms with those who have an in-depth understanding of the problems.

Lt. Col. McCallum deserves accolades for what he did to protect our national security --- not the continued destruction of his reputation and career. Congress must make it clear that the sacrifice of this dedicated public servant will only exacerbate our concerns about the Administration's past failings while raising continued doubts about the effectiveness of any reforms being implemented. I urge you to join with us in protecting Lt. Col. McCallum against the Administration's retaliatory effort by signing the attached letter to Secretary Richardson. Please contact Nancy Lifset in my office (X5-2011) if you are interested in signing or need additional information.

Sincerely,

Curt Weldon

Curt Weldon
Member of Congress

Draft of Letter to Energy Secretary Bill Richardson

Dear Mr. Secretary:

We are writing to protest the Department's actions with regard to Lt. Col. Edward McCallum, the dedicated DOE employee who fought for years to improve the safety and security of our nation's nuclear laboratories.

As DOE's Director of Safeguards and Security for ten years, and a Department employee for twenty-five years, this former Green Baret officer attempted numerous times to alert the Administration to grievous lapses in security which left our nation's nuclear facilities vulnerable to foreign espionage and terrorist attack. Those warnings were consistently ignored by the Department's leadership and White House personnel, placing our national security in jeopardy.

Now that the Cox-Dicks Committee has revealed the details confirming one of the most extensive and successful campaigns of nuclear espionage against this country, we are paying the price for the Department's disregard of Lt. Col. McCallum's assessments. The Administration's consideration of an "accountability" strategy that includes the firing of Lt. Col. McCallum is astounding. This "shoot the messenger" approach is not only grossly irresponsible, but it suggests that the Administration is more committed to preventing further criticism of its programs than working to implement credible reforms.

The Department will make no headway in resolving congressional concerns by removing one of the few responsible individuals who could have helped the Administration avoid the stealing of secrets. He is one of the few knowledgeable employees in whom we still have confidence to fix the problems that were revealed. The continued launching of unsupported charges against Lt. Col. McCallum will only serve to increase suspicions about Administration officials' liability for the problems that developed.

Lt. Col. McCallum deserves accolades for his efforts to protect national security -- not the continued destruction of his reputation and career. We want to convey in no uncertain terms that the sacrifice of this dedicated public servant will only exacerbate our concerns about the Administration's past failings while raising continued doubts about the effectiveness of any reforms being implemented. We ask that you publicly denounce these retaliatory attacks on Lt. Col. McCallum, and act to ensure his job security.

Appendix GG:

"Memorandum for the Headquarters NNSA Team," Bob Kuckuck, Principle Deputy Administrator, National Nuclear Security Administration

August 20, 2001

August 20, 2001

MEMORANDUM FOR THE HEADQUARTERS NNSA TEAM

FROM: Bob Kuckuck
Principal Deputy Administrator

SUBJECT: NNSA Headquarters Reorganization

On March 14, 2001, John Gordon announced plans to reorganize the Headquarters components of the NNSA to improve our ability to perform the NNSA core mission and to enable us to function semi-autonomously within the Department of Energy. As John's Deputy and as the Chair of the NNSA Management Council, I am writing to let you know that he formally approved the high-level structural changes associated with establishment of the NNSA Headquarters on August 2, 2001. I also want to advise you of the process, schedule and next steps agreed to by the Management Council to fully implement the new structure.

The Management Council is striving to ensure that the welfare of each NNSA employee is given the highest priority in every step of the reorganization process. Personally, I have stressed to the Council the importance of communicating with every employee all of the details of this complicated process. Please recognize that there are required formal steps that must be carried out which involve the consideration of employee rights and labor relations obligations. If you are not fully current on this process and its impacts on you and your current and/or future responsibilities, please talk with your supervisor.

NNSA HQ STRUCTURE

On May 3, we delivered a report to the U.S. Congress that explained how NNSA will be structured and outlined our plan for standing up the Headquarters structure by October 1, 2001. The primary structural changes, as illustrated in the attached organization chart, are the addition of support components which will address critical operational and administrative functions, thus enabling our program components to focus on our core mission. Two new support organizations have been added: Facilities and Operations (F&O) and Management and Administration (M&A). There are five offices within F&O and six offices within M&A. In addition, an Office of Emergency Operations has been established.

STAFFING THE NEW STRUCTURE

This reorganization is predominantly a functional realignment – with many employees continuing to perform their current functions in a new structure. A draft crosswalk of employees from the old to the new structure has been prepared and we have asked DOE's Office of Human Resources Management to review each proposed employee movement and the associated position descriptions

to ensure that any employee entitlements are being appropriately administered. We expect this review will be completed by the end of August.

Actual transfers will be effective on October 1, 2001, at which time we expect that just over 100 Defense Programs (DP) staff and about 20 Defense Nuclear Nonproliferation (NN) staff will be realigned or reassigned to one of the new NNSA Headquarters support components as part of the reorganization. Before October 1, many of these same employees will be detailed into the new organizations but will continue to report to their current supervisor. Indeed, the Administrator has already announced a number of details involving senior managers to establish the new structure. Each employee's appraisal for the past year, however, will be performed by his or her current supervisor.

I have asked each of your managers to ensure that everyone who is affected by this reorganization be fully informed before it becomes effective on October 1. Again, if you have any questions, please ask your supervisor.

During this reorganization we must also fulfill labor management obligations. To begin this process, the local union chapters have both been briefed by the NNSA Office of Human Resources. We are also establishing new organizational codes and routing symbols for all NNSA organizational components

IMPACTS ON NNSA EMPLOYEES

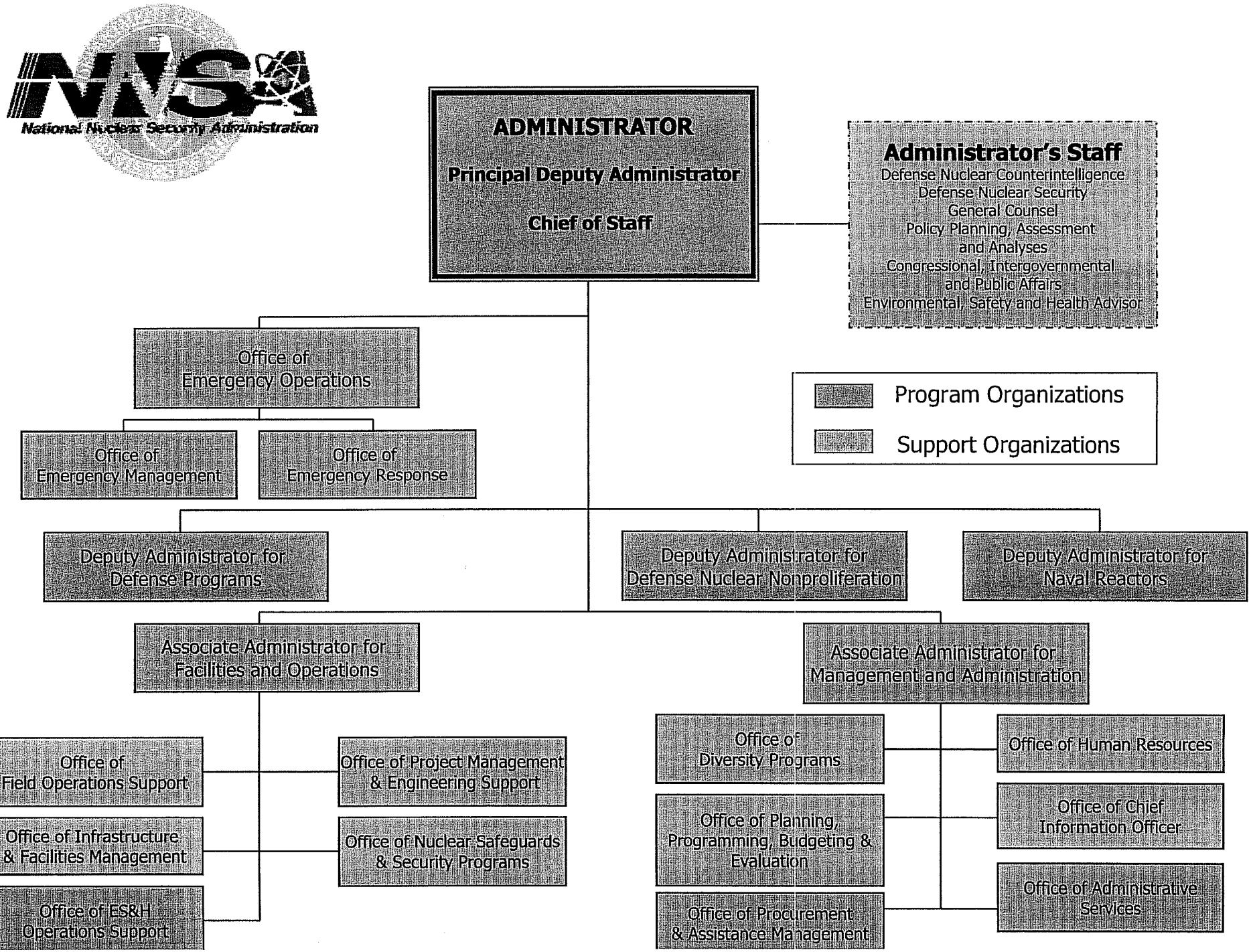
No adverse impact on employees is anticipated. No employee will be asked to geographically relocate, but consolidation of some staff from multiple offices will be needed to improve efficiencies and build new work teams.

AFTER OCTOBER 1, 2001

Let me be clear that having the reorganization complete "on paper" does not mean that our work is done. Additional organizational adjustments will be required. We will need to continue to establish and communicate new roles, responsibilities, processes and policies to realize the increased effectiveness intended by the creation of the NNSA. Change is not easy and we all understand and feel the stress it brings about. However, I am confident that the steps we are taking are the right ones and will lead us to achieving our vision of NNSA as an integrated nuclear security enterprise operating an efficient and agile complex.

At this stage in our progress, we ask for your support as well as your continued focus on our mission and the work before us as we strive to reorganize ourselves and improve the way we do business. My commitment to you is to provide on-going communication about what is happening, when and why. To that end, we have established an internal website to provide the NNSA Team with up-to-date information about reorganization activities. For example, it contains the memo signed by John Gordon approving the creation of the new support components and the high-level missions and functions statements defining the responsibilities of these new elements. You can view this site at: https://intranet.nnsa.doe.gov.

Our new human resources group is also ready to help answer any questions related to your employment status or benefits. You can reach Ray Greenberg on 3-6802 or 6-3661, or Mike Kane on 6-5753. Working together as a team, we will successfully build a stronger, more effective mission-centered NNSA. Thanks for your support.


National Nuclear Security Administration
ADMINISTRATOR
Principal Deputy Administrator
Chief of Staff
Administrator's Staff
Defense Nuclear Counterintelligence
Defense Nuclear Security
General Counsel
Policy Planning, Assessment and Analyses
Congressional, Intergovernmental and Public Affairs
Environmental, Safety and Health Advisor
Program Organizations
Support Organizations
Office of Emergency Operations
Office of Emergency Management
Office of Emergency Response
Deputy Administrator for Defense Programs
Deputy Administrator for Defense Nuclear Nonproliferation
Deputy Administrator for Naval Reactors
Associate Administrator for Facilities and Operations
Office of Field Operations Support
Office of Infrastructure & Facilities Management
Office of ES&H Operations Support
Office of Project Management & Engineering Support
Office of Nuclear Safeguards & Security Programs
Associate Administrator for Management and Administration
Office of Diversity Programs
Office of Planning, Programming, Budgeting & Evaluation
Office of Procurement & Assistance Management
Office of Human Resources
Office of Chief Information Officer
Office of Administrative Services

Appendix HH:

Energy Appropriations FY2002 House of Representatives Report

THIS SEARCH	*THIS DOCUMENT*	*GOTO*
Next Doc	Forward	New Search
Prev Doc	Back	Home Page
Doc List	Highlight Search Words	Help
	Doc Contents	

ENERGY AND WATER DEVELOPMENT APPROPRIATIONS BILL, 2002

SAFEGUARDS AND SECURITY

This program provides for all safeguards and security requirements at NNSA landlord sites. The Committee recommendation is $448,881,000, the same as the budget request, but an increase of nearly 14 percent over fiscal year 2001. Physical safeguards and security measures are only part of the solution to address security concerns throughout the weapons complex. With program needs going unmet and infrastructure deteriorating, the Committee strongly encourages the NNSA to review these growing costs and seek smarter and more efficient ways to meet security needs.

PROGRAM DIRECTION

The Committee recommendation of $250,000,000 for program direction is a reduction of $21,137,000 from the budget request of $271,137,000, and $566,000 below fiscal year 2001. Congress assumed that creation of the NNSA would lead to efficiencies and streamlined management. However, the result has been an increase in staff at Headquarters and in the field. The conference report to accompany the Fiscal Year 2001 National Defense Authorization Act (P.L. 106-398) decreased program direction funding for fiscal year 2001 because the conferees believed the Office of Defense Programs to be overstaffed. The conferees urged the Department to eliminate duplicative efforts and streamline management control and directed the Department to reorganize and realign headquarters and field offices roles and responsibilities. The Committee expects the NNSA to address this issue during fiscal year 2002 and seek additional efficiencies throughout the Headquarters and field organizations during fiscal year 2003.

FUNDING ADJUSTMENTS

The recommendation includes an adjustment of $184,985,000. This consists of a $28,985,000 security charge for reimbursable work as included in the budget request and a general reduction of $156,000,000.

DEFENSE NUCLEAR NONPROLIFERATION

Appropriation, 2001	$872,273,000
Budget Estimate, 2002	773,700,000
Recommended, 2002	845,341,000
Comparison:	
Appropriation, 2001	-26,932,000
Budget Estimate, 2002	+71,641,000

The Defense Nuclear Nonproliferation account includes funding for Nonproliferation and Verification Research and Development, Arms Control, International Materials Protection, Control, and Accounting, Russian Transition Assistance, HEU Transparency Implementation, International Nuclear Safety, Fissile Materials Disposition, and Program Direction. Descriptions of each of these programs are provided below.

The Department requested $7,000 for official reception and representation expenses in this account. The Committee recommendation transfers this funding and combines it with the request of $5,000 for official reception and representation expenses in the Office of the Administrator for a total of $12,000.

NONPROLIFERATION AND VERIFICATION RESEARCH AND DEVELOPMENT

The nonproliferation and verification research and development program conducts applied research, development, testing, and evaluation of science and technology for strengthening the United States response to threats to national security and to world peace posed by the proliferation of nuclear weapons and special nuclear materials. Activities center on the design and production of operational sensor systems needed for proliferation detection, treaty verification, nuclear warhead dismantlement initiatives, and intelligence activities.

The Committee recommendation is $216,102,000, an increase of $10,000,000 over the budget request of $206,102,000. The recommendation provides an additional $10,000,000 for ground-based systems for treaty monitoring which was reduced from $22,510,000 in fiscal year 2001 to $12,510,900 in the budget request.

Competitive Research.--Concerns have been raised repeatedly that there should be more opportunity for open competition in certain areas of the nonproliferation and verification research and development program. A report by an outside group established by the Department to review the Office of Nonproliferation Research and Engineering included a similar recommendation. The Committee expects the Department to act in good faith on the recommendations provided by the external review group and directs the Department to continue a free and open competitive process for 25 percent of its research and development activities during fiscal year 2002 for ground-based systems treaty monitoring. The competitive process should be open to all Federal and non-Federal entities.

Appendix II:

"Department of Energy: Key Factors Underlying Security Problems at DOE Facilities,"
General Accounting Office Testimony #T-RCED-99-159

April 20, 1999

United States General Accounting Office

GAO

Testimony

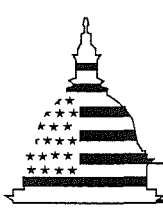
Before the Subcommittee on Oversight and Investigations, Committee on Commerce, House of Representatives

For Release
on Delivery
Expected at
2:00 p.m. EDT
Tuesday
April 20, 1999

DEPARTMENT OF ENERGY

Key Factors Underlying Security Problems at DOE Facilities

Statement of Victor S. Rezendes,
Director, Energy, Resources, and Science Issues,
Resources, Community, and Economic
Development Division



G A O

Accountability * Integrity * Reliability

GAO/T-RCED-99-159

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss our past work involving security at the Department of Energy's (DOE) facilities. These facilities, particularly its nuclear weapons design laboratories and its nuclear material and weapons production facilities, have long been viewed by DOE and the FBI as targets of espionage and other threats. Recent revelations of the possible loss of nuclear weapons design and other classified information to foreign countries have focused renewed attention on the effectiveness of security at DOE's facilities and have prompted concerns at high levels in the government, including the Administration and the Congress.

To protect its facilities from security threats, DOE created a multifaceted, defense-in-depth security strategy. Under such a strategy, various lines of defense are used to protect classified and sensitive information, nuclear materials, and equipment. Over the last 20 years, we have performed numerous reviews of security that, unfortunately, Mr. Chairman, show serious weaknesses in many of these lines of defense that have lead to losses of classified or sensitive information and technology.

In summary, Mr. Chairman, our work has identified security-related problems with controlling foreign visitors, protecting classified and sensitive information, maintaining physical security over facilities and property, ensuring the trustworthiness of employees, and accounting for nuclear materials. These problems include:

- Ineffective controls over foreign visitors to DOE's most sensitive facilities. We found in 1988, and again in 1997, that foreign visitors are allowed into DOE's nuclear weapons design laboratories with few background checks and inadequate controls over the topics discussed, and that other security procedures, such as access controls, to mitigate the risks from these visits may not be fully effective. In addition, counterintelligence programs to guard against foreign and industrial espionage activities received little priority and attention.
- Weaknesses in efforts to control and protect classified and sensitive information. We found one instance where a facility could not account for 10,000 classified documents. In 1987, 1989, and 1991, we reported that foreign countries routinely obtained unclassified but sensitive information that could assist their nuclear weapons capability. Earlier this year, we reported that under its program with Russia to prevent proliferation, DOE

may have provided Russian scientists with dual-use defense-related information that could negatively affect national security.

- Lax physical security controls, such as security personnel and fences, to protect facilities and property. Our reviews of security personnel have shown that these personnel have been unable to demonstrate basic skills such as arresting intruders or shooting accurately; at one facility, 78 percent of the security personnel failed a test of required skills. Furthermore, we found that equipment and property worth millions of dollars was missing at some facilities.
- Ineffective management of personnel security clearance programs has been a problem since the early 1980s. Backlogs were occurring in conducting security investigations, and later when the backlogs were reduced, we found some contractors were not verifying information on prospective employees.
- Weaknesses in DOE's ability to track and control nuclear materials. We reported in 1980 and again in 1991 that, at some facilities, DOE was not properly measuring, storing, and verifying quantities of nuclear materials. Also, DOE was not able to track all nuclear material sent overseas for research and other purposes.

The recent revelations about espionage bring to light how ingrained security problems are at DOE. Although each individual security problem is a concern, when these problems are looked at collectively over time, a more serious situation becomes apparent. While a number of investigations are currently underway to determine the status of these security problems, we have found that DOE has often agreed to take corrective action but the implementation has not been successful and the problems reoccur. In our view, there are two overall systemic causes for this situation. First, DOE managers and contractors have shown a lack of attention and/or priority to security matters. Second, and probably most importantly, there is a serious lack of accountability at DOE. Efforts to address security problems have languished for years without resolution or repercussions to those organizations responsible.

Security in today's environment is even more challenging, given the greater openness that now exists at DOE's facilities and the international cooperation associated with some of DOE's research. Even when more stringent security measures were in place than there are today, such as those in effect during the development of the first atomic bombs, problems have arisen and secrets can be, and were, lost. Consequently, continual vigilance, as well as more sophisticated security strategies, will be needed to meet the threats that exist today. Mr. Chairman, we are concerned that,

given DOE's past record, it may not be up to the challenge without congressional oversight to hold it accountable for achieving specific goals and objectives for security reform. Therefore, we are pleased that the Committee has taken a special interest in DOE's security problems and we have already begun to work on the Committee's request to have us assess the current status of these security problems.

Background

DOE has numerous contractor-operated facilities that carry out the programs and missions of the Department. Much of the work conducted at these facilities is unclassified and nonsensitive and can be, and is, openly discussed and shared with researchers and others throughout the world. However, DOE's facilities also conduct some of the nation's most sensitive activities, including designing, producing, and maintaining the nation's nuclear weapons; conducting efforts for other military or national security applications; and performing research and development in advanced technologies for potential defense and commercial applications.

Security concerns and problems have existed since these facilities were created. The Los Alamos National Laboratory in New Mexico developed the first nuclear weapons during the Manhattan Project in the 1940s; however, it was also the target of espionage during that decade as the then Soviet Union obtained key nuclear weapons information from the laboratory. In the 1960s, significant amounts of highly enriched uranium—a key nuclear weapons material —was discovered to be missing from a private facility under the jurisdiction of the Atomic Energy Commission, a predecessor to DOE. It is widely believed that in the early 1980s, China obtained information on neutron bomb design from the Lawrence Livermore National Laboratory in California.

Most recently, two incidents have occurred at Los Alamos in which laboratory employees are believed to have provided classified information to China. In one situation, a laboratory employee admitted to providing China classified information on a technology used to conduct nuclear weapons development and testing. In the other situation, which occurred earlier this year, DOE disclosed that it had evidence that indicated China obtained information on this nation's most advanced nuclear warhead and had used that information to develop its own smaller, more deliverable nuclear weapons. A laboratory employee has been fired as a result of recent investigations into how this information was obtained by China; however, no charges have yet been filed.

Problems Noted in Critical Security Areas

While the recent incidents at Los Alamos have been receiving national attention, these are only the most recent examples of problems with DOE's security systems. For nearly 20 years, we have issued numerous reports on a wide range of DOE security programs designed to protect nuclear weapons-related and other sensitive information and material. These reports have included nearly 50 recommendations for improving programs for controlling foreign visitor access, protecting classified and sensitive information, maintaining physical security over facilities and property, ensuring the trustworthiness of employees, and accounting for nuclear materials. While DOE has often agreed to take corrective actions, we have found that the implementation has often not been successful and that problems recur over the years. I would like to highlight some of the security problems identified in these reports.

Inadequate Controls Over Foreign Visitors

Thousands of foreign nationals visit DOE facilities each year, including the three laboratories—Lawrence Livermore National Laboratory in California and the Los Alamos National Laboratory and the Sandia National Laboratories in New Mexico[1]—that are responsible for designing and maintaining the nation's nuclear weapons. These visits occur to stimulate the exchange of ideas, promote cooperation, and enhance research efforts in unclassified areas and subjects. However, allowing foreign nationals into the weapons laboratories is not without risk, as this allows foreign nationals direct and possibly long-term access to employees with knowledge of nuclear weapons and other sensitive information. Consequently, DOE has had procedures to control these visits as well as other lines of defense—such as access controls and counterintelligence programs—to protect its information and technology from loss to foreign visitors.

In 1988, we reported that significant weaknesses exist in DOE's controls over foreign visitors to these laboratories.[2] First, required background checks were performed for fewer than 10 percent of the visitors from sensitive countries prior to their visit.[3] As a result, visitors with questionable backgrounds—including connections with foreign intelligence services—obtained access to the laboratories without DOE's

[1]Sandia also has a facility adjacent to the Lawrence Livermore facility in California.

[2]Nuclear Nonproliferation: Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories (GAO/RCED-89-31, Oct. 11, 1988).

[3]DOE's definition of sensitive countries has changed over time. Currently, DOE views certain countries as sensitive because of concerns about national security, nuclear nonproliferation, regional instability, or support of terrorism.

knowledge. Second, DOE and the laboratories were not always aware of visits that involved topics, such as isotope separation and inertial confinement fusion, that DOE considers sensitive because they have the potential to enhance nuclear weapons capability, lead to proliferation, or reveal other advanced technologies. Third, internal controls over the foreign visitor program were ineffective. Visits were occurring without authorized approvals, security plans detailing how the visits would be controlled were not prepared, and DOE was not notified of visits. Because DOE was not notified of the visits, it was unaware of the extent of foreign visitors to the laboratories.

At that time, DOE acknowledged problems with its controls over foreign visitors and subsequently set out to resolve these problems. Among other things, DOE revised its foreign visitor controls, expanded background check requirements, established an Office of Counterintelligence at DOE headquarters, and created an integrated computer network for obtaining and disseminating data on foreign visitors. However, at the same time the number of foreign visitors continued to grow. Between the period of the late-1980s to the mid-1990s, the annual number of foreign visitors increased from about 3,800 to 6,400 per year—nearly 70 percent —and those from sensitive countries increased from about 500 to over 1,800 per year—more than 250 percent.

We again examined the controls over foreign visitors and reported in 1997 that most of the problems with these controls persist.[4] We found that revised procedures for obtaining background checks had not been effectively implemented and that at two facilities, background checks were being conducted on only 5 percent of visitors from all sensitive countries and on less than 2 percent of the visitors from China. We also found that visits were still occurring that may involve sensitive topics without DOE's knowledge. Moreover, other lines of defense were not working effectively. Security controls over foreign visitors did not preclude them from obtaining access to sensitive information. For example, Los Alamos allowed unescorted after-hours access to controlled areas to preserve what one official described as an open "campus atmosphere." Evaluations of the controls in areas most frequented by foreign visitors had not been conducted.

Additionally, we found that the counterintelligence programs for mitigating the threat posed by foreign visitors needed improvements.

[4]Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories (GAO/RCED-97-229, Sept. 25, 1997).

These programs lacked comprehensive threat assessments, which are needed to identify the threats against DOE and the facilities most at risk, and lacked performance measures to gauge the effectiveness of these programs in neutralizing or deterring foreign espionage efforts. Without these tools, the counterintelligence programs lacked key data on threats to the facilities and on how well the facilities were protected against these threats.

Information Security

Information security involves protecting classified and/or sensitive information from inappropriate disclosure. We have found problems with information security at the nuclear weapons laboratories that could involve the loss of classified information and/or assist foreign nuclear weapons capability. For example, in February 1991, we reported that the Lawrence Livermore National Laboratory was unable to locate or determine the disposition of over 12,000 secret documents.[5] These documents covered a wide range of topics, including nuclear weapons design. The laboratory conducted a search and located about 2,000 of these documents but did not conduct an assessment of the potential that the documents still missing compromised national security. We also found that DOE had not provided adequate oversight of the laboratory's classified document control program. Although the laboratory's classified document controls were evaluated annually, the evaluations were limited in scope and failed to identify that documents were missing.

In 1987 and 1989, we reported that DOE had inadequate controls over unclassified but sensitive information that could assist foreign nuclear weapons programs.[6] Specifically, we found that countries—such as China, India, Iraq, and Pakistan—that pose a proliferation or security risk routinely obtain reprocessing and nuclear weapon-related information from DOE. We also found that DOE had transferred to other countries information appearing to meet the definition of sensitive nuclear technology, which requires export controls. Further, we found that DOE placed no restrictions on foreign nationals' involvement in reprocessing research at colleges and universities.

[5]Nuclear Security: Accountability for Livermore's Secret Classified Documents Is Inadequate (GAO/RCED-91-65, Feb. 8, 1991).

[6]Nuclear Nonproliferation: Department of Energy Needs Tighter Controls Over Reprocessing Information (GAO/RCED-87-150, Aug. 17, 1987) and Nuclear Nonproliferation: Better Controls Needed Over Weapons-Related Information and Technology (GAO/RCED-89-116, June 19, 1989).

In the 1990s, we continued to raise concerns. In 1991, we reported that DOE and its weapons laboratories were not complying with regulations designed to control the risk of weapons technology or material being transferred to foreign countries having ownership, control, or influence over U.S. companies performing classified work for DOE.[7] We estimated that about 98 percent of the classified contracts awarded at the weapons laboratories during a 30-month period that were subject to such regulations did not fully comply with those regulations.

As recently as February of this year, we reported on information security problems in DOE's Initiatives for Proliferation Prevention with Russia.[8] Under these initiatives, DOE may have provided defense-related information to Russian weapons scientists—an activity that could negatively affect U.S. national security. We reviewed 79 projects funded by DOE under this program and found nine to have dual-use implications—that is, both military and civilian applications—such as improving aircraft protective coating materials, enhancing communication capabilities among Russia's closed nuclear cities, and improving metals that could be used in military aircraft engines.

We note that the Department of Commerce has also recently raised concerns about nuclear-related exports to Russia from at least one DOE facility. Commerce notified Los Alamos in January 1999 that equipment the laboratory sent to nuclear facilities in Russia required export licenses and that the laboratory may be facing civil charges for not obtaining the required licenses.

Physical Security

Physical security controls involve the protection, primarily through security personnel and fences, of facilities and property. In 1991, we reported that security personnel were unable to demonstrate basic skills such as the apprehension and arrest of individuals who could represent a security threat.[9] Prior to that report, in 1990, we reported that weaknesses were occurring with security personnel, as some security personnel could not appropriately handcuff, search, or arrest intruders or shoot

[7]Nuclear Nonproliferation: DOE Needs Better Controls to Identify Contractors Having Foreign Interests (GAO/RCED-91-83, Mar. 25, 1991).

[8]Nuclear Nonproliferation: Concerns With DOE's Efforts to Reduce the Risks Posed by Russia's Unemployed Weapons Scientists (GAO/RCED-99-54, Feb. 19, 1999).

[9]Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons Facilities (GAO/RCED-92-39, Dec. 13, 1991).

accurately.[10] For example, we found that at the Los Alamos National Laboratory, 78 percent of the security personnel failed a test of required skills. Of the 54-member guard force, 42 failed to demonstrate adequate skill in using weapons, using a baton, or apprehending a person threatening the facility's security. Some failed more than one skill test. We also found that many Los Alamos' training records for security personnel were missing, incomplete, undated, changed, or unsigned. Without accurate and complete training records, DOE could not demonstrate that security personnel are properly trained to protect the facility.

Problems we have identified were not only with keeping threats out of the facilities, but also with keeping property in. For example, we reported in 1990 that the Lawrence Livermore National Laboratory could not locate about 16 percent of its inventory of government equipment, including video and photographic equipment as well as computers and computer-related equipment.[11] When we returned in 1991 to revisit this problem, we found that only about 3 percent of the missing equipment had been found; moreover, the laboratory's accountability controls over the equipment were weaker than in the prior year.[12] We also found that DOE's oversight of the situation was inadequate and that its property control policies were incomplete. We found similar problems at DOE's Rocky Flats Plant in 1994 where property worth millions of dollars was missing, such as forklifts and a semi-trailer. Eventually, property worth almost $21 million was written off.[13]

Other problems in controlling sensitive equipment have been identified, such as disposing of usable nuclear-related equipment, that could pose a proliferation risk. For example, in 1993, DOE sold 57 different components of nuclear fuel reprocessing equipment and associated design documents, including blueprints, to an Idaho salvage dealer. DOE subsequently determined that the equipment and documents could be useful to a group or country with nuclear material to process, and that the equipment could significantly shorten the time necessary to develop and implement a nuclear materials reprocessing operation. This incident resulted from a

[10]Nuclear Safety: Potential Security Weaknesses at Los Alamos and Other DOE Facilities (GAO/RCED-91-12, Oct. 11, 1990).

[11]Nuclear Security: DOE Oversight of Livermore's Property Management System Is Inadequate (GAO/RCED-90-122, Apr. 18, 1990).

[12]Nuclear Security: Property Control Problems at DOE's Livermore Laboratory Continue (GAO/RCED-91-141, May 16, 1991).

[13]Department of Energy: The Property Management System at the Rocky Flats Plant Is Inadequate (GAO/RCED-94-77, Mar. 1, 1994).

lack of vigilance at all levels for the potential impacts of releasing sensitive equipment and information to the public, and DOE conceded that system breakdowns of this type could have severe consequences in other similar situations where the equipment and documents may be extremely sensitive.

Personnel Security

DOE's personnel security clearance program is intended to provide assurance that personnel with access to classified material and information are trustworthy. We have found numerous problems in this area, dating back to the early 1980s. In 1987, and again in 1988, we found that DOE headquarters and some field offices were taking too long to conduct security investigations.[14] We found that the delays in investigations lowered productivity, increased costs, and were a security concern. We also found that DOE's security clearance database was inaccurate. Clearance files at two field offices contained about 4,600 clearances that should have been terminated and over 600 employees at the Los Alamos laboratory had clearance badges, but did not have active clearances listed in the files. In other cases, the files contained inaccurate data, such as incorrect clearance levels and names. We followed DOE's efforts to remedy these problems, and by 1993, DOE had greatly reduced its backlog of investigations.[15] However, some DOE contractors were not verifying information on prospective employees such as education, personal references, previous employment, and credit and law enforcement records.

Accounting for Nuclear Material

Material accountability relates to the protection of special nuclear material such as enriched uranium and plutonium. In 1991, we found that DOE facilities were not properly measuring, storing, and verifying quantities of nuclear materials.[16] Without proper accounting for nuclear materials, missing quantities are more difficult to detect. We also found that DOE facilities were not complying with a rule requiring that two people always be present when nuclear material is being accessed or used. This rule is

[14]Nuclear Security: DOE's Reinvestigation of Employees Has Not Been Timely (GAO/RCED-87-72, Mar. 10, 1987) and Nuclear Security: DOE Needs a More Accurate and Efficient Security Clearance Program (GAO/RCED-88-28, Dec. 29, 1987).

[15]Nuclear Security: DOE's Progress on Reducing Its Security Clearance Work Load (GAO/RCED-93-183, Aug. 12, 1993).

[16]Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons Facilities (GAO/RCED-92-39, Dec. 13, 1991).

designed to preclude a single individual from having access to and diverting nuclear material without detection.

In 1994 and 1995, we reported on DOE's efforts to develop a nuclear material tracking system for monitoring nuclear materials exported to foreign countries.[17] A nuclear tracking system is important to protect nuclear materials from loss, theft, or diversion. In 1994, we reported that the existing system was not able to track all exported nuclear materials and equipment; moreover, DOE had not adequately planned the replacement system. We recommended activities that we believed were necessary to ensure that the new system would be successful. In 1995, we found that DOE had not implemented our recommendations and had no plans to do so. We also found that the system still had development risks. DOE was not adequately addressing these risks and had no plans to conduct acceptance testing, and as a result of these problems, it had no assurance that the system would ever perform as intended. Our concerns were justified, as 3 months after the new tracking system began operating, the technical committee overseeing this system concluded that it faced a high probability of failure and that the system should not be used.

Key Factors Contributing to Security Problems

As you can see, Mr. Chairman, our work over the years has identified a wide variety of specific security problems at DOE facilities. While each individual security problem is a concern, when looked at collectively over an extended period of time, a more serious situation becomes apparent that stems from systemic causes. In our view, there are two overall systemic causes of the security problems. First, there has been a longstanding lack of attention and/or priority given to security matters by DOE managers and its contractors. Second, and probably most importantly, there is a serious lack of accountability among DOE and its contractors for their actions. These two causes are interrelated and not easily corrected.

Lack of Attention and Priority to Security

The lack of attention and priority given by DOE management and its contractors to security matters can be seen in many areas. One area is its long-term commitment to improving security. For example, in response to our 1988 report on foreign visitors, DOE required more background checks be obtained. However, 6 years later, it granted Los Alamos and Sandia exemptions to this requirement, and as a result, few background checks were conducted at those facilities. Also in response to our 1988 report, DOE

[17]Nuclear Nonproliferation: U.S. International Nuclear Materials Tracking Capabilities Are Limited (GAO/RCED/AIMD-95-5, Dec. 27, 1994) and Department of Energy: Poor Management of Nuclear Materials Tracking System Makes Success Unlikely (GAO/AIMD-95-165, Aug. 3, 1995).

brought in FBI personnel to assist its counterintelligence programs. However, the FBI eventually withdrew its personnel in the early 1990s because of resistance within DOE to implementing the measures the FBI staff believed necessary to improve security. We note with interest that in response to the current concerns with foreign visitors and other espionage threats against DOE facilities, the FBI is again being brought in to direct DOE's counterintelligence program.

The lack of attention to security matters can be seen in other ways as well. In 1996, when foreign visitors were coming in increasing numbers to the laboratory, Los Alamos funded only 1.1 staff years for its counterintelligence program. Essentially, one person had to monitor not only thousands of visitors to the laboratory but also monitor over 1,000 visits made by laboratory scientists overseas. This problem was not isolated to Los Alamos; funding for counterintelligence activities at DOE facilities during the mid-1990s could only be considered minimal. Prior to fiscal year 1997, DOE provided no direct funding for counterintelligence programs at its facilities. Consequently, at eight high-risk facilities, counterintelligence program funding was obtained from overhead accounts and totaled only $1.4 million and 15 staff. Resources were inadequate in other areas. In 1992, we reported that safeguard and security plans and vulnerability assessments for many of DOE's sensitive facilities were almost 2 years overdue because, among other reasons, DOE had not provided sufficient staff to get the job done. These plans and assessments are important in identifying threats to the facilities as well as devising countermeasures to the threats. In our view, not providing sufficient resources to these important activities indicates that security is not a top priority. This problem is not new. We reported in 1980 and again in 1982 that funding for security has low priority and little visibility.[18]

Earlier I mentioned missing classified documents at Lawrence Livermore Laboratory. In response to that report, both DOE and laboratory officials showed little concern for the seriousness of the situation and told us that they believed the missing documents were the result of administrative error, such as inaccurate record keeping and not theft. Although DOE is required to conduct an assessment of the missing documents' potential for compromising national security, at the time of our report DOE did not plan to do this for over 1 year after we reported the documents missing.

[18]Nuclear Fuel Reprocessing and the Problems of Safeguarding Against the Spread of Nuclear Weapons, (EMD-80-38, Mar. 18, 1980) and Safeguards and Security At DOE's Weapons Facilities Are Still Not Adequate, (C-GAO/EMD-82-1, Aug. 20, 1982).

Similarly, security problems identified by DOE's own internal security oversight staff often go unresolved, even today. For example, issues related to the inadequate separation of classified and unclassified computer networks were identified at Los Alamos in 1988, 1992, and 1994. This problem was only partially corrected in 1997, as classified information was discovered on Los Alamos' unclassified computer network in 1998. We found in 1991 that deficiencies DOE identified as early as 1985 at six facilities had not been corrected by 1990 because DOE did not have a systematic method to track corrective actions taken on its own security inspections.

The low priority given security matters is underscored by how DOE manages its contractors. DOE's contract with the University of California for managing its Los Alamos and Lawrence Livermore national laboratories contain specific measures for evaluating the university's performance. These measures are reviewed annually by DOE and should reflect the most important activities of the contractor. However, none of the 102 measures in the Los Alamos contract or the 86 measures in the Lawrence Livermore contract relate to counterintelligence. We reported in 1997 that DOE had not developed measures for evaluating the laboratories' counterintelligence activities, and DOE told us it was considering amending its contracts to address this problem. Performance measures for counterintelligence activities are still not in its contracts for these two laboratories. The contracts do contain a related measure, for safeguarding classified documents and materials from unauthorized persons, but this measure represents less than 1 percent of the contractor's total score. Safeguards and security performance measures in general account for only about 5 percent of the university's performance evaluations for the two laboratories.

The low priority afforded security matters may account for the low rating DOE has just given nuclear weapons facilities in its latest Annual Report on Safeguards and Security. Two weapons laboratories—Los Alamos and Lawrence Livermore—received a rating of "marginal" for 1997 and 1998. In its annual evaluation of Los Alamos' overall performance, however, DOE rated the laboratory as "excellent" in safeguards and security, even though the laboratory reported 45 classified matter compromises and infractions for the year. The previous 3-year rolling average was 20. DOE explained that the overall excellent score was justified based on Los Alamos' performance in many different aspects of safeguards and security. For future contracts, a new DOE policy will enable the Department to withhold a laboratory's full fee for catastrophic events, such as a loss of

control over classified material. We recommended as far back as 1990 that DOE should withhold a contractor's fee for failing to fix security problems on a timely basis. Both laboratories have been managed by the University of California since their inception without recompeting these contracts, making them among the longest-running contracts in the DOE complex.

Lack of Accountability

In the final analysis, security problems reflect a lack of accountability. The well-documented history of security lapses in the nuclear weapons complex show that DOE is not holding its contractors accountable for meeting all of its important responsibilities. Furthermore, DOE leadership is not holding its program managers accountable for making sure contractors do their jobs.

Achieving accountability in DOE is made more difficult by its complex organizational structure. Past advisory groups and internal DOE studies have often reported on DOE's complex organizational structure and the problems in accountability that result from unclear chains of command among headquarters, field offices, and contractors. For example

- The FBI, which examined DOE's counterintelligence activities in 1997, noted that there is a gap between authority and responsibility, particularly when national interests compete with specialized interests of the academic or corporate management that operate the laboratories. Citing the laboratories' autonomy granted by DOE, the FBI found that this autonomy has made national guidance, oversight, and accountability of the laboratories' counterintelligence programs arduous and inefficient.
- A 1997 report by the Institute for Defense Analyses cited serious flaws in DOE's organizational structure. Noting long-standing concerns in DOE about how best to define the relationships between field offices and the headquarters program offices that sponsor work, the Institute concluded that "the overall picture that emerges is one of considerable confusion over vertical relationships and the roles of line and staff officials." As a consequence of DOE's complex structure, the Institute reported that unclear chains of command led to the weak integration of programs and functions across the Department, and confusion over the difference between line and staff roles.[19]
- A 1997 DOE internal report stated that "lack of clarity, inconsistency, and variability in the relationship between headquarters management and field organizations has been a longstanding criticism of DOE operations . . . . This

[19]The Organization and Management of the Nuclear Weapons Program, Institute for Defense Analyses (March 1997).

is particularly true in situations when several headquarters programs fund activities at laboratories. . . ."[20] DOE's Laboratory Operations Board also reported in 1997 on DOE's organizational problems, noting that there were inefficiencies due to DOE's complicated management structure. The Board recommended that DOE undertake a major effort to rationalize and simplify its headquarters and field management structure to clarify roles and responsibilities.[21]

DOE's complex organization stems from the multiple levels of reporting that exist between contractors, field offices, and headquarters program offices. Further complicating reporting, DOE assigns each laboratory to a field operations office, whose director serves as the contract manager and also prepares the contractor's annual appraisal. The operations office, however, reports to a separate headquarters office under the Deputy Secretary, not to the program office that supplies the funding. Thus, while the Los Alamos National Laboratory is primarily funded by Defense Programs, it reports to a field manager who reports to another part of the agency.

We believe these organizational weaknesses are a major reason why DOE has been unable to develop long-term solutions to the recurring problems reported by advisory groups. Recent events at the Brookhaven National Laboratory in New York, for example, illustrate the consequences of organizational confusion. Former Secretary Pena fired the contractor operating the laboratory when he learned that the contractor breached the community's trust by failing to ensure it could operate safely. DOE did not have a clear chain of command over environment, safety, and health matters and, as a result, laboratory performance suffered in the absence of DOE accountability. To address problems in DOE's oversight, the Secretary removed the Chicago Operations Office from the chain of command over Brookhaven, by having the on-site DOE staff report directly to the Secretary's office. We found, however, that even though the on-site staff was technically reporting directly to the Secretary's office, the Chicago Operations Office was still managing the contractor on a day-to-day basis, including retaining the responsibility for preparing the laboratory's annual appraisal. Chicago officials told us that there was considerable confusion regarding the roles of Chicago and on-site DOE staff. As a result, DOE did not fundamentally change how it manages the contractor through its field offices.

[20]DOE Action Plan for Improved Management of Brookhaven National Laboratory, DOE (July 1997).

[21]Department of Energy: Uncertain Progress in Implementing National Laboratory Reforms, (GAO/RCED-98-197, Sept. 10, 1998).

This concludes my testimony, and I will be happy to answer any questions you may have.

Appendix JJ:

"Memorandum for All Department and Contract Employees,"
Secretary of Energy Bill Richardson

June 17, 1999

The Secretary of Energy
Washington, DC 20585

June 17, 1999

MEMORANDUM FOR ALL DEPARTMENT AND CONTRACT EMPLOYEES

FROM: BILL RICHARDSON

SUBJECT: Secretarial Policy Statement: Security Incidents and Violations

Protecting the national security of the United States is an integral requirement of our work. Since the Manhattan Project, the Department of Energy (DOE) and its predecessor agencies have been the custodian of the United States' most critical defense materials and information – nuclear weapons technology. In light of this profound responsibility, it is incumbent upon us to serve as the benchmark for a strong agency security policy.

Overall Security Policy

The protection of classified and sensitive information and nuclear weapons and materials is a critical mission of DOE, inherently linked to our strategic goals. We expect appropriate protective measures as a matter of course in the Department of Energy. Both Federal and contractor employees must practice sound security practices each and every day, in everything we do. Management must also create and foster a work environment that allows free and open expression of security concerns, where workers fear no reprisals or retaliation. It is our firm belief that these security objectives will be achieved only through a renewed and deepened commitment to compliance with all established security requirements.

The security regulations, directives, and policies already in place are designed to ensure the protection of classified and sensitive information and nuclear weapons and materials. All personnel are responsible for implementing these requirements. Over many years, incidents that resulted in classified or sensitive information being placed at risk suggest that we need to renew our commitment to sustained vigilance and strict compliance with all applicable security requirements.

Apathy and negligence can undermine even the best programs. Thus, we are establishing a policy of "zero tolerance" for violations of security requirements that place nuclear or other sensitive materials at risk, or compromise classified or sensitive information.

Appendix KK:

Letter from Glenn S. Podonsky, Director of Office of Independent Oversight to:
Ronald E. Timm, President RETA Security

March 5, 2001

Department of Energy
Washington, DC 20585

March 5, 2001

Mr. Ronald E. Timm, President
RETA Security, Inc.
Post Office Box 369
Lemont, Illinois 60439

Dear Mr. Timm:

The Secretary has received your letter dated February 9, 2001, and has asked me to reply. We appreciate and take seriously the security concerns expressed by our employees, our contractors, and other interested parties. Consequently, we assure you that the issues raised in your letter, as well as the similar issues raised in your January 2000 letter to General Eugene Habiger, have been thoroughly reviewed.

The Department concurs that one of our most important missions is to protect the national security assets entrusted to our care, including our inventories of special nuclear material. The main thrust of our safeguards and security program is to protect this material; and yes, we do spend a lot of money and considerable effort to ensure that we provide adequate protection to those assets. Your letter asserts that special nuclear material in DOE's custody may be in imminent danger of "detonation" or "abrupt theft" – particularly at three specified locations – with all the undesirable consequences of such an occurrence. You further assert that other departmental actions, or inactions, serve to allow these alleged dangerous conditions to continue. We do not concur with your conclusion that special nuclear material is at undue risk in the Department; our analyses lead us to the opposite conclusion. The bases of our conclusions and the various points you raised in your letter are addressed in the attachment.

The Department is serious about protecting all of our national security assets. Reviews and reports of the Department's independent oversight organization have identified deficiencies in need of correction, but have generally concluded, based on the overall performance of protection systems in place, that special nuclear material is not at immediate risk. Various other reports by DOE and external groups have reached the same conclusion. Further, there are numerous examples of the Department's timely response, immediate compensatory measures, and follow-on corrective actions regarding those deficiencies that have been identified. The Department's protection strategy relies on the identification and analysis of risk and the implementation of programs to eliminate identified risks or to reduce them to acceptable levels. In light of your background and experience, you surely understand that it is impossible to totally eliminate all risk associated with special nuclear material as long as such material exists. That is why the Department expends so much effort and so many resources to characterize and implement reasonable actions to reduce risk. We believe our protection programs are sufficiently robust to ensure that any residual risk is low, posing no significant threat to our assets, employees, facilities, or the public. Although it is troubling that an individual such as yourself should reach conclusions so different from those reached by countless other informed and objective parties,

we must nevertheless conclude that your concerns regarding the vulnerability of special nuclear material and the Department's protection program are overstated. While the Department's protection program may not be perfect, we firmly believe it is effective. Moreover, we constantly strive to improve it and will continue to closely inspect the Department's safeguards and security programs. We have seriously considered your concerns, as the IG has done previously, and we appreciate your interest in this program.

Sincerely,

Glenn S. Podonsky, Director
Office of Independent Oversight
and Performance Assurance

Attachment: Response to Points Made in February 9, 2001,
Letter to Secretary Abraham

cc:
K. McSlarrow, S
G. Friedman, IG-1
T. Gioconda, DP-1
C. Huntoon, EM-1
E. Fygi, GC-1
J. Decker, SC-1
M. Gunn, CH
J. Hamre, CSIS

ATTACHMENT

Response to Points Made In
February 9, 2001, Letter to Secretary Abraham

You indicate that during the Inspector General's investigation that followed your January 2000 letter to General Habiger you provided numerous documents "exposing" presumably unacceptable risks at the Rocky Flats Environmental Technology Site, the Office of Transportation Safeguards (formerly Transportation Safeguards Division) and Los Alamos National Laboratory. You also indicate that the Inspector General did not seriously consider your allegations of risk.

The Inspector General conducted an extensive review into the concerns you expressed in your January 2000 letter, including allegations of lying in the reporting of the status of safeguards and security programs at Departmental sites, allegations of retaliation against persons trying to correct security problems, and allegations that appropriate actions were not taken to address risks you had identified. After reviewing thousands of pages of classified and unclassified documents, including those provided or identified by you (and including the referenced "point papers"), and interviewing more than thirty senior and knowledgeable security officials, the Inspector General concluded that: there was no evidence that Departmental officials lied in reporting the actual status of security; appropriate Departmental officials were aware of your risk concerns and that there was no evidence that they arbitrarily decided to ignore those concerns; and no Departmental officials interviewed indicated that they had suffered retaliation for their part in reviewing Safeguards and Security Site Plans (SSSPs) or for assisting the mentioned special assistant. The Inspector General also found that several actions had been taken in response to your security concerns. The Inspector General also noted that some of your concerns had not been resolved due to disagreements over the underlying bases of your concerns. While the Inspector General thoroughly addressed the January 2000 allegations indicated, he did not attempt to determine whether Special Nuclear Materials were actually at risk; that determination was beyond the scope of his investigation and within the responsibility of the Department's security offices. Experts in those offices have reviewed your concerns in this area and, again, disagree with your conclusions. Surely you are aware that the quality assurance process of which you were a part suffered from low credibility among many security professionals in the Department and that some of the tools and techniques you employed are considered inappropriate or improperly applied to the SSSP quality assurance process.

Concerning your allegations that Special Nuclear Materials are at risk at the Rocky Flats Environmental Technology Site, while in the custody of the Office of Transportation Safeguards, and at Los Alamos National Laboratory, we are convinced that current conditions lead to a different conclusion. The Department, through various line management and independent oversight activities, has identified some deficiencies at Rocky Flats. A Department-level inspection of safeguards and security at Rocky Flats last occurred in March-April 2000, and did not find special nuclear materials to be at risk. While some deficiencies were identified, Rocky Flats developed and implemented plans to address those deficiencies. A subsequent review found that Rocky Flats is successfully working towards its improvement goals. There is

significant decontamination and decommissioning work ongoing at Rocky Flats. Much of the special nuclear material has been removed from the site, and the remaining material has been consolidated into fewer locations, which aids physical protection efforts. Rocky Flats deploys a large protective force contingent in the immediate vicinity of the remaining potential targets. The most recent review of protection at Rocky Flats concluded that the Special Nuclear Material remaining is not at risk.

The Department has similarly inspected the Office of Transportation Safeguards (OTS) on a regular basis. Those inspections have sometimes included major performance tests. The last full Department-level inspection occurred in November 1999, with follow-up activities in early 2000. Those inspection activities sometimes identified protection concerns regarding OTS operations. OTS has usually responded quickly to such concerns and in the recent past has made significant upgrades or changes to weapons, equipment, and tactics. The Department's last independent oversight evaluation of OTS found that they had met the Phase 1 "goalpost" improvements set for them by the Department and that they maintained adequate capabilities to protect their cargos. The Office of Independent Oversight and Performance Assurance is currently in the process of conducting a comprehensive inspection of OTS, that will, in part, assess the progress being made toward completion of the mandated Phase 2 "goalpost" improvements.

Over the past two years in particular, Los Alamos has received considerable oversight by line management and independent oversight organizations. As mentioned in your letter, an October 2000 inspection identified deficiencies in the Los Alamos vulnerability analysis process and also identified protection deficiencies at specific locations. You may not be aware that Los Alamos and the Office of Defense Programs (DP) instituted compensatory measures and developed corrective action plans to address those deficiencies. A Department-level follow-up visit to Los Alamos in December 2000 verified the implementation of the compensatory measures and progress on corrective actions. The Office of Independent Oversight and Performance Assurance is scheduled to conduct a comprehensive inspection at Los Alamos, including major performance tests, during June 2001.

You indicate your belief that, while the Office of Independent Oversight and Performance Assurance (OA) has identified vulnerabilities during its inspections, the executive summaries of its reports are "politically expedient" and "less than candid,"and that OA does not criticize Defense Programs or Environmental Management sites. OA has a long history of identifying existing deficiencies in protection throughout the Department. In fact, OA's efforts in recent years have been concentrated on the Defense Programs and Environmental Management sites, because those are the sites that contain the greatest amounts of the most sensitive materials and information. You also claim that OA is critical of non-weapons program sites, but does not criticize weapons program sites. A careful review of OA inspection reports clearly demonstrates that your claim is erroneous. OA reports discuss the detailed results of inspections in the report body or in separate appendices that concentrate on a specific security discipline. The details of identified deficiencies and what needs to be fixed are found in those portions of OA reports. The Summary Report, or, in shorter reports the Executive Summary, is intended to provide a concise overview for senior managers and an overall sense of the inspection results and the areas that require additional management attention. While the Summary Report/Executive Summary does not typically discuss deficiencies in great detail, it does identify all significant deficiencies,

explains why they are important, and clearly indicates whether corrective actions are needed. Further, it serves to place inspection results in the appropriate context and perspective based on the total results (favorable and unfavorable) of the inspection activity and provides a conclusion regarding the overall effectiveness of the site's protection program.

You imply that information in point papers provided to former Secretary Richardson by a special assistant, and specifically a December 2000 paper regarding "vulnerabilities" at Los Alamos, have not been properly addressed by the Department. We can assure you that the special assistant's point papers to the former Secretary were referred by Mr. Richardson to the appropriate organizations, were reviewed by those organizations, and that warranted actions were taken. The Inspector General also reviewed the point papers that had been submitted at the time of their (previously described) investigation. It should also be noted that the special assistant accompanied OA on a December 2000 follow-up visit to Los Alamos, the purpose of which was to verify that necessary compensatory measures were in fact in place. The OA team determined that required compensatory measures were in place and Los Alamos was conducting performance testing and vulnerability analyses to complete their implementation of a revised protection strategy. The special assistant's subsequent point paper nevertheless reiterated his previous position that the site in question at Los Alamos should be shut down and the nuclear materials moved elsewhere. Based on the assessment of the other trained security specialists, the Department determined that conditions at Los Alamos did not warrant such immediate and drastic action.

You charge that changes in the Department's analytical process used in the development of security strategies is "dumbed down," and imply that the purpose of the change is to avoid identifying risks that managers don't want to have to address. The Department has recognized the need for improvement in this area, as the historical tools and methods employed have not been optimally effective and efficient. We have experienced considerable difficulties in developing comprehensive and effective security plans, due in no small part to the fact that certain analytical tools have proven to be expensive and not always effective in identifying vulnerabilities. We are still using various tools, but have decided to improve the planning and analysis process through the increased use of expert judgment and less blind reliance on flawed analytical techniques. This does not mean that we intend to discontinue the use of analytical techniques; rather, we will use a more judicious blend of analytical methods, expert judgment and performance testing. We expect the new process to be quicker and more easily applied than the more complicated methods that haven't worked well in the past. The Inspector General review concluded that the new procedures have the potential for significantly enhancing the process, but that strong management involvement will be needed to ensure that the new process achieves its potential. We also believe that the process holds great promise; however since it is new, the Department has not yet had the opportunity to fully evaluate the effectiveness of its implementation across the Department.

Finally, you charge that the Department has taken retaliatory action against a Senior Security Analyst who tried to alert the public to security dangers at Los Alamos. As you yourself hold a DOE security clearance, I'm sure you are aware that individuals entrusted with our nation's most sensitive information are held to a high standard of trustworthiness. The individual you refer to had his security clearance suspended due to his admitted release, without prior authorization, of a

draft DOE Inspector General report on sensitive DOE security matters. His action was in direct contravention of his signed "Security Responsibility Statement" promulgated by the DOE Office of Security Affairs specifically to prevent such releases. His case is currently being processed under the DOE's administrative review procedures (Title 10 Code of Federal Regulations), which afford the Analyst opportunity to explain his actions while he remains employed by the Department in a position that does not require a security clearance.

Appendix LL:

Letter from Ronald E. Timm, President RETA Security to:
Secretary of Energy Spencer Abraham

February 9, 2001

RETA
SECURITY

February 9, 2001

The Honorable Spencer Abraham
Secretary
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, DC 20585

Subject: Risk to Special Nuclear Materials in the Department of Energy's Sites and Transportation.

Dear Mr. Secretary:

RETA Security, Inc has provided security engineering and analysis services to the DOE and its contractors since 1984. Since 1994 we have been designated as "key persons" in the prime support contract to the Headquarters Office of Safeguards and Security. In 1997 we were assigned a Quality Assurance role to review Safeguards and Security Site Plans for the 11 Class A nuclear sites in DOE. We have been the principal analysts for review of all SSSPs for DOE Headquarters since 1997. We have received numerous written commendations from DOE for our security efforts.

The clear possibility of a nuclear detonation or explosion with the spread of radioactive contamination has been documented in numerous studies and from numerous sources. The risk of abrupt theft of Special Nuclear Materials (SNM) has also been demonstrated, particularly during transit. However, time has shown that the existing bureaucracy at DOE have not adequately acted upon the issue of risk to the public other than in ineffective and reactive ways. I am writing this letter to bring this to your immediate attention. When the country's Special Nuclear Materials stockpile is at risk, the health and safety of American citizens is at risk. The primary mission of the DOE is the safeguard and security of the nation's nuclear inventory. This mission was a key point in your testimony in your confirmation hearing which I attended when I was in Washington for the inauguration.

Presidential Decision Directives (PDD) order protection against the terrorist risk to assets of societal importance of which Special Nuclear Materials in DOE is a primary element. Approximately $1.3B of taxpayer dollars are spent annually toward fulfilling this mission. Recent reports and several commissions have highlighted the threat to the US by terrorists using a weapon of mass destruction. Considering the lax security at DOE, and the resultant vulnerability of Special Nuclear Materials,

P. O. Box 369 Lemont, IL 60439 Tel: 630.257.3520 Fax: 630.257.3530 www.retasecurity.com

terrorists have a ready supply of Special Nuclear Materials already existing and available within our borders. The DOE has avoided addressing this serious fact for the past eight years.
In January 2000 we sent a letter to General Habiger, the recently named "Security Czar," entitled "Lying and Retaliation in the SO-20 Department." General Habiger forwarded the letter to the Inspector General (IG) for investigation and a report "Summary Report on Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process" (IG-0482) was published in classified and unclassified versions. During the ensuing Inspector General investigation we provided over 200 classified documents clearly exposing the risk at Rocky Flats, the Transportation System Division (TSD), and Los Alamos National Laboratory (LANL). These documents were prepared by a consortium of senior DOE officials, senior RETA analysts/engineers, senior Sandia National Laboratory analysts, and DOD Special Forces personnel as part of an Office of Security & Safeguards nuclear security quality assurance program. In our letter to General Habiger we referred to "risk" to Special Nuclear Materials nine times, yet the resulting Inspector General report avoided any serious consideration of risk. Unfortunately, in the unclassified version, the Inspector General minimized the severity of the problem. The Inspector General addressed this risk as the last bulleted item in the executive summary! However, the classified version of the Inspector General report, both in the body and appendices, cited clear evidence of actual risk to Special Nuclear Materials at key DOE sites and in transit. Unfortunately, both versions of the report leave the existence of risk to the reader, rather than explicitly stating "Special Nuclear Materials at risk." When we read the Inspector General report we assumed that any uninformed reader could see the persistent issue of vulnerabilities to Special Nuclear Materials across the complex - yet, shockingly, nothing was done.

The Inspector General's solution to the chronic vulnerabilities was to endorse implementation of a nebulous "new" and seriously "dumbed down" analytical process at some time in the future; a process that was proposed by the management that avoided the problem of risk in the first place. Special Nuclear Materials were at risk then, Special Nuclear Materials are at risk today, and, without significant changes, Special Nuclear Materials will be at risk in the future. The issue of risk to Special Nuclear Materials cannot be avoided by a "new" process that does not provide protection (detection, delay, and response) at the affected sites. Insufficient processes failed the USS Cole, Dahran Barracks, and Oklahoma City. Loss prevention processes were available to, but not practiced by, senior personnel who are steeped in national defense or law enforcement backgrounds. Such experience does not prepare them for proactive planning or implementation practices.

Secretary Richardson, in an effort to investigate and understand the security issues, appointed a Special Assistant for Security, Peter D. H. Stockton. From the spring of 1999 to December of 2000, Mr. Stockton prepared a series of point papers for the Secretary identifying these risks to Special Nuclear Materials. The Inspector General never interviewed Mr. Stockton. These point papers covered the period of the investigation and all of CY2000. They consistently pointed out risk to Special Nuclear Materials. The point papers were provided by the Secretary to General Habiger. Mr. Stockton's most recent paper, dated December 20, 2000, specifically referred to the "Phoney SSSP" at Los Alamos. An independent test verified the vulnerabilities there. This was the same issue in our original letter, but one year later. The DOE Orders require immediate compensatory actions when Special Nuclear Materials are vulnerable to sabotage or theft. The Secretary had to become

personally involved to affect any action. Accountability for this issue and other critical deficiencies is not, and has never been, a priority of the DOE bureaucracy.

The risk to Special Nuclear Materials and the public continues despite an Independent Oversight Program (OA). The program has routinely failed to address the existing risk. Both Mr. Stockton and I have briefed the Oversight Program on risk at Los Alamos and the Transportation Division. Detailed findings in the Oversight Program reports bear out the vulnerabilities, but the politicized Executive Summaries of their reports reveal little substance. The Oversight Program management decisions have been less than candid and ignored the critical quality assurance functions they are chartered to identify. A recent exception that proves the rule was at Argonne Laboratory at the Idaho Site. "In your face" problems were documented that required massive improvements in lab physical security and immediate manpower for compensatory actions. However, this site has little bureaucratic clout in the agency making it an easy target for the Oversight Program. This site is not part of the weapons complex. It is much more taboo to criticize Defense Program's (DP) sites, managed by the National Nuclear Security Agency (NNSA), or Energy Management's (EM) sites, and they have not. Los Alamos and the Transportation Division are examples of the Oversight Program seeking politically expedient prose in their executive summaries.

There have been a series of retaliations by DOE management to a variety of persons attempting to address these problems. In the summer of 2000, a Senior Security Analyst, in desperation, sent a copy of the draft Inspector General report that detailed security dangers at Los Alamos to two news organizations. As a result of this action he has been placed on temporary assignment and has had his clearance suspended pending administrative actions. This example, of an a-typical act by the DOE employee, points out the frustration of attempting to address the issues of risk to the public and Special Nuclear Materials within the existing DOE bureaucracy.

The issue of risk to the public and Special Nuclear Materials has continued to fester: the security of the nation's inventory is not only in question, but the security cannot be assured by any objective measurement. Yet the status quo persists! The dysfunction in the DOE was documented by Senator Rudman and the President's Foreign Intelligence Advisory Board last year. More recently the General Accounting Office (GAO) also identified the dysfunction. A dysfunctional organization, by its very definition, is made up of personnel who continue to perpetuate their twisted agenda of least resistance and will not change. If the nation's well being remains secondary to lethargic and incompetent bureaucracy, then the risk to the nuclear inventory and the American public will persist.

I urge you to take this matter seriously and provide the leadership necessary to resolve these dangers to our nation before an accident, or deliberate terrorist action causes the loss of many lives or even the loss of one of our cities.

Sincerely,

Ronald E. Timm,
President
Certified Protection Professional

References:

1. "Summary Report on Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process." IG-0482. Sept. 2000.
2. "Summary Report on Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self-Assessment at Los Alamos National Laboratory. IG-0471. May 2000

cc:
Honorable Daniel Akaka, HI
Honorable Jeff Bingaman, NM
Honorable Richard Durbin, IL
Honorable Carl Levin, MI
Honorable Joseph Lieberman, CT
Honorable Frank Murkowski, AK
Honorable Richard Shelby, AL
Honorable Bob Smith, NH
Honorable Fred Thompson, TN
Honorable John Warner, VA
Honorable Dan Burton, IN
Honorable John Dingell, MI
Honorable Mark Kirk, IL
Honorable Ed Markey, MA
Honorable Ike Skelton, MO
Honorable Bob Stump, AZ
Honorable W.J. "Billy" Tauzin, LA
Honorable C.W. Bill Young, FL
Honorable Donald Rumsfeld, Secretary, DOD
General John A. Gordon, DOE, NNSA
Honorable David Walker, GAO
Gary H. Friedman, Inspector General, DOE
John Hamre, President and CEO, CSIS
Executive Director, Danielle Brian, Project On Government Oversight

Appendix MM:

"Summary Report on Allegations Concerning the Department of Energy Site Safeguards and Security Planning Process," Department of Energy Office of Inspector General

September 2000

DOE/IG-0482

INSPECTION REPORT

SUMMARY REPORT ON ALLEGATIONS CONCERNING THE DEPARTMENT OF ENERGY'S SITE SAFEGUARDS AND SECURITY PLANNING PROCESS

SEPTEMBER 2000

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF INSPECTIONS

Department of Energy

Washington, DC 20585

September 28, 2000

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman /s/
Inspector General

SUBJECT: INFORMATION: Summary Report on "Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process" DOE/IG-0482

BACKGROUND

The Director, Office of Security and Emergency Operations provided the Office of Inspector General with a letter he had received which raised allegations of serious improprieties in the Department of Energy's Site Safeguards and Security Planning (SSSP) process. Specifically, the letter included allegations that a number of people within the Department were "lying in the reporting of the actual status of security" at the Department's most important nuclear sites, and that a contractor's findings under the SSSP Quality Assurance (QA) process were either ignored or not acted upon in a timely manner. In addition, it was alleged that "illegal" retaliation was taken against those who were trying to correct the Department's security problems through SSSP reviews or through assistance to a special assistant to the Secretary on Department security issues. The Office of Inspector General initiated an inspection to evaluate these issues.

RESULTS OF INSPECTION

While the inspection disclosed significant problems in the SSSP process as it was functioning at the time referred to in the allegations, the evidence did not support the principal points raised in the letter. Specifically, the inspection findings did not support the allegations that Department officials:

- lied in the reporting of the actual status of security at the Department's most important nuclear sites; or

- suffered retaliation for their part in the review of SSSPs, or for assisting a special assistant to the Secretary of Energy.

We did find that an employee of a support services contractor believed that an Office of Safeguards and Security program manager threatened him with a reduction in contract activity for his role in supporting the SSSP QA process and for assisting the special assistant to the Secretary. However, the program manager denied making such threats.

We did identify significant problems in the manner in which SSSPs were reviewed and SSSP QA issues were closed during the period referred to in the allegations. Specifically:

- There were substantial differences in what was being reported as the actual status of security at Department sites by the SSSP QA function, and what was being reported by the cognizant sites.

- Final Departmental decisions on how to address the SSSP QA issues were often complicated or delayed by disagreements between field and Headquarters elements over fundamental questions such as interpretation of the Design Basis Threat, adversary capabilities, and the assumptions related to worst case scenarios. These relationships were often so acrimonious as to threaten the effectiveness of the SSSP process.

- Since there was no process to resolve SSSP QA issues in coordination with the SSSP QA function, certain "Risk" issues remained unresolved at the SSSP QA level or were not fully evaluated.

The inspection disclosed that the allegations primarily concerned an SSSP process that has been phased out by the Department. The Office of Security and Emergency Operations is implementing a new process that is intended to address many of the problems that developed during past reviews of SSSPs. We concluded that the Department's restructuring of the SSSP process, if implemented and executed as planned, has the potential for resolving disagreements over the fundamental questions that affect SSSP "Risk" determinations.

This report includes several recommendations for the Director of the Office of Security and Emergency Operations: most notably, to establish a policy on what actions are required once high and moderate risks are identified through the SSSP process; and, to ensure that a dispute resolution process resolves disagreements that occur.

MANAGEMENT REACTION

The Director of the Office of Security and Emergency Operations stated that he had reviewed the Draft Report, and concurred. The Director stated that the conclusions offered in the Draft Report were appropriate. Although the Director has not committed to implementing the inspection recommendations, he stated that he would review the relevance of the recommendations in light of other policy initiatives currently underway to ensure that they are complementary. He also stated that if it is determined that the recommendations are appropriate and represent added value to the Site Safeguards and Security Planning Process, they will be implemented.

Attachment

cc: Deputy Secretary
Under Secretary for Nuclear Security/Administrator for National Security
Under Secretary for Energy, Science and Environment
Deputy Administrator for Defense Programs
Director, Office of Security and Emergency Operations
Director, Office of Security Affairs
Director, Office of Safeguards and Security
Director, Office of Defense Nuclear Security
Assistant Secretary for Environmental Management
Manager, Albuquerque Operations Office
Manager, Rocky Flats Field Office
Director, Transportation Safeguards Division
Director, Office of Security Support, Defense Programs

SUMMARY REPORT ON ALLEGATIONS CONCERNING THE DEPARTMENT OF ENERGY'S SITE SAFEGUARDS AND SECURITY PLANNING PROCESS

TABLE OF CONTENTS

Overview

INTRODUCTION AND OBJECTIVE

In January 2000, the Office of Inspector General received an allegation that there were serious improprieties in the Department's Site Safeguards and Security Planning (SSSP) process. Specifically, it was alleged that a number of people within the Department were "lying in the reporting of the actual status of security" at the Department's most important nuclear sites. Specific allegations were made regarding the Rocky Flats Environmental and Technology Site (RFETS), the Transportation Safeguards Division (TSD), and Los Alamos National Laboratory (LANL). In addition, it was alleged that "illegal" retaliation was taken against those who were trying to correct the Department's security problems through SSSP reviews or through assistance to a special assistant to the Secretary on Department security issues.

Based on these allegations, the Office of Inspector General initiated an inspection to determine if:

- officials within the Department were lying in the reporting of the actual status of security at the Department's most important nuclear sites;
- appropriate actions were taken to evaluate and resolve High Risk concerns;
- there was a systematic pattern of "dumbing" down the SSSP process; and,
- there has been retaliation against those who were trying to correct security problems.

As noted above, this inspection focused on the manner in which the contractor's concerns were addressed by Department security officials once they were raised. The issue of whether or not certain risk conditions actually existed at Department sites, as alleged, was beyond the scope of our review.

OBSERVATIONS AND CONCLUSIONS

REPORTING OF THE ACTUAL STATUS OF SECURITY

The Office of Inspector General found no evidence to support the allegation that Department officials lied in the reporting of the actual status of security at RFETS, TSD, and LANL. Contrary to this allegation, the results of our inspection revealed that Department officials took steps to assure that many of the SSSP QA issues reported by the contractor and the QA function were briefed at the highest levels of Department management.

However, a comparison of the SSSP QA analyses prepared by the contractor, and SSSP correspondence and documentation prepared and approved by the Department's Field and Headquarters Program Offices, did reveal substantial differences in what was being reported as the actual status of security at these three sites. We found that these differences were the result of significant, and, at times, bitter disagreements over the underlying basis of the SSSP QA issues raised by the contractor. The contractor's QA concerns were not well received at the Field Office level, the Program Office level, or by certain elements of the Office of Safeguards and Security. In several instances, the QA analyses performed by the contractor used different assumptions than had been used by the sites to develop their draft SSSPs, creating contention over the contractor's determinations of risk. The risk conditions identified and reported by the contractor were not universally accepted within the Office of Safeguards and Security or by the affected field sites and Program Offices.

ACTIONS TO EVALUATE AND RESOLVE HIGH RISK CONCERNS

Field and Headquarters elements considered and reviewed the QA issues identified by the contractor and the QA function. However, decisions on how to address the QA security concerns were often complicated or delayed by disagreements over fundamental questions such as interpretation of the Design Basis Threat, adversary capabilities, and the assumptions that went into the identification, modeling, and testing of worst case scenarios. For example:

- The contractor and the QA function reported a High Risk concern at a RFETS facility in March 1997. The condition underlying the High Risk concern was not resolved at the QA level for nearly two and one-half years, and the corrective actions taken in October 1999 were still disputed by the site with regard to the necessity for these actions.

Many of the QA issues were briefed within the highest levels of Department management, yet we could not identify a systematic process for resolving and closing the QA issues in coordination with the QA function. As a result, certain issues remained

unresolved at the QA level or were not fully evaluated. For example:

- The contractor and the QA function reported two High Risk scenarios involving TSD operations during its review of TSD's draft September 1998 SSSP. However, the High Risk label was removed from the discussions on one of these issues, and the issue of High Risk in this case was never resolved with the QA function. The Office of Safeguards and Security and TSD did agree to address many of the underlying security concerns that contributed to the QA assertion of High Risk.

- During a limited review of LANL's draft 1999 SSSP, the contractor and the QA function reported that SNM was not at low risk at a LANL facility. However, the issues identified in the contractor's final SSSP QA analysis were not forwarded to the Albuquerque Operations Office or the site for evaluation prior to SSSP concurrence by the Office of Security Affairs.

NO EVIDENCE OF "DUMBING" DOWN THE SSSP PROCESS

We concluded that the "new" SSSP procedures being implemented by the Office of Security and Emergency Operations did not reflect a systematic pattern of "dumbing" down the SSSP process. In fact, we concluded that the new SSSP procedures have the potential for significantly enhancing the SSSP process. Nevertheless, given the Department's past experiences in the security area, strong management involvement will be needed to assure that the "new" process achieves its potential. The Secretary of Energy assigned this role to the Director, Office of Security and Emergency Operations, in June 1999, and stated that the new Director has "the experience, expertise and determination to change the security culture at DOE." This role will have to be re-evaluated in light of the establishment of the National Nuclear Security Administration.

The Department began restructuring the SSSP process in May 1999. The Office of Safeguards and Security believed that the "old" SSSP QA process caused a great deal of contention when Headquarters Offices performed "a post-facto" verification and validation exercise using tools or approaches different than those used to perform the initial risk assessment by the sites. In May 1999, the Under Secretary directed that an SSSP Working Group be formed to provide "new" detailed procedures for the development and approval of SSSPs. The most significant changes from the "old" to the "new" SSSP process was the introduction of a "participatory approach" to the preparation of the SSSPs. The "participatory approach" involves field elements and various Headquarters offices in the SSSP development from the beginning,

eliminating the need for a "post-facto" QA function. Under the "participatory approach," agreement is to be reached on the Design Basis Threat, adversary capabilities, and the assumptions that go into the identification, modeling, and testing of worst case scenarios early in the process, thereby avoiding the introduction of different interpretations and assumptions at the end.

The "new" process also introduced a different approach to "Risk." Under the new process, "risk avoidance" was replaced by the concept of "risk management." As described to us, the "new" process emphasizes the necessity of a common, up front agreement on factors that are absolutely critical to the structure of the protection systems designed to counter adversary acts. We concluded that the "new" process must not only move the discussion on the Design Basis Threat, adversary capabilities, and worst case scenarios to the beginning of the SSSP process, but must also provide for the resolution of disputes on these issues when they occur. We also concluded that the "new" process can be most effective if the "Risk" determinations are driven by a consensus within the Department on the interpretation of the Design Basis Threat, adversary capabilities, and worst case scenarios rather than based on the preferences of a single site and/or a Program Office. The Director of the Office of Safeguards and Security told us that "this will be the case."

The inspection disclosed that the "new" process appears to be evolving in a way that will address disputes and the factors affecting "Risk." For example, a newly formed Threat Assessment Quality Panel has assumed responsibility for matters relating to the Design Basis Threat, and any issues not resolved by this panel will be raised to the Security Management Board.[1] In addition, the Threat Assessment Quality Panel has recently issued guidance to Department sites regarding the applicable adversary capabilities under the specific elements of the Design Basis Threat.

The "new" process was first used in April 2000 for the 2000 TSD SSSP. We have not evaluated the effectiveness of this process.

RETALIATION

We found no evidence of retaliation as alleged with respect to Department officials. Interviews of Department officials who were alleged to have been retaliated against for their part in the review of SSSPs, or for assisting a special assistant to the Secretary of Energy on security issues, did not support the allegation of retaliation. However, one support services contractor believed that

[1] The Security Management Board was abolished in October 1999, and a new organization to take over its responsibilities has not been established.

an OSS program manager threatened him with a reduction in contract activity for his role in supporting the SSSP QA process and for assisting the special assistant. The contractor said that he did not receive any contract work in the area of field assistance after the alleged threat was made, and that he viewed the elimination of his field assistance activities as retaliation. However, the OSS program manager denied any retaliation and said that he had no opportunity to provide contract work to this individual during the period in question. Subsequently, the contractor received other contract work, including work from the Director, Office of Security and Emergency Operations, and did not seek to formally address any concerns about alleged retaliation.

We also found no evidence that another support services contractor was retaliated against. The contractor offered a reduction in billable hours as evidence that the contractor was being retaliated against. However, while some Office of Safeguards and Security officials expressed dissatisfaction with the contractor, the use of the contractor by the Office of Safeguards and Security has continued. Office of Safeguards and Security records show that the contractor's billable hours had dropped off significantly in one area, but a review of the contractor's total direct productive labor hours over the past year showed only a slight decline in the overall use of the contractor by the Office of Safeguards and Security.

The evidence shows that the Department's shift from the "old" to the "new" SSSP process, and not retaliation on the part of any OSS official, more likely than not was the cause of this decline. The shift from the "old" to the "new" SSSP process nearly eliminated this company as a support services contractor. However, the contractor's direct productive labor hours have been sustained close to previous levels by providing support in other security areas.

Recommendations

We recommend that the Director of the Office of Security and Emergency Operations:

1. Establish policy on what actions are required once High Risk and Moderate Risk are identified through the SSSP process, including the resolution of High Risk and Moderate Risk issues within specific timeframes; and the consideration for compensatory measures, formal acceptance of risk, and mitigation of risk through operational changes.

2. Ensure that a dispute resolution process is incorporated within the responsibilities of the Threat Assessment Quality Panel and the successor organization to the Security Management Board so that disagreements on the interpretation of the Design Basis Threat, adversary capabilities, and the assumptions that go into the identification, modeling, and testing of worst case scenarios are addressed at the highest level of management.

3. This recommendation is classified.

4. Ensure that TSD validates the Special Response Force through the use of performance testing of the worst case scenarios.

5. Evaluate TSD's performance testing program and assure that all performance tests used to validate their SSSPs (a) are not encumbered by training priorities, (b) constitute legitimate force-on-force activities without coaching by instructors/controller, and (c) provide results that are conclusive in terms of measuring the ability of Special Agents to perform in response to an actual attack.

6. Ensure that TSD validates all other corrective actions that were identified on the "TSD Interim Disposition of NN Comments" matrix.

7. Ensure that TSD identifies a site suitable for conducting force-on-force exercises for worst case scenarios.

8. Evaluate the concern that a "Super Adversary" is created by the application of the Design Basis Threat to worst case scenarios, and determine what action is needed to disseminate more prescriptive policy on adversary capabilities so that the threat and adversary attributes contained in the Design Basis Threat are clear, concise and universally understood by the Office of Security Affairs, Office of Independent Oversight and

Performance Assurance, the Program Offices, and all affected field elements.

It should be noted that certain recommendations originally sent to the Director, Office of Security and Emergency Operations for comment are now the responsibility of the Under Secretary for Nuclear Security/Administrator for National Security.

MANAGEMENT COMMENTS

Officials from the Office of Security and Emergency Operations provided several comments to the initial Draft Report dated July 21, 2000. Appropriate changes were made based on these comments, and a second draft report was issued on August 31, 2000.

In comments provided to the second Draft Report, the Director of the Office of Security and Emergency Operations stated that he had reviewed the Draft Report, and concurred. The Director stated that the conclusions offered in the Draft Report were appropriate, and that it appeared that most of the comments provided by members of the Office of Security and Emergency Operations on the initial Draft Report had been incorporated into this version.

While the Director did not commit to implementing the recommendations, he stated that he would review the relevance of the recommendations in light of other policy initiatives currently underway to ensure that they are complementary. He also stated that if it is determined that the recommendations are appropriate and represent added value to the Site Safeguards and Security Planning Process, they will be implemented. In addition, the Director stated that he would forward to the National Nuclear Security Administration, Office of Defense Nuclear Security, those recommendations that fall under their purview.

INSPECTOR COMMENTS

Since the Director of the Office of Security and Emergency Operations did not specifically concur or non-concur with the report recommendations, we believe it is critical that the Director's initial submission under the Department's Audit Report Tracking System (DARTS) clearly defines the rational for determining that any of the recommended actions are not appropriate or do not represent added value to the Site Safeguards and Security Planning Process. In addition, the Office of Security and Emergency Operations, in coordination with the National Nuclear Security Administration, should clearly define their plan for corrective actions in their initial submission under DARTS.

Appendix A

SCOPE AND METHODOLOGY

While reviewing the allegations discussed in this report, we evaluated:

- The reporting of the status of security at RFETS, TSD, and LANL through the SSSP process.
- The appropriateness of the actions taken by Department management to evaluate and resolve High Risk concerns identified by the contractor and the SSSP QA function.
- The appropriateness of the actions taken by Department management to evaluate and resolve other security weaknesses identified by the contractor.
- Changes to the SSSP process that eliminated the post-facto SSSP QA reviews.
- The issue of retaliation as it related to certain Department and contractor employees who were involved in the SSSP QA process.

As part of our review, we interviewed officials from the contractor organization, Los Alamos National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Department officials from the Office of Security and Emergency Operations, the Office of Safeguards and Security, the Office of Security Affairs, the Office of Defense Programs, the Office of Environmental Management, TSD, and the Albuquerque Operations Office.

In addition, we also reviewed documentation relating to the SSSP QA process, including: (1) SSSPs for TSD and LANL; (2) SSSP QA reports, including ALPHA Reports, Physical Security Systems Reports, an Integrated Report for TSD, and JTS Reports; (3) a Format and Content Guide for SSSPs; (4) Acceptance Criteria and Review Guide for SSSPs; (5) a Final Report of the Design Basis Threat Working Group and the SSSP Working Group; (6) the SSSP Rollout 2000 Workshop Report and the Tool Box Evaluation; (7) the Vulnerability Assessment Program Workshop Report; and (8) applicable Department of Energy Orders and Directives regarding security at Department sites.

This inspection was performed between January and June 2000. This inspection was conducted in accordance with the "Quality Standards for Inspection" issued by the President's Council on Integrity and Efficiency.

Appendix B

BACKGROUND

The SSSP describes safeguards and security programs and vulnerability and risk analysis at applicable sites. The SSSP is the primary instrument that the Department's Operations Office Managers use to certify to the Secretary of Energy the accuracy of risk and the measures used to assure that the public, employees, environment, and national assets are adequately protected. The SSSP is approved by Heads of Field Elements and concurred in by the cognizant Program Office and the Office of Security Affairs.

All SSSPs are to be certified annually as being current and valid, and are to be updated and approved at least once every five years unless a more frequent cycle is warranted. The Operations Office/Field Office Manager, in consultation with the Program Offices, Office of Independent Oversight and Performance Assurance, and the Office of Security Affairs, can direct that the SSSP be updated to reflect evolving threats and changes in a site's security posture.

In 1997, the Office of Nonproliferation and National Security began what they called "a rigorous and disciplined" QA process as part of the "review and verification" of the Department's SSSPs (referred to as the SSSP QA process). The Office of Safeguards and Security had found significant deficiencies in reporting "Risk," often due to the characterization of the Design Basis Threat and scenarios that did not stress the worst case. During this period, the Office of Safeguards and Security assigned the contractor the task of supporting the SSSP QA effort.

In an August 21, 1997, memorandum to various OSS Division Directors, the Director of OSS issued criteria and methodology that would be employed in the reviews of SSSPs. The purpose of this criteria and methodology was to address systemic SSSP verification issues that had arisen during prior reviews.

The SSSP QA process employed the use of three specific tools for review and verification of the Department's SSSPs. These included:

- Joint Tactical Simulation (JTS) - an interactive, entity-level conflict simulation modeling tool;
- Advanced Logic Protection Heuristic Analysis (ALPHA) - a vulnerability assessment tool; and,
- Physical Security Systems Reviews (PSSRs) - examinations, tests, and evaluations of the effectiveness of physical security systems.

In a November 4, 1998, memorandum to the OSS Acting Director, Field Operations Division, the OSS Director stated that he considered the reviews of SSSPs to be a "critical principle" function of OSS. The Director stated that the three "primary tools" used, ALPHA, JTS, and PSSRs, must be carefully integrated and appropriately documented for each SSSP. The Director also stated that it was expected that each of these tools would be used to evaluate all SSSPs unless timely equivalent information existed. The Director recognized that a "constructive tension condition" existed between the Safeguards and Security office responsible for the SSSP QA process and the Safeguards and Security office responsible for field assistance and expediting OSS concurrence with SSSP's. However, he stated that these checks and balances would result in a more effective safeguards and security program.

As part of its support role associated with the SSSP QA effort, the contractor reported that High Risk security conditions existed at the Rocky Flats Environmental Technology Site, and the Transportation Safeguards Division. Further, with regard to Los Alamos National Laboratory, the contractor concluded that "there is insufficient evidence to provide reasonable assurance that SNM [Special Nuclear Material] is protected to the standard required by the Department. . . . That is, SNM is not at low risk . . . ."

The contractor alleged that findings at these three sites were either ignored, or not acted upon in a timely manner. For example, it was alleged that the contractor identified High Risk at RFETS in March 1997, but no action was taken to address the High Risk condition until November 1999. Also, the contractor allegedly identified High Risk conditions involving TSD operations in the fall of 1998 that were never addressed, and that allegedly remain today. In reviewing the LANL SSSP in November 1999, the contractor allegedly found major problems with the ability of the protective force to deal with worst case scenarios that were never addressed, and also allegedly remain today. The contractor also alleged that the SSSP QA review process is currently being restructured, and that documents for this effort show a systematic pattern of "dumbing" down the SSSP process. The contractor explained that the SSSP QA process is being subverted so that SSSP development becomes a joint Field/Headquarters function with no independent review.

Appendix C

DEFINITIONS

Risk	Risk is defined as Low, Moderate, or High. Risk ratings are determined by evaluating the effectiveness of the protection system against events such as the threat of the theft of Special Nuclear Material (SNM), weapons, and weapons components. Department policy states that Low Risk Ratings are acceptable.
Design Basis Threat	The Design Basis Threat is a postulated threat used to design protective forces and security systems for the guarding of nuclear sites. The Design Basis Threat describes the most credible and serious potential adversaries, their tactics, numbers, and capabilities. The purpose of the Design Basis Threat is: (1) to provide a stable basis for security planning and budgeting that is predicated on a predetermined threat estimate which is not dependent on tactical intelligence, (2) to provide a baseline for DOE-wide protection standards for our most attractive nuclear assets, and (3) to provide a standard against which to evaluate the performance of protective forces and the effectiveness of installed security systems.
Verification and Validation	Verification is accomplished through the conduct of vulnerability assessments, use of modeling tools, evaluation of training and maintenance records, and table-top exercises of varying degrees of formality. Validation is a process where assumptions reached through assessments, modeling and evaluation activities are tested for validity, the predominant tool utilized being the performance test (ranging from tests of an individual's skills to a full scale force-on-force exercise).

Appendix NN:

DOE Notification Letter from Owen Johnson, Director Office of Safeguard and Security

October 26, 2000

Department of Energy
Germantown, MD 20874-1290

OCT 2 6 2000

[redacted]

Dear [redacted]

NOTIFICATION LETTER

Reference is made to the letter from Floyd R. McCloud, Acting Director, Headquarters Operations Division, Office of Safeguards and Security, dated [redacted] notifying you that your Department of Energy (DOE) access authorization had been suspended.

This letter is to notify you that reliable information in the possession of the DOE has created a substantial doubt under title 10, Code of Federal Regulations, Part 710 (10 CFR 710), regarding your continued eligibility for a DOE access authorization. That information is contained in the enclosed summary of information developed which is entitled, "Summary of Information Creating a Substantial Doubt Regarding Continued Eligibility for Access Authorization" (Enclosure 1).

For the purpose of supporting your continued eligibility for a DOE access authorization, you have two options. You may request that I make a final determination in your case on the basis of the existing information, or you may appear personally before a Hearing Officer. To avail yourself of the opportunity for a hearing, you must, within 20 calendar days of the date of receipt of this letter, request in writing a hearing before a Hearing Officer. You may also file with me your written answers to the reported information in the enclosed statement of charges. If you request a hearing without responding to the summary of information developed, your request will be considered as a general denial of all of the reported information.

Upon receipt of your request for a hearing before a Hearing Officer, a hearing will be scheduled with due regard for the convenience and necessity of the parties or their representatives. The Hearing Officer will be appointed by the Director, Office of Hearings and Appeals, DOE. The purpose of the hearing is to afford you the opportunity to support your eligibility for access authorization.

You will have the right to appear personally before the Hearing Officer and present evidence in your behalf through witnesses or by documents, or both, and subject to limitations set forth in 10 CFR 710, Section 710.26 (g), be present during the entire hearing. You may also be accompanied, represented, and advised by counsel or representative of your choice at each and every stage of the proceedings, at your own expense. The DOE Counsel will be participating on behalf of and representing the DOE in any proceedings in this matter, and any statements you make to the DOE Counsel may be used in subsequent proceedings.

Should you fail to file a written request for a hearing before a Hearing Officer within the time specified (unless time deadlines are extended for good cause), this failure will be considered as a relinquishment by you of your right to a hearing. In such event, I will make a final decision regarding your eligibility for a DOE access authorization on the basis of existing information in your case, and that decision will not be subject to appeal.

A copy of 10 CFR 710, Subpart A, which governs the procedures followed in this matter, is enclosed for your information and guidance (Enclosure 2).

Should you desire any further information, including an explanation of your rights with respect to access to your DOE personnel security file under the Freedom of Information and/or Privacy Acts (FOI/PA), you or your representative may contact Ms. Dorothy Turner who has been designated the DOE official point of contact in this case. Ms. Turner may be reached at (301) 903-3743.

This letter has been marked "Official Use Only" merely to maintain the privacy of this matter between you and the United States Government, but does not preclude use of it as you may deem appropriate.

Sincerely,

Owen B. Johnson
Director
Office of Safeguards and Security

Enclosures

Enclosure 1

SUMMARY OF INFORMATION CREATING A SUBSTANTIAL DOUBT REGARDING CONTINUED ELIGIBILITY FOR ACCESS AUTHORIZATION

[redacted]

I. Information in the possession of the U. S. Department of Energy (DOE) indicates that you have engaged in unusual conduct or are subject to circumstances which tend to show that you are not honest, reliable, or trustworthy, or which furnishes reason to believe that you may be subject to pressure, coercion, exploitation, or duress which may cause you to act contrary to the best interests of the national security. Such conduct or circumstances include, but are not limited to, criminal behavior, a pattern of financial irresponsibility, or violation of any commitment or promise upon which DOE previously relied to favorably resolve an issue of access authorization eligibility. This constitutes substantially derogatory information within the meaning of title 10, Code of Federal Regulations (10 CFR 710), Section 710.8(l). The bases for this statement are as follows:

A. On June 26, 2000, an unsuccessful attempt was made to transmit an 18 page facsimile of information to the Editor of The Washington Post from the facsimile machine in room E-364 of the DOE Germantown Building. It appeared from a communication result report at the scene that the originator of this failed transmission was [redacted]an employee in the Office of Safeguards and Security. [redacted]denied any knowledge of, or participation in this matter.

Additional information was developed showing that a successful transmission was made on June 26, 2000, to USA Today of a facsimile consisting of a cover sheet and 18 pages of information, from the facsimile machine in room C-361 of the DOE Germantown Building. This facsimile was intended for Jeff Stinson, a reporter for USA Today.

B. Efforts by DOE security personnel to identify the facsimile originator, the content of the above facsimiles, and whether facsimile information was classified, were the focal points of DOE security interviews of a number of Federal and contractor employees assigned at the Germantown DOE Building. In this regard, you were interviewed on August 4, 2000, during which you identified your DOE office space at Germantown, acknowledged that you have a key to the office of 2 subordinates, and identified the locations of various facsimile machines available to you and DOE Field Operations employees at Germantown. You stated that you were unaware of any official reason that an employee of the Office of Safeguards and Security would contact news

organizations independently. You indicated that it was your understanding that DOE employees' responsibility with regard to direct contact with news organizations was to route all such requests through the DOE "chain of command." When asked by a DOE security representative if you knew who "Jeff Stinson" was, you replied, "no." During this August 4, 2000 interview, you were not queried directly if you had sent the facsimiles in question, but you were informed that an extensive effort was underway to ascertain the content and source of the facsimiles; and at no time did you offer information about any involvement on your part.

C. During a reinterview by DOE security representatives on August 7, 2000, you were again informed that the goal of the inquiry was to identify whoever was responsible for the facsimile messages to the news media on June 26, 2000, the specific nature of the information, and whether it was classified. You were also advised that a significant amount of evidence had been gathered which strongly suggested that you were responsible for sending the 2 facsimiles in question. You asked whether this matter would be resolved if you took a polygraph examination and it indicated that no classified information had been transmitted. You were advised that the documents for the news media had to be identified, and even if the information was not classified, there was still the issue of communicating directly with the news media. You commented that "it wasn't classified" and declined to answer any more questions.

D. In accordance with your August 8, 2000, telephonic request, you were reinterviewed on August 9, 2000. At that time, you admitted that you sent 2 facsimiles to news organizations on June 26, 2000, the first of which was to the Editor of The Washington Post newspaper, transmitted from the facsimile machine in room E-364 of the DOE Germantown Building. You added that you sent the second facsimile to Jeff Stinson of USA Today newspaper, from the facsimile machine in room C-361 of the DOE Germantown Building. You said that both facsimiles were of the same DOE document, a draft report by the DOE Office of Inspector General dated March 22, 2000, alleging deficiencies in security surveys conducted by the Albuquerque Operations Office and Security Self Assessments conducted by the Los Alamos National Laboratory. You stated that you obtained a copy of the OIG report from your supervisor who informed you that the report had been evaluated as unclassified. You made a copy of the report, and when you heard that an inquiry into this matter had been initiated, you shredded the document you had sent; and while you could not reconstruct what you transmitted, you said that it is entirely possible that you sent 18 pages of text plus a 1 page facsimile cover sheet to both news organizations.

As to your rationale in transmitting the draft OIG report to USA Today, and attempting to transmit it to The Washington Post, you said that on the weekend of June 24-25, 2000, there were several television news reports concerning security lapses at Los Alamos National Laboratory (LANL) which criticized DOE and LANL for what you considered relatively minor security lapses; whereas, you believed there were other issues of greater security significance involved, including the inadequacy of DOE's Security Survey Program. You said that you

thought that if you brought this inadequacy to light, then senior DOE officials might be "sparked" into improving that program. Accordingly, you decided to send a copy of the draft OIG report to the news media to "make things better." You added that you used the name, "[redacted]" on the facsimile cover sheet for 2 reasons: (1) you did not want to use your own name out of fear that a Washington Post reporter might follow up with you at work which could alert DOE personnel as to what was going on; (2) you wanted the facsimile transmission to be taken seriously, and if a reporter would scan the DOE phone book or the DOE web site to verify that [redacted] was indeed a DOE security employee, it would add validity to the facsimile. You admitted calling representatives of both news organizations after sending the facsimile to USA Today and apparently sending the same facsimile to The Washington Post to confirm receipt of your transmissions.

Continuing in your August 9, 2000 reinterview, you said that you did not believe that the information you sent or attempted to send to the news media in this case was classified, proprietary, or sensitive. You also denied knowing that it is not permissible to send DOE information directly to the news media. Your denial is contrary to your comments in the August 4, 2000 interview contained in paragraph I.B., supra. You also said that you did not remember having read the memorandum from the Director, Office of Security Affairs, dated March 18, 1999, regarding unauthorized contact with the news media; nor could you remember having signed a statement that you would protect classified, proprietary, and sensitive information.

E. The memorandum of March 18, 1999, from the Director, Office of Security Affairs, to all Federal and contractor employees in the Office of Security Affairs and the Office of Safeguards and Security, addressed the integrity of DOE security operations, stating:

> "I regret to report to you that I have received information that a person or persons working in the Office of Security Affairs or the Office of Safeguards and Security may have released, or caused to be released, internal drafts and other information concerning the Department's security operations to persons outside the Department with no official need to know of this information.
>
> "I am particularly disturbed by the possibility of unauthorized disclosures from our security organizations because of the extremely sensitive nature of the information we possess, including not only highly classified information, but also Privacy Act protected sensitive law enforcement, and proprietary information. We are also the organization charged under Departmental orders to investigate unauthorized disclosures of

> classified or sensitive information. The possibility that we cannot ensure the protection of information entrusted to us is completely unacceptable. Simply put, I have zero tolerance for unauthorized disclosures and I will take every action available to me, under law, authorities delegated to me by the Secretary and Departmental directives, or seek appropriate additional action from other authorities, against any person or persons found responsible for unauthorized disclosures.
>
> "To this end, I am requesting that all Federal employees and support contractors assigned to the Office of Security Affairs and the Office of Safeguards and Security execute the attached statement attesting that they understand fully their responsibilities to protect the information entrusted to us. If any person has questions concerning their responsibilities, please let your supervisor know and we will provide prompt answers. Thank you for your support in this vital initiative, and I ask your continuing commitment to preserve the integrity of our security operations."

On March 29, 1999, you signed the security responsibility statement attached to the foregoing memorandum, and returned it to the Director, Office of Security Affairs.

F. Your June 26, 2000 facsimile transmission to the news media of the 18-page OIG draft report, entitled, "Report on the Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operation' Self Assessments at Los Alamos National Laboratory," was one of two OIG reports on the same subject that were forwarded by OIG memorandum of March 22, 2000, to the DOE Office of Security and Emergency Operations to determine if they contained classified information. The first was intended for public dissemination, while the second (the one which you sent to USA Today and the one you attempted to send to The Washington Post) contained significantly more detail and was intended for "limited distribution due to Privacy Act considerations." The OIG memorandum of March 22, 2000, cautioned:

> "These reports are the property of the Office of Inspector General and should be protected as Secret/National Security Information, until reviewed and determined to be unclassified. Appropriate safeguards should be provided for the reports and access should be limited to Department of Energy officials who have proper clearance and need to know. Since the draft reports are subject to change and, and (sic) therefore, do not represent the final position

> of the Office of Inspector General, the contents should be appropriately controlled and maintained. Public disclosure is determined by the Freedom of Information, Title 5, U.S.C. 552, and the Privacy Act, Title 5, U.S.C. 552a."

On March 29, 2000, the Office of Nuclear and National Security Information declared that both draft OIG reports were unclassified; and on May 30, 2000, the OIG released the public version of its report by publishing it on the OIG internet website. The second version of the OIG report, the one that you disseminated, was written for limited distribution within DOE, and was never distributed to the public, except for your unilateral decision to do so. You claimed to have closely reviewed the document involved when you received it from your supervisor; so you should have taken due notice of the precautionary language in the OIG cover memorandum. Your earlier contention, therefore, that the document was not sensitive, is not justified.

With additional emphasis on the gravity and consequences of your transmission to the news media of the draft DOE OIG report, an OIG official advised that that report contained sensitive Privacy Act information, including the identities of individuals interviewed by OIG as well as the nature of the information they furnished during the inquiry into alleged wrongdoing within the security survey and self assessment programs at the Albuquerque Operations Office and Los Alamos National Laboratory. Further, that draft report was protected under the Privacy Act and the Freedom of Information Act, and should not have been sent to anyone except those few DOE officials designated by OIG. According to the DOE OIG Director, Office of Program Operations, Office of Inspections, OIG did not give anyone permission to transmit the draft report outside of DOE channels. And there is an issue with respect to violating Title 5, U.S. Code, Sections 552 and 552a, by disseminating a document considered to be sensitive and to be protected by those laws.

G. DOE security officials again interviewed you on August 16, 2000. You reiterated your previous observation that "it was astounding" that there was so much interest on issues within DOE that were "not critical," leading to your decision to share with the media the information in the draft OIG report, which you described as "public information," to bring focus on the problems in the survey program. You opined that "nothing in that report targeted people, personalities or organizations, but rather, it was process related." You said you weren't sure what "pushed you over the edge" to disseminate that document, but guessed that it was more stories about Los Alamos.

You recalled your conversation with Jeff Stinson of USA Today concerning Stinson's receipt of the your facsimile, when Stinson asked you if this was the facsimile from [redacted] and your acknowledgment that it was the referenced facsimile but that [redacted] did not send it and that "that was just a name I used." When asked in this DOE interview why you used [redacted] name, you replied that you wanted to use a name different from your own because you assumed

concern was that you would be embarrassed or turn red as you know you do when you are "lying or embarrassed;" whereas, if a reporter were to call [redacted] about this matter [redacted] could say that he didn't know what they were talking about, and that "would be the end of the story." You said that you chose [redacted] name at random for the appearance of authenticity. You admitted that attributing the facsimile to him was a "very bad error in judgment" on your part; that you do not dislike [redacted] and were not trying to "set him up." You said that you now know that using [redacted]'s name was a "huge mistake."

Continuing in the interview of August 16, 2000, with earlier reference to the proper interface with news organizations and your comment about going through the DOE "chain of command," you said that you recalled saying then that official communications with the press were handled by the Office of Public Affairs, but that you still felt that individuals had the right to go directly to the news media if they so desired. When asked if you recalled receiving an e-mail from the Director of the Office of Safeguards and Security about interaction with the press, you stated that you did not recall such a message. You added that you thought what you were doing was "all right, but it obviously was not all right." You denied providing the press with any other documents at any other time, adding that you had access to a large number of documents which "would prove embarrassing to the Department," but that you would never release them. You also said that after the inquiry began in this matter, you decided to "never send anything to the newspapers again;" and that you were not "out to get" any of your managers, and had no intention of harming anyone.

II. Information in the possession of the DOE indicates that you have deliberately misrepresented, falsified, or omitted significant information from a Personnel Security Questionnaire, a Questionnaire for Sensitive Positions, a personnel qualifications statement, a personnel security interview, written or oral statements made in response to official inquiry on a matter that is relevant to a determination regarding eligibility for DOE access authorization, or proceedings conducted pursuant to sections 710.20 through 710.31. This constitutes substantially derogatory information within the meaning of title 10, Code of Federal Regulations (10 CFR 710), Section 710.8(f). The bases for this statement are as follows:

A. In your first interview with DOE security representatives on August 4, 2000, you acknowledged the procedures for handling media contact included going through the DOE "chain of command." In a subsequent interview, you said that your recollection of your August 4, 2000 comments were that "official" contact with the press should have been through the Office of Public Affairs, although that you still held a conflicting view that an individual employee could provide information directly to media sources. Your surreptitious behavior in releasing the OIG document to the press while concealing your own identity to the potential detriment of a fellow employee was at the least dishonest, and possibly illegal in its misrepresentation of the situation.

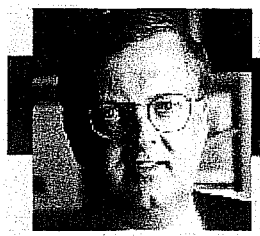
B. Also, in your first inquiry interview, you denied having any knowledge of the identity of Jeff Stinson; however, you later admitted Stinson was your point of contact at USA Today. You subsequently further qualified your statement about knowing Stinson by saying that you had not lied previously, and that you did not recall his name until you checked your records. These statements have a ring of disingenuousness considering that your comments throughout the interviews demonstrated that you were aware of the severity of your actions; that it was unlikely that if you had done this sort of thing only once, you would be so nonchalant about it to the point that you would not recall the name of the person to whom you transmitted the OIG document; and finally you acknowledged that having sent the information to the media would likely have a negative impact on your clearance and possibly your job. Attempting to conceal your identity as the source of the document and your transmission of it during the early morning hours when you would stand less of a chance of being observed further strengthen the contention that you were aware of the severity of your actions.

III. The cumulative effect of the information chronicled above in paragraphs I.A. through II. concerning the apparent abdication of your security responsibilities, your demonstrated lack of respect for security regulations in unilaterally interpreting and adjudicating what constitutes sensitive information and the conditions under which it is releasable in whole or in part by you, flouts basic DOE authority, and serves to directly impugn your judgment, reliability, and trustworthiness.

Appendix OO:

Statement of Edward J. McCallum, Director Office of Safeguards and Security

June 8, 1999



CONGRESSMAN CURT WELDON

7th District Pennsylvania

Edward McCallum, a whistle blower within the Department of Energy, has faced repercussion from a Clinton-Gore Administration who was not pleased with his brave and valiant efforts to ensure the protection of American nuclear secrets and improved security at DOE labs. What has been done to him is an injustice, but you can judge that for yourself.

Statement of Edward J. McCallum

Mr. Chairman, thank you for the opportunity to speak with the committee today on the Department of Energy's Safeguards and Security Program. Over the past nine years, I have served as the Director of DOE's Office of Safeguards and Security. In this capacity, I have been responsible for the development and promulgation of policy that governs the protection of the national security assets entrusted to the department, to include those assets that are part of the nation's nuclear weapons program. I am also responsible for providing training and specialized technical advice and assistance to DOE field sites when requested. My office is also charged with conducting special inquiries into incidents of security concern to include, but not limited to, those incidents involving the unauthorized disclosure of classified information.

As you may know the Department of Energy has placed me on Administrative Leave since April 19, 1999. DOE officials allege that I committed a security infraction by claiming that I disclosed classified information during a conversation with a whistleblower from the Rocky Flats site. Based on the Department's own classification procedures and guidelines (CG-SS-3, Chap 10, Dispersal of Radioactive Material), I firmly believe that these allegations are completely unfounded. I have been an authorized classifier in the DOE and it's predecessor organizations for over 25 years and helped develop the first classification guide in this area in 1975. Further DOE also failed to follow its own procedures in investigating these issues before placing me on Administrative Leave. I believe this action to be an obvious act of retaliation against the individual and the office that has tried to bring an increasingly distressing message of lax security at the DOE Laboratories forward since 1995.

Prior to joining the Office of Safeguards and Security I held several high level positions within the department's safeguards and security program areas. From 1988-1989 I served as Director, Office of Security Evaluations. In 1978 I joined the DOE at the Chicago Operations Office and in 1979 became the Director of the Safeguards and Security Division. Prior to joining DOE I served as an officer in the U.S. Army. Active military service included a number of Military Intelligence and Special Forces assignments in Europe and Southeast Asia. I culminated my military duty after over thirty years of active and reserve service.

In fulfilling my responsibilities as the Director, Office of Safeguards and Security, I have attempted to provide senior DOE management with the most sound, professional judgment possible concerning the status of security within the department, along with recommendations as to how best to rectify shortcomings. As you are no doubt aware, much of what I have offered over recent years has not been altogether positive, nor well received. The steady decline in resources available to the DOE

safeguards and security program as well as a lack of priority have allowed the department's protection posture to deteriorate to a point where a program that long operated in a defense in depth mode, where no single point failure permitted the system to fail, can no longer afford such a strategy.

The information presented in this statement is not new. It has been repeated consistently over the last decade in Departmental reports such as the Annual Reports to the Secretary in 1995, 1996 and 1997 by the Office of Safeguards and Security. External reviews such as the Report to the Secretary in 1991, by General James Freeze, and the Nuclear Command and Control Staff Report on Oversight in the DOE in 1998 cite similar concerns. There have also been a large number of General Accounting Office Reports on these areas. However, for numerous reasons the department has not been able to resolve these serious and longstanding problems.

COMPUTER SECURITY

One of the primary interests expressed by the Committee, and indeed widely covered by the media recently, is the loss of classified information from the computer systems at the National Laboratories. Indeed, we may be sitting at the center of the worst spy scandal in our Nation's history.

The DOE Computer Security Program suffers from a variety of problems. One of the primary concerns is the protection of unclassified sensitive information processed by the Department and the relationship of these systems to the classified architecture. Relatively little guidance has been issued on how to protect sensitive but unclassified information. System administrators are charged with the responsibility for designing their own protective measures. Unfortunately, many of them do not have the computer security background or knowledge required to implement a sound computer security program. Attempts to issue comprehensive guidance by my office and the Chief Information Officer as early as 1995 met with significant Laboratory resistance. Several Laboratories complained that providing protection such as firewalls and passwords were unnecessarily expensive and a hindrance to operations. Implementation of the proposed Computer Security Manual in 1996 would have prevented many of the problems being reported today.

Another area of great concern is the migration of classified information from systems approved for processing classified data to less secure unclassified processing systems. My office has noted a number of problems in this area to include: Failure to conduct classification reviews before placing information onto an unclassified processing system, intentionally creating unclassified data that is very close to classified data to ease processing, and using personal computers at home to process classified information.

A variety of computer security tools and techniques, such as encryption devices, firewalls, and disconnect features, are available and their use is required; however, these protective measures are not always used. In some cases, this is due to lack of knowledge by system administrators. In other cases, it is due to lack of funding or priority for the required equipment.

PROTECTIVE FORCES

While much of the attention of late has been directed toward the area of foreign visitors and the protection of classified information, equally serious cause for concern exists in other areas as well. For instance, since 1992, the number of protective forces at DOE sites nationwide has decreased by almost 40% (from 5,640 to the current number of approximately 3,500) while the inventory of nuclear material has increased by more than 30%. The number of Protective Force Officers has

declined to the point where it is questionable at some facilities whether the DOE Protective Force could defeat an adversary. By 1996 several facilities were no longer capable of recapturing a nuclear asset or facility if it were lost to an adversary. Indeed, a number of sites stopped even training for this mission because resources had been reduced below the minimum level necessary to expect success. We have had some success in increasing these numbers of recent years so that at this time all sites report they can meet this minimum capability. Several sites are using performance tests to verify that their Protective Force can defeat the adversary; however, many of these tests are not realistic. For example, performance tests sometimes are not consistent in providing the adversary with the weaponry or explosive breaching devices used by terrorist groups. At times artificial `safety constrains' are imposed on exercise adversary teams that effectively neutralize their ability to operate. This results in `winning' the performance test, in a less than realistic scenario.

There have been several other consequences of the reduction in the number of Protective Force Officers. First is a relatively older Protective Force (the average Protective Force Officer is now in his/her early 40s). Second, DOE sites are relying on local law enforcement agencies to handle serious security threats. Their ability in nuclear terrorist situations is questionable. Third, sites have difficulty increasing the tempo of security operations during high threat periods. Fourth, Protective Force personnel are displaying lower morale due to reduced training and job stagnation. Finally, an average annual overtime rate in our nuclear weapons facilities of approximately 25% has detrimental effects on safety, training, and response capabilities.

EXERCISES

A centrally funded and well-integrated National-level security exercise program is critical to meet the safeguards and protection needs of DOE and the nation. Exercises that address site response and management of security crisis are required by regulation to be held annually at critical DOE facilities. However, participation by State and local law enforcement, regional offices of the Federal Bureau of Investigation (FBI) and other Federal agencies is inconsistent and varies considerably across the complex. Under Presidential Decision Directives 39 and 62, the Secretary of Energy is directed to conduct exercises to ensure the safety and security of its nuclear facilities from terrorism. DOE is also tasked to support the FBI in its lead as the Federal agency responsible for managing all domestic incidents involving terrorist threat or use of weapons of mass destruction (WMD). In addition, the recent creation of the Department of Justice National Domestic Preparedness Office, the FBI Critical Incident Response Group (CIRG), and other National crisis response assets, requires that DOE plan and practice a new and expanded role in supporting a security crisis response beyond the local site and internal Department level.

Currently, the present DOE organizational structure separates exercise responsibility between Program offices and Safeguards and Security; this hampers the integration of sequential training objectives that can be monitored and tracked and creates confusion at the site level. More importantly, the majority of the funding resides at the site level where expenditures must vie with other program needs each fiscal year, often to their detriment.

PHYSICAL SECURITY SYSTEMS

Another area of concern involves aging and deteriorating security systems throughout the DOE complex. Physical security systems are critical to ensure the adequate protection of Special Nuclear Material (SNM). Many facilities have systems ranging in age from 14 to 21 years, and are based on mid-70's to early-80's technology. Because of the obsolescence of these systems, replacement parts

and services are increasingly expensive and hard to obtain. Expensive compensatory measures (i.e., protective force response) are required to ensure needed confidence levels of adequate protection. Older systems are also increasingly vulnerable to defeat by advanced technologies that are now readily and cheaply available to potential adversaries. Continual reductions, delays or cancellations in line-item construction funding increases the vulnerability risks to sites protection capability. Also, DOE is not realizing significant savings available through advancements in technology that have increased detection, assessment, and delay capabilities.

Some sites are using a variety of nonstandard security alarm and access control systems that have not been fully tested to determine if they contain vulnerabilities, or if they meet Departmental requirements without compensatory measures. Such systems may have back doors or viruses, that allow the insider adversary to cripple the entire site protection system, thus leaving the site vulnerable. Some sites do not have qualified personnel to conduct these vulnerability tests and are generally unwilling to conduct any type of attack on the system to determine if such vulnerabilities can be accomplished.

COUNTERTERRORISM MEASURES

PDD-39, The United States Policy on Counterterrorism, requires all governmental agencies to implement security measures to defend against Weapons of Mass Destruction, including chemical and biological weapons. The Office of Safeguards and Security has developed the necessary policies and requirements for implementing PDD-39. Field Elements, however, have been slow to purchase and install explosive detection systems, with only a limited number of sites having done so. Program Offices claim that there is no funding for such equipment.

PERSONNEL SECURITY

I fear that a recent decision by the department to have program offices fund the cost of clearances for field contractor personnel will have severe repercussions. Since implementing this new approach at the beginning of FY 1999, we have already begun to see a dramatic increase in the backlog of background investigations. As with other security areas, program offices must decide upon competing interests when determining those areas to be funded. Unfortunately, security activities are relegated to a lower tier in terms of importance by some program offices and selected field sites. This appears to be the case with the funding of security background investigations. As the first line of defense against the `insider' threat, the adequate funding and timely conduct of reinvestigations is critical to ensuring the department maintains a protection posture commensurate with the level of threat.

ROLES AND RESPONSIBILITIES

Operating beneath the surface of these major challenges are some fundamental issues that, if properly addressed, could provide the impetus to effect real progress. These challenges, for the most part, are not new, nor are their solutions.

Organizational Structure: In all of the reviews of the safeguards and security program conducted during the last decade, there is a recurring theme. Simply, the Department's organizational structure of the Safeguards and Security Program is such that programmatic authority and responsibility are not properly aligned. The Safeguards and Security Program in its current structure has one organization developing policy, training and providing technical field assistance (NN), another

organization providing funding and `implementing guidance' (Headquarters Program Offices), a third organization (Field Site) is responsible for implementation of policy, while a fourth (EH) is responsible for oversight. A fundamental change in both the organizational structure and funding of the Safeguards and Security Program is absolutely necessary before the Department can begin to systematically address the major challenges previously addressed. These organizations must be consolidated with policy, guidance and implementation in one location, with an appropriate budget to participate in the Department decision making.

Safeguards and Security Program Funding: This is the central, driving issue. Budget cutbacks have adversely affected all of DOE. As previously alluded to, however, when Program Offices face funding shortfalls, there is a tendency to cut security programs on a pro rata basis without the benefit of assessing the impact these cuts would have on the department's protection posture. The implementation of virtually every security program, from the Information Security Program to the Protective Force Program, has suffered significantly as a result. I believe many of these cuts are shortsighted and ill advised as they eventually lead to security lapses. Nevertheless, my office has no authority to force the Program Offices to implement departmental security policies and requirements. Similarly, my office has no funds to provide to Program Offices or Field Elements to help pay for appropriate security measures. Without an adequate budget there is simply no authority.

Security Policy and Requirements Formulation. DOE security policies and requirements are based upon current threat data and requirements identified by outside intelligence organizations. DOE, the Department of Defense, the Nuclear Regulatory Commission, the Federal Bureau of Investigation, and the Central Intelligence Agency meet every two years to evaluate current threat data and formulate an agreed upon threat statement that governs security programs throughout the U.S. Government. In addition, the Department of Energy internally reviews this threat statement annually. In DOE parlance, the resulting document is known as the Design Basis Threat. Program Offices are required to use the Design Basis Threat as the baseline for planning security measures. Security requirements are also levied upon the Department by the Office of the President, Congress, and the General Services Administration. For example, Presidential Decision Directive 39 directed all Executive Branch agencies to protect against terrorist attacks. This resulted in an increased need for explosive detection equipment, more frequent security patrols, and hardening of structures. In some cases, Program Offices have directed their field elements not to implement departmental security requirements. This is due to 2 main reasons: The program offices can't afford the new directive, or they simply don't agree with it. In other cases, they have issued interpretive guidance that changes the security policy or undermines the effectiveness of that policy. Again, the Office of Safeguards and Security has no authority to demand compliance with departmental security policies and requirements.

ACCOMPLISHMENTS

I would be less than forthcoming if I failed to mention some positive aspects of the department's safeguards and security program. Let me start by saying that the program is staffed by hard working dedicated men and women throughout the country who are firmly committed to protecting the critical national security assets entrusted to their care. The responsibilities of these individuals are most demanding, even dangerous in some respects. Yet despite the dwindling resources made available to them, these individuals continue to perform in outstanding fashion. Where this department has failed is in providing these professionals the necessary resources to allow them to perform their responsibilities appropriately. The Department has also failed to provide protection so that individuals will bring forward problems and deficiencies without fearing retaliation.

Progress has been made in some of the areas I previously addressed. In the area of physical security, the Department is working to correct identified weaknesses. Specifically, the Department augmented security at some field sites by deploying new technologies to safeguard special nuclear materials and weapons; worked with other agencies to train departmental protective forces; identified and developed more sophisticated detection and deterrent systems; and hired additional security personnel. New explosive detection systems are being installed at selected nuclear facilities and some sites are upgrading access control systems.

In the area of information security, the Secretary recently directed the shut down of classified computer operations at three national laboratories until such time as he was assured that information processed on the systems is being done so securely. From a longer-term perspective, the department is requesting a dramatic increase in budget for information security. The additional funding will be used to help further secure the department's classified and unclassified computer networks. The improvements will help strengthen fire walls, develop better intrusion detection devices, and fund rapid response teams to work with the FBI to detect and track cyber intruders.

In the area of the control, measurement and accountability of special nuclear materials, the Department has established the Fissile Materials Assurance Working Group (FMAWG) to assess needed areas of improvement and make recommendations. In this regard, the FMAWG identified unmeasured materials and initiated actions to resolve discrepancies. They further identified issues regarding the safeguarding of irradiated material and are promulgating policy for implementation. The Department is developing new technologies for tamper indicating devices and proposing pilot projects for field implementation.

A PATH FORWARD

All of these positive steps are good, necessary actions to ensure the adequacy of our protection posture. More is needed, however. As previously addressed, organizational realignment of safeguards and security activities is sorely needed. I understand that this is now under review by the department. While addressing the problems inherent in the current organizational structure of the Department will not in itself solve all of the issues contained in this report, it will establish the necessary framework to allow resolution in a more effective and lasting manner. Simple organizational realignment, however, by itself, will not result in the fundamental change in approach that is required. The Department should work closely with Congress to establish a budget line item for safeguards and security. Doing so will enable a more accurate accounting and control of safeguards and security expenditures. It will also improve the likelihood that policy will be issued in conjunction with the necessary resources to implement that policy.

It should be apparent that attempts to have effective internal oversight of the DOE safeguards and security program have failed over a twenty-year period. While there have been high points and periods when oversight has been effective, organizational and budget pressures have played too central a theme for this function to remain within DOE. An organization like the Defense Nuclear Facilities Board should be established to independently review Security at DOE and the Laboratories. Further a direct reporting mechanism should be established to one or more of the Congressional Committees.

Perhaps the biggest challenge facing the department today as we strive to meet our protection responsibilities is the attitude throughout the complex toward security. There are some that believe

that safeguards and security is an overhead expense. I disagree, strongly. Safeguards & security is a mission-critical element. Without it, why bother creating new national defense technologies, if present or future foes can have ready access to it? To treat it as a mission-critical element requires a greater sense of accountability than seen to date. Secretary Richardson has committed to establishing and maintaining a sound safeguards and security program. It will take the commitment not only of the Secretary, however, but of each and every program official throughout the department if this mission essential element is to be fulfilled. It is incumbent upon senior departmental management to make safeguards and security a priority. It is too important to be relegated to a secondary status where its operations are viewed as ancillary. Both Congress and the public rightfully expect our best effort in executing this vital program. We should demand no less from ourselves.

--

--

Department of Energy,
Germantown, MD, January 27, 1997.

Memorandum for Distribution List

From: Edward J. McCallum, Director, Office of Safeguards and Security.

Subject: Status of Safeguards and Security.

This report provides a comprehensive review of Safeguards and Security activities throughout the Department of Energy complex during 1996 and provides a candid look at the future of the Program. The report is structured to present a Departmental perspective of the Safeguards and Security Program to senior management and all safeguards and security professionals. For the first time the report also contains a section which summarizes safeguards and security participation in National Nuclear Command and Control activities.

During the past year disturbing trends continued that resulted in additional budget reductions, further diminishing technical resources, reducing mission training and undermining our ability to protect nuclear weapons, special nuclear materials and other critical assets. This is occurring at a time of increased responsibilities resulting from the international transfer of nuclear materials and dismantling of U.S. nuclear weapons. Although traditional and time proven protection principles are still emphasized, it is becoming increasingly difficult to adequately protect our nation's nuclear stockpile in the face of inadequate resources, obsolescent systems, aging protection forces and funding uncertainties. This has increasingly resulted in a `hollow-force' that goes below the `bottom line' and makes it more difficult to fulfill National Security mandates. It is imperative that the Safeguards and Security downward resource spiral be immediately halted. Further, nuclear materials must be consolidated to reduce costs or additional resources must be found for protection. Adequate investment is essential to sustain a vital Safeguards and Security Program that continues to support the nation's security, the public health, safety and our environment.

I am confident that the report will be a valuable tool to stimulate open conversation, provide constructive feedback and assist in addressing the continued viability of the Department's Safeguards and Security Program. Collectively, we must continue to strive to maximize the use of our resources necessary to ensure requisite security for the Nation's and the Department's most vital assets.

Attachment.

Central Intelligence Agency,
Washington, DC, March 16, 1999.

Dr. Ernest Moniz,
Acting Deputy Secretary, Department of Energy, Washington, DC

Dear Dr. Moniz: As the Central Intelligence Agency's representative to the Department of Energy (DOE) Security Management Board, I would like to convey some important perspectives concerning on-going discussions to reorganize the Department's security element. Of concern is consideration that is being given to further decentralize DOE's security management apparatus and assignment of security expenses to indirect costs (i.e., overhead) at the individual sites and Laboratories. In my judgment, and based on our experience at CIA, DOE should undertake such reorganizational and budgetary alignments advisedly.

Using CIA's experience as an example, reorganization through division can be highly ineffective and inefficient. Shortcomings to CIA's 1994 decision to divide the Office of Security were quickly exposed, including: expensive duplication of security activities, deteriorated management focus over a tangential security program, elimination of a coherent security career service, and dilution of CIA's leadership role in the Community. Adding to the difficulties, security managers under this arrangement had limited control over their fiscal fate, having been placed alongside and beneath numerous budgetary layers.

Director Tenet recognized these inefficiencies immediately, and placed me in charge of consolidating CIA's program in 1997. In addition, he has provided security with a stronger voice in its fiscal future. The process to reconstitute our security apparatus has been challenging; but, its benefits have already become apparent through a stronger, more viable security program.

The lessons learned after CIA decentralized its security organization have also been experienced by other agencies, several of which have chosen to reconsolidate their activities. With such stark examples of the shortcomings of decentralization in security apparatuses, I urge you to give strong consideration to the implications of such reorganization of DOE.

Furthermore, in today's world of sophisticated technological threats, and given the developing review at one of the National Laboratories so widely publicized, I would further caution against leading the charge toward field autonomy, and anticipated the Department looking toward reinforcing centralized security expertise.

When appointed to the Security Management Board a year ago I expected that the Department wanted the input of the representatives from other Agencies in security issues of this nature. In fact, I believed that obtaining such outside counsel on issues of this nature was the purpose for which the Board was created. Unfortunately, my experience with the Board indicates that it is a feckless exercise with no accomplishments almost fifteen months after it was established. I would welcome the opportunity to further discuss my views with you at your convenience.

Sincerely,
RAYMOND A. MISLOCK, JR.

Associate Deputy Director
For Administration for Security.

--

--

From the Wall Street Journal, May 3, 1999

[FROM THE WALL STREET JOURNAL, MAY 3, 1999]

Congress Brings New Inquires Into Weapons Security Failures

(BY JOHN J. FIALKA)

Washington: House and Senate investigators are launching new inquires into the Energy Department's $800 million security program and how it failed to stop the apparent compromise of many of the nation's most valuable nuclear-weapons secrets.

Rep. John D. Dingell, the Michigan Democrat who led several of the House Commerce Committee's previous investigations in the 1980s and early 1990s, charged that the department runs a system of `inverse reward and punishment.' People who have identified lax security at the nation's defense labs have been punished and those who somehow finesse, ignore or abuse the program have been rewarded, he said.

The panel will hold hearings this week on the latest example of this seeming paradox: Edward McCallum, the Energy Department's top internal critic of security deficiencies, has been put on leave and is being investigated by the Federal Bureau of Investigations for allegedly leaking secret information. At the same time, Wen Ho Lee, the former Los Alamos nuclear-weapons scientists who allegedly transferred many of the nation's most sensitive nuclear-weapons codes to an unprotected computer between 1983 and 1995, is described by the FBI as being `unprosecutable.'

There is no evidence that China obtained any of the codes, although Mr. Lee met with China's weapons experts on two occasions during the 1980s and Chinese scientists were among the most frequent visitors to the lab.

The Commerce Committee has threatened to subpoena 13 Energy Department officials who know about the investigation of Mr. McCallum, a 25-year department veteran who, among other things, has complained about difficulties in trying to protect the secret computer system at Los Alamos. The network of 2,000 computers is used to store digital models of nuclear tests that show, moment-to-moment, how nuclear weapons work.

Committee members have invited Mr. McCallum to testify along with another department veteran, Glenn Podonsky, who runs internal inspections for the agency. While Republicans are leading the charge in the various congressional investigations, the two witnesses and others are expected to tell

of foul-ups and budget shortfalls that date to the Carter administration.

Energy Department reports show that Mr. Podonsky, as early as 1994, had identified the problem that researchers could transfer data from the secured computer system to the unprotected one.

Over the weekend, Department of Energy officials said that a classified report prepared by U.S. intelligence agencies in November showed that there had been numerous efforts to penetrate the weapons laboratories' unclassified computer system. The secret report also noted that China was among a number of nations the laboratories should regard as a threat. Still, investigators didn't examine Mr. Lee's computer until March and didn't close down the classified system until last month. The report's findings were first published in the New York Times.

Brooke Anderson, a spokeswoman for Energy Secretary Bill Richardson, said the secretary `is extremely concerned that the hearing may bring potential disclosures of classified information and his priority is to protect the national security.' Mr. Richardson, a former member of the Commerce Committee, irritated its leaders after a security hearing last week, accusing the panel of `exhuming the past.'

David Tripp, Mr. McCallum's lawyer, said the information involved in the allegations against Mr. McCallum wasn't classified and that he is being punished for being `a pain in the neck' about exposing security problems. Rose Gottemoeller, the assistant energy secretary who removed Mr. McCallum from his job, denied that was the reason, calling Mr. McCallum `a valued security professional' who has made `major improvements.'

Despite substantial spending on `gates, guards and guns,' one problem that had received relatively little scrutiny is the so-called insider threat. As the Cold War has faded, the threat has grown because many Americans now shun careers in engineering, physics and mathematics--skills in demand at the weapons labs. The shortage forced the labs to turn to foreign-born experts who had become naturalized U.S. citizens, such as Mr. Lee, Taiwanese whose skills included modeling nuclear-weapons explosions on supercomputers.


Home Page | About Curt | News | Projects | Constituent Services
Federal Links | 7th District | How to Contact Curt | It's an Outrage

Appendix PP:

"Nuclear Safety: Potential Security Weaknesses at Los Alamos and Other DOE Facilities,"
General Accounting Office Report #RCED-91-12

October 1990

United States General Accounting Office

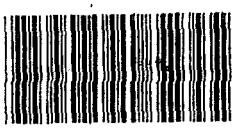
GAO

Report to Congressional Requesters

October 1990

NUCLEAR SAFETY

Potential Security Weaknesses at Los Alamos and Other DOE Facilities



GAO/RCED-91-12

GAO
United States
General Accounting Office
Washington, D.C. 20548

Resources, Community, and
Economic Development Division

B-240972

October 11, 1990

The Honorable John D. Dingell
Chairman, Subcommittee on Oversight
and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Pete V. Domenici
United States Senate

The Honorable Jeff Bingaman
United States Senate

At your request, we examined issues related to the adequacy of security at the Department of Energy's Los Alamos National Laboratory, New Mexico; the Department's security inspection process; and the feasibility of federalizing the Department's security forces. This report presents the results of our efforts.

Unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of this letter. At that time, we will send copies to the appropriate congressional committees; the Secretary of Energy; and the Director, Office of Management and Budget. We will also make copies available to others upon request.

This work was performed under the direction of Victor S. Rezendes, Director, Energy Issues, who can be reached at (202) 275-1441. Other major contributors are listed in appendix III.

J. Dexter Peach
Assistant Comptroller General

Executive Summary

Purpose

In March 1989 the contract security force at the Department of Energy's (DOE) Los Alamos National Laboratory began a 10-week strike, primarily because of quality of life issues. During the strike, DOE used temporary replacements from other facilities. Los Alamos carries out nuclear weapons research, development, design, and testing activities. Therefore, continuous, effective security is essential to protect nuclear materials, weapons, and information.

Concerned about the effect of the strike on site security, the Chairman, Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, and Senators Domenici and Bingaman asked GAO to evaluate (1) the adequacy of security at Los Alamos and other DOE facilities, (2) DOE's oversight of protective forces, and (3) the feasibility of establishing federal security forces at DOE facilities.

Background

DOE is responsible for the nation's nuclear weapons program and owns a broad spectrum of facilities to carry out research, development, and production activities. Contractors provide security services at all but one DOE facility—the Albuquerque Operations Office. For all facilities, DOE established 12 minimum skills that security force members must meet and the annual training they should receive. Periodically, DOE conducts inspections and/or performance tests to assess the effectiveness of the security forces. (See ch. 1.)

Results in Brief

GAO raises concerns about the adequacy of security at Los Alamos before, during, and after the strike. Before the strike, DOE could not demonstrate that the security force was properly trained to protect the facility because training records for some of the force were missing, incomplete, or inaccurate. During the strike, many replacements did not meet the 12 required skills. After the strike, an unannounced exercise showed that as late as April 1990 more than 75 percent of the regular force did not meet one or more of nine required skills.

GAO also raises concerns about security at some other DOE facilities that it reviewed. DOE inspections identified recurring and similar weaknesses; yet, DOE rated only one security program as unsatisfactory. GAO believes that this occurred because DOE lacks criteria specifying the severity and frequency of inspection findings that would result in a satisfactory or unsatisfactory rating. Also, DOE does not have an effective mechanism to ensure that corrective actions are taken on inspection findings. GAO

found that some inspection findings went uncorrected for as much as 5 years.

DOE believes that federal and contract security forces are equally capable of protecting its facilities, and the costs for both are similar. However, DOE does not have current cost data, and GAO estimates that annual labor and benefit costs could be about $15 million less if DOE federalized the security forces at the nine facilities GAO reviewed.

Principal Findings

Potential Security Weaknesses at Los Alamos

DOE and Los Alamos officials believe that security before, during, and since the 1989 strike was adequate. GAO was unable to verify this assertion but did find indications that potential security weaknesses exist. Before the strike, training records for some security force members were missing, undated, incomplete, or inaccurate. Therefore, DOE could not demonstrate that Los Alamos' force was properly trained to protect the facility.

During the strike, DOE waived physical fitness and medical requirements for about half of the replacement force, and many were not certified in 1 or more of 12 skills required of the regular Los Alamos force. These situations may not have occurred if DOE had established skill requirements for replacements and required contractors to develop contingency plans specifying the methods to be used to meet the requirements during a strike. Further, although a facility is most vulnerable during the early stages of a strike, DOE did not conduct an inspection at Los Alamos until 2 weeks, nor test the replacements' proficiencies until 6 weeks, after the strike began. Also, DOE never conducted a force-on-force simulated attack test over the strike's duration even though such a test is the best measure of a security force's overall ability to protect life and property. Therefore, DOE had little assurance that the replacements could adequately protect Los Alamos.

Since the strike, GAO found that most of the regular security force lacked one or more of nine skills that DOE officials say are needed to ensure the minimum level of protection for the site. Over 75 percent of the regular security force lacked such skills during an unannounced April 1990 exercise that DOE conducted at GAO's request. (See ch. 2.)

Other Facilities Have Security Program Weaknesses

DOE periodically inspects its facilities to assess the effectiveness of security policies, procedures, operations, and force proficiencies. DOE inspections of Los Alamos and eight other facilities since 1985 found some weaknesses that were similar and recurring. For example, DOE found that some security force members at Los Alamos, Argonne, Sandia, and Savannah River could not appropriately handcuff, search, or arrest intruders and shoot accurately. DOE also found weaknesses in the training programs related to those programs. Despite finding similar problems at the nine facilities, DOE rated only Argonne as unsatisfactory over the 5-year period. GAO believes that the differences occurred because DOE does not have criteria specifying the severity and frequency of inspection findings that would result in a satisfactory or unsatisfactory rating. In the highly important area of security at sensitive nuclear weapons facilities, DOE should be conservative and consistent—if one situation warrants an unsatisfactory rating, then other facilities with similar weaknesses should be similarly rated.

Also, DOE has no systematic method to track or confirm the corrective actions taken on inspection findings. GAO found that deficiencies identified as early as October 1985 at six facilities had not been corrected as of May 1990. DOE's allowing this situation to occur could send a message to contractors that security is not important and could perpetuate an environment in which contractors have little incentive to take corrective actions. DOE has a mechanism to improve this situation—the awards fee process. For contractors with repeat security inspection weaknesses, DOE could vary the amount of fees awarded depending upon the timing and effectiveness of corrective actions taken. (See ch. 3.)

Some Contract Forces May No Longer Be Cost-Effective

DOE believes that the abilities of, and costs for, a federal and contract force are similar, but a critical factor is the force's ability to provide uninterrupted service. A major advantage of a federal force is that it cannot legally strike, whereas a major disadvantage of a contract force is that generally it can strike. The Los Alamos strike cost about $1.6 million over and above the almost $17 million contract cost. According to a DOE Office of General Counsel official, no legal obstacles exist to DOE's negotiating a never-strike provision in its security force contracts but estimated that it would be costly to do so. Also, turnover may be lower with a federal force. During the 26 months before the strike, Los Alamos experienced between 11- and 15-percent turnover; the Albuquerque Operations Office federal force experienced no turnover. In contrast, a contract force, according to DOE and Los Alamos officials, can more quickly be reduced or increased to meet changing work demands.

Generally, the advantages and disadvantages of both types of forces offset each other, and the primary issue becomes cost. DOE conducted cost studies in the early 1980s for four facilities but has not updated the studies or conducted additional analyses to determine whether it is still cost-effective to have contract forces at all its facilities. DOE officials said they have not done so because privatization was emphasized throughout the 1980s, and they could not obtain positions for federal forces. Since that time, contract employee costs have increased faster than federal employee costs. GAO estimates that federal labor and benefit costs could be at least $15 million less each year than similar contract costs at 9 facilities, representing more than 60 percent of DOE's 5,500 security force members. (See ch. 4.)

Recommendations

To help ensure that security forces have the maximum capability to protect sensitive nuclear weapons facilities, GAO has made a number of recommendations to the Secretary of Energy to

- standardize skill requirements for all security force members including strike replacements,
- ensure that security force members receive all required training,
- withhold a portion of award fees when contractors do not take timely corrective actions on security inspection weaknesses, and
- evaluate the relative costs of federal and contract security services across the nuclear weapons complex and convert to federal forces at locations where it is cost-effective to do so.

Agency Comments

GAO discussed the facts presented in this report with DOE, Los Alamos, and the security force contractor. The officials generally agreed with the facts but offered some clarifications that were incorporated where appropriate. As requested, GAO did not ask DOE, Los Alamos, or the contractor to comment officially on this report.

Contents

Tables

Abbreviations

DOE	Department of Energy
GAO	General Accounting Office
OMB	Office of Management and Budget
OSE	Office of Security Evaluations
OSS	Office of Safeguards and Security
SSIIS	Safeguards and Security Issues Information System

Introduction

In March 1989 the security force at the Department of Energy's (DOE) Los Alamos National Laboratory, New Mexico, began a strike that lasted 10 weeks. Los Alamos conducts both unclassified and classified activities related to all phases of nuclear weapons research, development, design, and testing. Therefore, a security force possessing the necessary skills is the first line of human defense against terrorist or other attacks, theft or misuse of classified information and materials, and sabotage at sensitive nuclear facilities and is a key factor in DOE's physical security program. Security force members who cannot individually or as a team successfully perform all assigned tasks raises serious questions about the adequacy of security at these facilities.

To provide security force protection, the University of California, which operates Los Alamos for DOE, has contracted with Mason and Hanger-Silas Mason Company, Inc., since 1981. The company employs several hundred security inspectors, including officers and a rapid response team, who are authorized to detain, arrest, and use force if necessary to protect the facility. Security inspectors must meet minimum competency levels in 12 basic skills and be physically fit to perform their duties.

Causes of the Strike

Mason and Hanger has a labor agreement with the International Guards Union of America, Local 69. In February 1989 the labor agreement expired, and on March 13, 1989, the security force began a 10-week strike, which ended on May 21, 1989. During the strike, DOE used temporary replacements from its other sites as well as the Department of Defense facilities. DOE and Los Alamos officials told us that the causes of the strike included longstanding, unresolved labor-management relations problems—primarily Mason and Hanger's overtime, disciplinary, and sick leave policies.

According to Mason and Hanger officials, the overtime occurred because they never had enough job applicants with DOE security clearances to fill positions left vacant by security force members who resigned, retired, or were fired. Applicants, they said, became discouraged by the long wait for clearances (up to 18 months), and many were no longer interested in, or available for, employment by the time DOE granted their clearances. About one out of every four applicants were not available to accept job vacancies once the clearances had been received.

Some security inspectors told us that the overtime would have been more bearable, and the attrition rate lower, if Mason and Hanger had instituted fairer and more sympathetic policies. Fourteen security

inspectors said that the mandatory overtime was excessive and that the company's disciplinary policy was harsh. For example, some said that employees had been disciplined for frivolous reasons (eating while on duty). Similarly, according to some of these individuals, the sick leave policy was arbitrary, and in some cases, the company overruled doctors' opinions and forced employees to use vacation in lieu of sick leave. According to these individuals, these policies caused security force members to quit or be fired.

Actions Taken Since the Strike

To minimize future labor problems, a Mason and Hanger official said that in May 1989 the company changed its policies to require less mandatory overtime. At the same time, the company removed all demerits that most security inspectors had accrued and modified its sick leave policy by allowing security inspectors to charge sick leave starting with the first day of absence, provided they obtain a note from their doctor.

In addition, the company hired a human relations manager to serve as a liaison with the security force, and officials believe that labor relations have improved. According to a DOE industrial relations specialist, the agency suggested that Los Alamos use the Federal Mediation and Conciliation Service to facilitate meetings between Mason Hanger and the union. Los Alamos did so through December 31, 1989. As of May 1990, according to several security inspectors, Mason and Hanger was not always responsive to inspectors' grievances, and the possibility existed that a wildcat strike might occur because labor relations had deteriorated. The industrial relations specialist told us that a wildcat strike has never occurred at a DOE facility.

Organization for Overseeing Security

The Assistant Secretary for Defense Programs is responsible for directing the activities conducted by DOE's nuclear weapons facilities. Within Defense Programs, the Office of Safeguards and Security (OSS) establishes policies pertaining to the skills and qualifications that security force applicants must meet, the type and amount of annual training they should receive, and the content of plans for emergencies and other contingencies. Also, the Office of Security Evaluations (OSE) under the Assistant Secretary for Environment, Safety, and Health periodically assesses the effectiveness of DOE safeguards and security policies, procedures, systems, and operations. In making these assessments, OSE is required to periodically conduct performance tests: a simulated

attack on specific DOE targets (force-on-force) or a limited-scope assessment of, for example, a force's response to a simulated crisis, emergency, or unplanned events, such as activation of security alarms. The limited-scope test can either be announced or unannounced.

DOE headquarters has delegated responsibility for significant aspects of the security program to eight field offices called operations offices that oversee the facilities. DOE's Albuquerque Operations Office, New Mexico, oversees Los Alamos and eight other nuclear weapons laboratories and production facilities. To carry out its responsibilities, Albuquerque conducts various types of security surveys to ensure that the facilities maintain effective safeguards and security programs. In an unusual event, such as a strike, Albuquerque may also conduct special surveys or performance tests.

In turn, the operations offices have delegated certain oversight responsibilities to the contractors that operate the facilities. For example, the University of California is responsible for overseeing Mason and Hanger's operations to ensure that they comply with DOE's policies and procedures. Finally, Mason and Hanger establishes additional skill requirements for the Los Alamos security force, provides training, and tests to ensure that the force meets DOE's and its requirements.

Objectives, Scope, and Methodology

Concerned about the security implications of the strike, the Chairman, Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, and Senators Domenici and Bingaman, asked us in May 1989 to evaluate (1) the adequacy of security at Los Alamos and eight other DOE facilities,[1] (2) DOE's oversight of the protective security forces at the nine nuclear weapons facilities, and (3) the feasibility of federalizing DOE security forces currently under contract. In subsequent discussions with congressional staff, we agreed to concentrate on Los Alamos and gather information on the other eight sites from DOE headquarters and operations offices. We did not conduct work at the eight other sites. Further, we did not assess other aspects of DOE's physical security requirements, such as adequacy of fences, barriers, and alarms. Since we agreed to issue an unclassified report, some of the information cannot be presented in its entirety.

[1]Argonne National Laboratory, Illinois; Lawrence Livermore National Laboratory, California; Nevada Test Site, Nevada; Pantex, Texas; Rocky Flats, Colorado; Sandia National Laboratories, New Mexico; Savannah River Plant, South Carolina; and the Oak Ridge Y-12 plant, Tennessee.

To obtain an overall perspective on the three issues, we reviewed relevant provisions of the Atomic Energy Act of 1954, as amended, and DOE's security policies and procedures. Also, we met with the head of DOE's Safeguard and Security Task Force that was reviewing a broad range of safeguards and security issues at DOE facilities. A classified report of the task force's results is expected to be available during the fall of 1990. We also met with Nuclear Regulatory Commission staff about that agency's security program requirements.

Adequacy of Security

We met with DOE headquarters, Albuquerque Operations Office, Los Alamos, and Mason and Hanger security and procurement officials as well as 14 Los Alamos security force members about the causes of the strike; adequacy of security before, during, and after the strike; and adequacy of training. We judgmentally selected 11 security force members from Mason and Hanger's staff roster and invited others to meet with us. Three accepted the invitation, for a total of 14 (app. I contains the views expressed). The 11 individuals that we selected worked on the day, swing, and midnight shifts in all possible job categories and included union and nonunion members, females and males, and security inspectors and supervisors. Because of time constraints, we did not take a valid statistical sample; therefore, the results cannot be projected to all the Los Alamos security force.

In addition, we reviewed DOE's, Los Alamos', and Mason and Hanger's security force skill and qualification requirements and examined 1989 training records for about 330 regular security force members and the 391 strike replacements. To validate security force performance, we asked DOE to conduct a "no-notice" limited-scope performance test of the Los Alamos security force in 9 of 12 required basic skills—security operations, use of deadly force and limited arrest authority, communication procedures, firearms, tactics, physical conditioning, self-defense, nonlethal weapons, and site protection. The security force members were asked to shoot their handgun (firearms), demonstrate eight basic moves with a baton (nonlethal weapon similar to a billy club), run at least one-half mile (physical conditioning), and apprehend suspects demonstrating the six other required skills. We did not test the remaining three skills: vehicle safety, standards of conduct, and first aid/fire fighting.

For the test, we selected a statistical sample of security force members from those working the three primary shifts over a 24-hour period. Staff

from our Offices of Security and Special Investigations who are knowledgeable about apprehension, arrest, and baton procedures supplemented the audit team to observe and critique the tests. With the exception of the running exercise, the tests were conducted on April 3 and 4, 1990. Prior to a running test, DOE requires participants to receive a medical examination. To comply with this requirement, the running exercises were conducted on April 11 and 12, 1990. Our results can be projected with a 96-percent confidence level to the security force members from which the sample was taken.

We also reviewed contracts between DOE and the University of California, the University's subcontract with Mason and Hanger, and the company's agreement with the union. We limited our examination to provisions that pertain to the length of the contract, work stoppages, contingency requirements, oversight responsibilities, and termination.

DOE Oversight

To determine the actions that DOE takes to oversee the protection of its facilities, we reviewed the process used to inspect and rate facilities and the methods employed to ensure that the contractors take corrective actions on the deficiencies identified. In this regard, DOE headquarters and Albuquerque provided us with inspection reports for the period 1985-89 for the nine sites in our scope. We compared DOE's findings in these reports to identify trends or patterns, such as repeat deficiencies at a particular site. We also obtained DOE's contingency plan criteria, draft criteria that Albuquerque had developed, and six plans from contractors under Albuquerque's purview.[2] We compared the six plans with Albuquerque's draft criteria but did not evaluate the adequacy of the criteria. Using this and other information discussed above, we assessed DOE's internal controls for ensuring security at its facilities and work stoppage preparedness.

Federalization

To determine the advantages and disadvantages of federalizing the Los Alamos security force, we interviewed DOE headquarters, Albuquerque, Los Alamos, and the Office of Management and Budget (OMB) officials as well as Mason and Hanger security force members. We reviewed four cost analyses that DOE had prepared in the early 1980s. Also, we developed wage and benefit cost data for the nine facilities in our scope and a hypothetical federal force. We analyzed wages and benefits because (1)

[2]Pantex, Texas; Los Alamos, New Mexico; Pinellas, Florida; Kansas City plant, Missouri; Mound, Ohio; and Rocky Flats, Colorado.

they represented 60 to 76 percent of the costs in DOE's four analyses and (2) an OMB official said that labor costs normally represent about 85 to 90 percent of a contract guard force costs. The costs that we did not analyze included overtime and shift differential pay, operations overhead, general and administrative expenses, and contract administration that would normally be part of a full cost study. We also reviewed the Law Enforcement Pay Commission report. We determined that the Commission's findings were not applicable to the scope and nature of this review because the report addressed only specific law enforcement officers and jobs, such as the Federal Bureau of Investigation, and did not include federal security inspectors and guards.

We discussed the facts presented in this report with DOE, Albuquerque, Los Alamos, and Mason and Hanger officials. They generally agreed with the information but offered some clarifications, which we incorporated where appropriate. As requested, we did not ask these officials to comment officially on this report. Our work was conducted between July 1989 and May 1990 in accordance with generally accepted government auditing standards.

Concerns About the Adequacy of Security at Los Alamos

Although DOE and Los Alamos officials believe that security was adequate during the strike, we were unable to verify this assertion. However, we did find indications that potential weaknesses in overall security exist. During the strike, DOE did not conduct a force-on-force simulated attack to verify the replacement force's proficiencies. Also, 2 weeks elapsed before DOE conducted an inspection, and 6 weeks elapsed before DOE conducted a limited-scope test of the replacements' performance. In addition, DOE waived physical and medical requirements for almost 50 percent of the 391 replacements, and most were not certified in the minimum job skills required of the regular security force.

Throughout the 1980s, three strikes occurred at other DOE facilities; yet, neither DOE nor Los Alamos was prepared for the strike. For instance, DOE had not provided its contractors guidance on how to prepare for or deal with a strike. As a result, Los Alamos' contingency plan did not specify all the actions that should be taken during a strike. Los Alamos is not unique in this regard; we found similar weaknesses in the contingency plans of five other DOE facilities that we reviewed. As a result of the Los Alamos strike, in February 1990 DOE headquarters sent criteria to its operations offices and contractors to use for preparing strike contingency plans.

Aside from the strike situation, the regular Los Alamos security force may not be properly trained or proficient in protecting other employees, laboratory assets, or themselves. First, Mason and Hanger's training and certification records for 1989 were incomplete, inaccurate, or missing. Second, the results of the unannounced test that DOE conducted at our request in April 1990 showed that about 75 percent of the Los Alamos security force were not proficient in 1 or more of the 12 minimum required skills.

Was Security Adequate During the Strike?

DOE and Los Alamos officials contend that security was adequate during the strike. However, we identified several issues that raise questions about their position. For example, DOE did not conduct inspections during the early days of the strike, when the facility was the most vulnerable because not all replacements were on board and those that were on board were not familiar with their duties, weapons, or the uniqueness of the site and terrain. In addition, under its policies, DOE is required to periodically test security force performance, particularly when changes

occur in procedures, measures, or practices.[1] However, DOE did not test the proficiencies of the replacement force until 6 weeks after the strike began and then only on a limited basis and never conducted a force-on-force simulated attack—the best measure of a security force's overall ability to effectively protect life and property at a nuclear weapons facility. According to DOE officials, a force-on-force performance test would have been impractical during the strike because the extra staff needed to simulate an attack were not available.

The strike began on March 13, 1989, but 2 weeks passed before DOE conducted its first inspection to determine whether the replacements were competent and capable of protecting Los Alamos. DOE found no problems during the inspection, which involved visits to guard posts and interviewing personnel, but the inspection did not include performance tests of any of the 12 minimum security force skills.

Then, in mid-April 1989 (about 4 weeks into the strike), staff from the Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, notified DOE that they had received allegations of many instances of firearms "horseplay" by the replacement force. The following day, two Albuquerque officials conducted an inspection. Although they found no misuse of firearms, the officials did find that 12 of 30 replacements interviewed lacked proficiency with various weapons that they were required to use. In response, Mason and Hanger provided weapons training to the 12 individuals.

Even with this information, DOE did not conduct performance tests. Only in late April 1989, after another inquiry from the Subcommittee staff about the replacement force's training and competency, did DOE conduct a limited-scope test. DOE conducted the test at two sensitive areas at Los Alamos using three scenarios: entry with (1) a pipe bomb, (2) an incorrect badge, and (3) illegal drugs. DOE found that the replacement force responded correctly during the test.

Later, DOE conducted two additional inspections and identified some security problems, such as failure to find drug equipment during a simulated entry attempt, but the reports stated that security was adequate, at a high state of readiness, or satisfactory. Albuquerque officials told us that about 5 weeks into the strike they assigned a security official to

[1]DOE Order 5632.8, Protection Program Operations: Systems Performance Tests, Feb. 4, 1988, and DOE Order 5634.1A, Facility Approvals, Security Surveys, and Nuclear Materials Surveys, Feb. 3, 1988.

monitor, not test, the replacement force until May 16, 1990—1 week before the strike ended. The official's reports stated that no problems relating to excessive fatigue, incompetencies, or other security-related problems existed.

Many Replacements Did Not Meet Critical Skills

Many of the replacement force did not meet 1 or more of the 12 minimum skills required of the regular Los Alamos security force. This situation occurred because DOE's policies do not specify that temporary replacements should possess all such skills.

The several hundred replacements consisted of auxiliary and augmentee personnel. Mason and Hanger, the Department of Defense, and DOE's Pantex facility in Texas provided most of the auxiliary personnel. Auxiliary replacements normally work in scientific or engineering rather than security-related jobs and, in accordance with DOE's policies, fill security inspector positions on an "as-needed" basis upon request (usually in an emergency). On the other hand, the augmentees were full-time security inspectors from other DOE facilities, such as the Nevada Test Site, Savannah River plant, and the Oak Ridge Y-12 plant. As shown in table 2.1, many replacements were not certified in the minimum skills required of the regular Los Alamos force.

Table 2.1: Number of Replacement Force That Were Not Certified in Certain Skills

	Replacement force	
Skill	**Auxiliary[a]**	**Augmentees[a]**
Physical fitness	191	7
Arrest	38	35
Baton	191[b]	66
Weapons:		
Pistol (day)	7	7
Pistol (night)	190	8
Shotgun (day)	7	14
Shotgun (night)	190	15
Rifle (day)	7	9
Rifle (night)	190	20

[a]Some individuals lacked more than one skill.

[b]No auxiliary personnel were issued batons.

Also, 34 auxiliary personnel did not have the required medical certifications to show that they had the necessary mental, sensory, and motor

skills to perform their assigned duties safely and effectively. Albuquerque realized this about 2 weeks into the strike. Albuquerque also realized that none of the auxiliary personnel were certified in the physical fitness requirements of the regular force—run a 40-yard dash and at least a one-half mile distance run. DOE considers these requirements important because protective forces must perform normal and emergency duties without undue hazard to themselves, fellow employees, the site, or the public. Nevertheless, Albuquerque requested, and OSS granted, a waiver of the medical and physical fitness requirements for the auxiliary personnel.

In addition, DOE did not have qualification requirements for the auxiliary force even though sufficient time had elapsed since three prior strikes at other DOE nuclear weapons facilities.[2] Although the University of California required the replacement force to be qualified in weapons (pistol, shotgun, or rifle) needed to protect Los Alamos and capable of performing all Los Alamos protective force duties, some auxiliary personnel were not certified to use a pistol, shotgun, or rifle. Also, the auxiliary force were not trained on night use of weapons, even though some were assigned to the night shift during the strike. Finally, none of the auxiliaries were issued batons because they were not qualified to use them.

Although a scientist or engineer (auxiliary personnel) may not have all the required security force skills, the more perplexing issue is: Why would a regular security inspector from another DOE nuclear weapons facility (an augmentee) lack all the skills needed to protect Los Alamos? The simple answer, according to the Director, OSS, and other DOE officials is that each security force contractor establishes different competency requirements. For example, some contractors require proficiency in using a shotgun, rifle, or baton, while others do not. DOE officials also noted that each site is unique; therefore, if a contractor's security inspector augments another contractor's security force, the security inspector may not possess all the needed skills for a particular location. Also, the Director, OSS, told us that between 12 and 18 months are needed for new security staff to learn the tactics, geography, and targets at a particular facility.

Because of the lessons learned from the strike, DOE issued several memoranda concerning the use of replacements from other DOE sites. In January 1990 OSS issued a memorandum stating that allowing unqualified

[2]Oak Ridge in 1980, Pantex in 1981, and Oak Ridge in 1983.

individuals to use weapons raises questions about their ability to carry out routine and emergency duties and exposes DOE to unnecessary liability. A February 1990 memorandum stated that the Director, DOE's Central Training Academy, would collect and maintain a computerized data base of qualified security inspectors and special response team personnel throughout the DOE complex for use in extreme emergencies.

DOE Sites Were Not Prepared for Strikes

Neither DOE nor Los Alamos was prepared for the strike because DOE's policies pertaining to the content of plans for foreseeable contingencies do not require contractors to specifically address the actions that should be taken if a strike occurs.[3] We found that contingency plans prepared for Los Alamos and five other DOE nuclear weapons facilities varied in detail and coverage. For example, four plans identified posts that could be shut down, curtailed, and/or consolidated while two did not.

Following the strike, both DOE headquarters and Albuquerque initiated actions to improve contingency planning for strikes. In June 1989 Albuquerque asked seven facilities, including Los Alamos, to submit their plans for review.[4] Albuquerque wanted to determine whether the contractors could effectively deal with emergencies, especially security force strikes. Six contractors submitted their plans; the seventh (Sandia) did not have a plan because contractor officials believed that productive bargaining would prevent a strike.

On the basis of its review of the plans and lessons learned from the strike, Albuquerque's Security and Nuclear Safeguards Division drafted contingency plan criteria that included 18 elements. Our comparison of the six plans with Albuquerque's draft criteria showed that none met even 50 percent of the criteria (app. II shows our comparison of the six facilities compliance with Albuquerque's draft contingency plan criteria).

In August 1989 OSS sent a memorandum to the operations offices that included minimal contingency plan criteria. For example, the memorandum stated that the plans should identify those security functions that could be performed by other staff. The memorandum also requested each facility contractor to submit its contingency plan to OSS.

[3]DOE Order 5632.7, Protective Forces, Feb. 9, 1988.

[4]Los Alamos, New Mexico; Kansas City, Missouri; Mound, Ohio; Pantex, Texas; Pinellas, Florida; Rocky Flats, Colorado; and Sandia, New Mexico.

None did so, and the office did not follow up on its request to get the plans submitted.

In February 1990 OSS sent another memorandum to the operations offices requesting them to submit a summary of their facility contractors' contingency plans by May 1990. The memorandum also instructed each operations office to incorporate a contingency plan section in its future Master Safeguards and Security Agreement.[5] According to an OSS official, the memorandum reminded the operations offices that contingency plans were now required for strikes and was intended to serve as guidance, rather than requirements, on preparing the plans. We noted that the memorandum identified only 4 of the 18 elements in Albuquerque's draft contingency plan criteria. Albuquerque officials told us that they required contractors under their purview to revise their plans by April 1990 in accordance with the memorandum. All did so. Because Albuquerque received these plans near the end of our work, we could not assess the information provided.

Security Force May Not Have Been Properly Trained

We found that many training and certification documents for the security force before the strike were missing, incomplete, undated, changed, or unsigned. Without accurate and complete documentation, neither Mason and Hanger nor DOE can demonstrate that the regular Los Alamos security force is properly trained to protect the facility.

DOE's policies specify the training and physical requirements that a security force must meet and require contractors to maintain records showing that they have complied with the policies.[6] Although Mason and Hanger officials told us that they retain training records indefinitely, we found the opposite—records for training provided in 1989 to about 330 security inspectors were missing or had such deficiencies as being incomplete, inaccurate, unsigned, or undated. Table 2.2 shows our findings for arrest, baton, and physical fitness.

[5]An agreement between the Assistant Secretary for Defense Programs and an operations office concerning the types of security measures to be taken, risks to be considered, and ways to increase security effectiveness.

[6]DOE Order 5632.7, Protective Forces, Feb. 9, 1988.

Table 2.2: Incomplete, Missing, or Deficient Training Records

Skill	Number of employees	Number of records available	Number of records missing	Number with deficiencies
Arrest	333	244	89	121
Baton	333	306	27	[a]
Physical Fitness	333	312	21	0

[a]Although all records indicated a perfect score, we verified 21 randomly selected records and found that only 5 were signed, dated, and completely filled out. Further, 50 percent of the security inspectors that we interviewed said they needed additional training in this area.

Concerning weapons proficiencies, we cross-checked 14 randomly selected source documents to Mason and Hanger's computerized information and found one missing record. The remainder had no data entry errors. However, we noted three problems with the source documents: (1) the range master (firearms instructor) certified his own qualification record, (2) some records had been altered by erasures or correction fluid, and (3) all entries were in pencil instead of ink. In addition, security inspectors must be medically fit to perform their assigned duties. We found that Mason and Hanger's computerized medical records were not up to date, and 47 of 333 inspectors (about 14 percent) had missed part of their annual medical examination.

According to Mason and Hanger officials, the documentation problems occurred because they did not have sufficient resources (staff and funds) to properly maintain the documents. To correct these problems, Mason and Hanger officials said that the company (1) has sent three employees to recordkeeping classes, (2) is obtaining new computer hardware to provide greater recordkeeping capability, (3) is updating training records, and (4) is identifying and scheduling training for some of the security force. Mason and Hanger officials said they took these actions not only because of our findings but also because they were concerned that security inspectors might bring injury suits or otherwise hold the company liable for failing to train them as happened in a recent city government case.[7] In such a situation, accurate and timely training documentation would be vital. A company official also said that, if employees won the suit, the costs would be passed on to the government because their subcontract with the University of California is cost reimbursable as is the University's contract with DOE.

According to the Director, OSS, DOE recognizes that these problems exist not only at Los Alamos but throughout the nuclear weapons complex. As

[7]City of Canton, Ohio, vs. Geraldine Harris, et. al., 489 US 378 (1989).

a result, DOE will require the Central Training Academy to assess the status and quality of training provided to all security forces. DOE also plans to ask the Central Training Academy to develop a standardized course for force members and certify the qualifications of those individuals who will provide the training.

Los Alamos' Security Force Did Not Perform Well During a Surprise Test

According to some DOE officials and Nuclear Regulatory Commission staff, a no-notice test is the best way to assess a security force's ability at any given time. DOE's policies allow for such tests, but DOE has not conducted unannounced tests in the past because, according to officials, they raise safety concerns, are difficult to plan, disrupt the work force, and create stress for all participants. Because of the training record problems that we found, DOE in April 1990 conducted an unannounced test at our request of the regular Los Alamos security force in 9 of 12 skills, including weapons, baton, running, and arrest or defense tactics. According to the Director, OSS, these skills are similar to those required of a police officer and are applicable to the majority of DOE's security force members. Table 2.3 shows the number of security force members that participated in the tests and those that did not meet the skill requirements.

Table 2.3: Results of an Unannounced Test

Skills[a]	Number tested	Number passed	Failed	
			Number	Percent
Weapons	54	52	2	4
Baton	54	51	3	6
Running	50[b]	50	0	0
Apprehension	54	15	39	72
Test summary	54	12	42[c]	78

[a]The apprehension test combines six skills: force and arrest, security operations, communications, tactics, self-defense, and site protection.

[b]Three participants were not medically fit to run, and one was on sick leave the day of the test.

[c]The total does not add because some participants failed more than one test.

Although the security force had a basic understanding of selected skills and generally met the handgun, baton, and running requirements, only 12 (22 percent) of the 54 force members tested passed all 9 skills. The remaining 78 percent lacked one or more of the skills needed to arrest, apprehend, communicate, and survive in an adversarial situation; protect laboratory resources or staff; or defend themselves. For example, when the participants encountered an adversarial situation, many failed

to stay behind cover and assess the situation. Instead, they left their cover and walked up to the potential adversary to ask what they were doing. As a result, in many instances the adversary took a visible weapon, "killed" the participant or hostage, and left with the classified documents or government property. In total, 24 participants and hostages were "killed" during this testing.

If we project the test results to the 191 security force members sampled, 149 would lack one or more of the above skills. As discussed in chapter 3, security force performance weaknesses have been a longstanding problem at Los Alamos. DOE inspections conducted in 1986 and 1988 identified problems similar to those found in our unannounced test.

Conclusions

A security force must be able to protect DOE's sensitive nuclear weapons facilities from such threats as terrorist attacks, unauthorized entry, and theft of classified documents. To minimize the potential for a security breach, the security force must meet certain employment qualifications and continually maintain its skills. When a security force—the first line of human defense—cannot perform its duties, is ineffective, or improperly trained, little assurance exists that sensitive facilities are appropriately safeguarded. Yet, this is the situation that we found at Los Alamos before, during, and since the 1989 strike.

First, the available evidence does not show that either the regular or replacement force was properly trained to protect Los Alamos. Training and proficiency records for the regular security force were missing, incomplete, or inaccurate. Second, many of the strike replacements did not meet all the skills required of the regular force. Finally, the results of our unannounced exercise showed that about 75 percent of the security force—as late as April 1990—did not have all the skills needed to protect the facility or defend themselves.

Also, about 50 percent of the replacements used during the strike normally worked in jobs other than protective services, and DOE waived some requirements for these replacements, thereby increasing the vulnerability of the site. Also, DOE did not test the proficiencies of the replacements until 6 weeks after the strike began—and then only on a limited basis—and never conducted a simulated, force-on-force, adversarial test over its duration. Instead, DOE relied on limited security inspections and the on-site observations of an Albuquerque official to ensure that Los Alamos was appropriately protected.

We believe that these situations occurred because neither DOE nor Los Alamos was prepared for the strike. DOE had no skill requirements for a temporary replacement force and did not require its contractors to develop contingency plans for strikes. Although three other strikes had occurred at DOE facilities throughout the 1980s, DOE did not take such threats serious enough and require all contractors to appropriately plan for work stoppages that could pose a security risk. In a February 1990 memorandum, DOE attempted to correct this oversight. The memorandum, however, provided only limited specifics on the plans contents, thereby increasing the potential that contractors will not address significant issues for dealing with strikes.

Recommendations to the Secretary of Energy

To continuously and completely protect sensitive and valuable documents, personnel, and government property, DOE needs trained and proficient security forces at its facilities. Therefore, we recommend that the Secretary of Energy

- expeditiously develop specific contingency plan criteria for strikes and require all contractors to prepare plans that meet the criteria;
- establish standardized qualification and skill requirements for all protective forces and ensure that strike replacements meet the requirements;
- ensure that security force members receive all required training and institute a mechanism to ensure that contractors document and retain this information; and
- conduct unannounced inspections and performance tests, particularly immediately upon the initiation of an unusual event, such as a strike, to obtain more realistic indications of security force competencies.

DOE's Security Inspection Process Can Be Improved

Weaknesses exist in DOE's security inspection and evaluation process. DOE lacks specific criteria for the types of deficiencies that would result in either a satisfactory or unsatisfactory rating for a facility's security force. As a result, DOE inspections between 1985 and 1989 identified similar and recurring problems at Los Alamos and eight other facilities, yet DOE rated six facilities satisfactory, two marginally satisfactory, and only the Argonne National Laboratory as unsatisfactory. Despite these longstanding inconsistencies, DOE has not developed specific rating criteria or performance incentives for security force contractors to minimize poor performance.

Further, DOE does not have appropriate controls to ensure that contractors take corrective actions on security program weaknesses identified during inspections. We found that some deficiencies went uncorrected for as much as 5 years even though DOE's computerized system showed that contractors' had taken corrective actions. This situation may not have occurred if DOE had confirmed that contractors took the needed actions. In April 1990, Albuquerque took steps to ensure that corrective actions had actually been taken on inspection findings.

DOE Lacks Specific Criteria for Rating Facilities

DOE's policies do not specify the severity and frequency of inspection findings that would result in a satisfactory, marginal, or unsatisfactory performance rating. Therefore, inspection ratings can vary even though the results are similar and recurring. Further, DOE's reports did not indicate that the uniqueness of a site would cause variances in the inspection ratings assigned. Between 1985 and 1989, DOE inspections found some similar and recurring weaknesses at nine facilities including Los Alamos but only one received an unsatisfactory rating. Under DOE's policies, OSE, OSS, and operations offices, such as Albuquerque, are required to periodically inspect the security activities conducted by the contractors that operate nuclear weapons facilities.[1] On the basis of the inspection results, both headquarters and the operations offices assign a rating of satisfactory, marginal, or unsatisfactory to the contractor's program.

Within headquarters, OSS and OSE are responsible for periodically inspecting the weapons facilities. According to an OSE official, the inspection team provides an unrated draft of its findings to the operations offices for comments and then the report and the team's proposed

[1]DOE Orders 5630.12, Safeguards and Security Inspection and Evaluation Program, Feb. 3, 1988; 5634.1A, Facility Approvals, Security Surveys, and Nuclear Materials Surveys, Feb. 3, 1988; and 5632.8 Protective Program Operations: System Performance Tests, Feb. 4, 1988.

rating are reviewed by inspection branch chiefs and division director and OSE's Director. These individuals either concur with the suggested rating or, with the team leader, adjust the rating, considering technical, management, and other issues, such as the contractor's performance in each topical area reviewed.

According to an official, OSE does not have clear-cut criteria specifying the values assigned to deficiencies that result in a facility being rated satisfactory or unsatisfactory. The official also noted that, although OSE strives for objectivity by involving more than one individual in the process and examining a number of parameters, the ratings will always be highly subjective. Also, an Albuquerque official, involved with inspections at OSE and the operations office, confirmed that no criteria exist for inspectors to consider the severity of findings when making rating recommendations.

Thus, we found that DOE assigned satisfactory ratings to facilities even though the inspection reports identified numerous deficiencies. Between 1985 and 1989, DOE identified similar and recurring inspection problems at nine facilities but rated six as satisfactory, two as marginally satisfactory, and one—Argonne National Laboratory—as unsatisfactory. Table 3.1 shows the types of findings at the nine facilities.

Table 3.1: Security Force Weaknesses Cited in DOE Inspection Reports, 1985-89

Type of finding	Number of inspections[a]								
	A	B	C	D	E	F	G	H	I[b]
Not skilled on metal detector							1		
Cannot find concealed weapon	1								
Cannot find drug equipment	1								
Unfamiliar with weapons	2						1		
Command/control weaknesses	1	1		1			1		
Handcuff/search/arrest weaknesses	3	3	1		3		1	1	
Cannot appropriately apprehend suspects	1	2						1	
Failed to keep weapon from adversary	1								
Failed to search following handcuffing	1								
Not skilled in M16	1								
Unfamiliar with night vision devices	1								
Radio/communication weaknesses	1	2			3		1		
Patrol not reporting security condition	1								
Failed to control security situation	1								
Undocumented performance tests	1	1		1			1		
Lacked firearm skills	2	1		1	1		1	1	
No firearms training		1							
First aid program deficiencies		1							
Training program deficiencies	2	2	1	2	1			1	1
Security inspector missing from post					1				
Past-due medical examinations	1								
Hostile aircraft training weaknesses	1								
Patrols not conducted to procedures					1				
Lacked theft/diversion requirements					1				
Failed to assign weapons to post					1				
Supervisors lack knowledge					1				
Lack emergency warning signal knowledge							1		
Poor weapons inventory/maintenance	1			1		1			

[a]Number of inspections that identify the finding noted.

[b]A = Los Alamos National Laboratory, New Mexico.
B = Argonne National Laboratory, Illinois.
C = Rocky Flats, Colorado.
D = Oak Ridge Y-12, Tennessee.
E = Savannah River, South Carolina.
F = Lawrence Livermore National Laboratory, California.
G = Nevada Test Site, Nevada.
H = Sandia National Laboratories, New Mexico.
I = Pantex, Texas.

As shown in table 3.1, DOE found that the security forces at Argonne (three inspections), Savannah River (three inspections), Sandia (one inspection), and Los Alamos (three inspections) could not appropriately

handcuff, search, or arrest intruders and lacked weapons skills and accuracy. DOE also found weaknesses in the training programs at the four facilities. Despite finding similar problems, DOE only rated the security program at Argonne as unsatisfactory. Because DOE lacks criteria concerning the extent to which severity is considered in rating a security force program, we could not determine—and DOE officials could not effectively explain—the rationale for assigning different ratings. According to the Director, OSS, training and headquarters oversight are more important than developing severity criteria. He said that DOE has attempted to develop severity models to overcome dissimilarities with ratings, but the attempts had not been successful. However, during the spring of 1990, DOE reorganized OSS to help improve rating consistency by, in part, increasing the training provided to inspection teams.

DOE Does Not Have an Effective System to Track Corrective Actions Taken

DOE does not have an effective system to monitor and follow up on actions taken as a result of its inspection findings. As a result, we found that security force performance weaknesses identified as much as 5 years ago had not been corrected as of May 1990. For example, in 1986 OSE found that the Los Alamos security force could not effectively detain and/or arrest intruders. In 1988, an Albuquerque inspection identified the same deficiencies. The University of California reported to Albuquerque that corrective actions had been taken to resolve these problems. We found that these problems still existed as of April 1990.

According to OSS officials, they developed a classified computerized information system, the Safeguards and Security Issues Information System (SSIIS), in June 1985 to help monitor inspection weaknesses found at all facilities and ensure that corrective actions were taken. In 1989 DOE found that the SSIIS data were not reliable or complete and took actions to update and correct the data. As of February 1990, the system contained information on DOE headquarters inspection findings from November 1988 and operations offices' findings from January 1989.

OSS officials say that SSIIS was used primarily to monitor the status of corrective actions and ensure that headquarters received complete, timely, and reliable data on operations offices' findings. An auxiliary benefit was to encourage operations offices to develop data bases to monitor inspection findings and corrective actions taken by the contractors under their jurisdiction. According to Albuquerque security officials, they do not use SSIIS because the data are not complete or reliable, and their staff could not access the data directly from their computers. To correct these situations, OSS officials told us that they are developing

a new data base to replace SSIIS. The officials estimated that the system would be available to the operations offices after about a year.

In the interim, Albuquerque uses three data bases to track inspection findings and corrective actions taken. One provides a facility-specific summary of the number of findings, those requiring corrective actions, and their status. The second data base provides more detailed information on inspection findings and the status of corrective actions. According to an Albuquerque official, the office strives to keep the information current, but some backlogs have occurred because staff were not available to input the data. Albuquerque has also developed a data base to track OSE's inspection findings for contractors under its purview.

Despite having three systems to track their own and DOE headquarters inspection results, as late as March 1990, Albuquerque did not know the status of corrective actions taken on inspection weaknesses identified as early as 5 years ago. According to an official who tracks this data, Albuquerque did not have up-to-date information on DOE headquarters findings until 1989. The official subsequently found that six contractors under Albuquerque's jurisdiction had not corrected security program deficiencies identified as early as 1985.

As a result, Albuquerque plans to more closely monitor the contractors' activities. In April 1990 Albuquerque sent a memorandum to its area offices requiring officials to validate corrective actions taken as a result of internal—DOE headquarters and Office of Inspector General—and external—General Accounting Office—reviews and/or inspections. The area offices must certify in writing that the actions have been taken; Albuquerque security personnel will take a sample during subsequent inspections to validate the area offices' certification.

Other Options to Ensure Corrective Actions

Under DOE's policies, the operations offices are responsible for ensuring that contractors institute effective programs to protect and secure nuclear weapons facilities; the operations offices can curtail or suspend facility operations if an immediate and unacceptable national security or public health and safety risk exists.[2] Also, DOE's contracts with the University of California and others that operate nuclear weapons facilities

[2]DOE Order 5630.11, Safeguards & Security Program, January 22, 1988.

state that DOE can terminate a contract when DOE determines that termination is in the best interest of the government, such as for unsatisfactory performance.

Between 1985 and 1989 DOE had identified numerous weaknesses in contractors' security programs. Also, in three evaluations (one in 1986 and two in 1989), DOE had identified numerous, repeat security program deficiencies at Argonne that eventually resulted in one marginally satisfactory and two unsatisfactory ratings. In 1989 DOE curtailed the operations at Argonne until corrective actions could be taken and replaced the contractor in June 1990. According to officials, DOE prefers to work with contractors to correct security force weaknesses rather than terminate a contract for poor performance.

However, DOE has another mechanism that it could use to encourage contractors to take timely and effective corrective actions on security inspection deficiencies—the awards fee process. DOE uses award fees, over and above reimbursing normal costs, to encourage effective contractor performance. We noted that in fiscal years 1987 and 1988 DOE had delineated security—including protective forces and systems—as a functional area for the award fee determination at Pantex and the Oak Ridge Y-12 plant but not at Rocky Flats. However, the weight—or importance given to security—varied between the facilities. At Oak Ridge, DOE consistently considered security as 10 percent of the total fee; at Pantex, the weight ranged from 10 to 20 percent.

In November 1989 DOE published in the Federal Register a final rule for withholding award fees if a contractor fails in one major functional area. For facilities with repeat security inspection deficiencies, DOE could include a functional area in the award fees process to specifically measure contractor performance, including the timing, and effectiveness of, corrective actions taken for inspection findings.

Conclusions

The security at other DOE facilities may be as questionable as the situation that we found at Los Alamos. DOE inspections at other facilities since 1985 have identified recurring and similar security force weaknesses that seem to justify a less than satisfactory rating. Yet, in only one instance—Argonne—did DOE determine that the security program was unsatisfactory. We believe that in the highly important areas of security and adequacy of protective services at facilities involved in the research, development, or production of nuclear weapons, DOE should take a conservative approach and should not allow security weaknesses

to persist. If DOE finds the same problems at more than one facility, then DOE should similarly assess the level of security. If one situation warrants an unsatisfactory rating, it seems reasonable that other facilities would be similarly rated.

Also, DOE's actions can send a message to contractors that security is not important and perpetuates an environment in which corrective actions are not taken on the problems identified. In this regard, DOE does not have an effective mechanism to ensure that actions are taken to correct inspection weaknesses. The ineffectiveness of DOE's process is best illustrated by the fact that inspections of the nine facilities over 5 years identified some of the same problems; therefore, many deficiencies did not get corrected. If DOE used the award fee or some other mechanism to affect the contractors' profits or instituted other punitive measures, such as terminating security force contracts for poor performance, the contractors may pay greater attention to quickly and effectively correcting weaknesses identified in security inspections.

Recommendations to the Secretary of Energy

To ensure consistency among inspection ratings and provide an incentive for security forces' contractors to correct inspection deficiencies, we recommend that the Secretary of Energy

- develop specific criteria to eliminate any inconsistency for rating facility's security as either satisfactory, marginal, or unsatisfactory and
- withhold a portion of award fees when contractors do not take timely corrective actions on security inspection weaknesses.

Some Contract Forces May No Longer Be Cost-Effective

We estimate that federal labor and benefit costs would be at least $15 million less each year than similar contract costs at the nine DOE facilities we reviewed. Nearly all 5,500 security personnel that protect DOE's nuclear weapons facilities are contractor employees. In the early 1980s, DOE assessed the costs of contracting for security functions at four facilities and found that contract costs were less than federal costs. DOE has not updated the analyses or conducted additional ones to determine whether contract costs are still less than federal costs.

According to DOE officials, both contract and federal forces are equally capable of protecting sensitive nuclear facilities, but a critical factor is the force's ability to provide uninterrupted service. A major advantage of a federal force is that it cannot legally strike, whereas a major disadvantage of a contract force is that it generally can. The Los Alamos strike cost about $1.6 million over and above the almost $17 million contract cost. According to a DOE Office of General Counsel official, no legal obstacles exist to DOE's negotiating a never-strike provision in its security force contracts but estimated that it would be costly to do so. Also, turnover may be lower with a federal force. During the 26 months before the strike, Los Alamos experienced between 11- and 15-percent turnover; the Albuquerque Operations Office federal force experienced no turnover. In contrast, a contract force, according to DOE and Los Alamos officials, can more quickly be reduced or increased to meet changing work demands. Although both types of security forces offer advantages and disadvantages, they generally offset each other, and the primary issue becomes cost.

DOE believes that federalizing security force services may be more acceptable today than under previous administrations, which emphasized privatization of such activities. Also, OMB officials told us that they would work with DOE to prevent a recurrence of past budgetary problems that hindered the hiring of federal employees for security force positions.

Federal Security Force May Be More Cost-Effective at Some Locations

For nine DOE facilities we reviewed, we found that DOE could save about $15 million annually in labor and benefit costs by converting to federal forces.[1] We estimated that contract labor and benefit costs ranged from 5 to 38 percent higher than similar federal costs at the facilities. Table 4.1 shows the contract and federal security force costs at the nine facilities.

Table 4.1: Contract Versus Federal Labor and Benefit Costs at Nine DOE Facilities[a]

	Security force costs		Difference	
Facility	**Contract**	**Federal**	**Dollars**	**Percent**
Argonne	$1,538,950	$1,336,500	$202,450	15
Lawrence Livermore	7,559,378	5,986,156	1,573,222	26
Los Alamos	11,782,093	9,556,950	2,225,143	23
Nevada Test Site	13,547,681	10,154,262	3,393,419	33
Oak Ridge (Y-12)	16,588,826	14,760,534	1,828,292	12
Pantex	10,933,211	10,040,871	892,340	9
Rocky Flats	9,867,181	7,146,206	2,720,975	38
Sandia	5,495,996	4,585,083	910,913	20
Savannah River	19,983,746	18,951,143	1,032,603	5
Total	**$97,297,062**	**$82,517,705**	**$14,779,357**	

[a]Total number of employees at the nine facilities was over 3,000; total contract security force costs were $193.1 million.

However, the estimated annual savings shown in table 4.1 could be even higher. First, we did not include overtime costs in this comparison. Contractor salaries are more than federal salaries; therefore, overtime, which is calculated as a multiple of base pay, would be higher for a contract than federal force. Second, the estimated federal salaries were developed using the salaries of DOE's federal nuclear materials courier force.[2] The courier force salaries would be higher than federal security inspector's because the couriers have higher skill and training requirements. For these reasons, our estimated annual labor and benefit savings of about $15 million may be conservative.

Also, DOE's Inspector General Office is currently evaluating the cost-effectiveness of selected support service contracts. According to Inspector General officials, their analyses will include all costs and their

[1]The nine facilities represented more than 60 percent of DOE's 5,500 total security force members for 1989.

[2]DOE has three federal courier forces. They are comparable to the Los Alamos security force because both are responsible for protecting sensitive material. However, specific emergency reactions are different because the security force protects a fixed site while the courier force protects nuclear material transported by truck between DOE facilities.

tentative findings indicate that significant cost savings could result from federalizing the services performed by these contractors.

DOE Has Not Updated Its Cost Comparisons

DOE officials believe that the costs for a contract or federal force would be similar. However, DOE has not updated four cost comparisons prepared in the early 1980s nor has it conducted additional analyses. On the basis of the earlier analyses, DOE converted three federal forces to contract forces (including Los Alamos); the Albuquerque Operations Office force remained as the only federal force. The 1980 Los Alamos study concluded that DOE could save about $2 million over a 3-year period by replacing the federal force with a contract force.

In addition, a 1981 DOE cost study for Oak Ridge showed that the agency could save $274,000 over a 3-year period by replacing the federal force with a contractor force. In 1982, we found that DOE's study was deficient and concluded that DOE's converting the Oak Ridge force may increase government costs by as much as $1.2 million over the 3-year period.[3] At that time, we recommended that the Secretary of Energy reassess the decision to contract for the Oak Ridge guard services. DOE did not terminate the contract. The cost results presented in table 4.1 show that the Oak Ridge contractor's 1989 wage and benefit costs exceeded federal force costs by more than $1.8 million.

According to DOE officials, they have not updated or conducted additional cost comparisons because (1) the prior administration emphasized privatization throughout the 1980s, (2) the government's policy is to contract for security forces unless some "overwhelming" reason precludes doing so, and (3) DOE could not obtain OMB's approval for the number of federal positions needed. An OMB official told us that agencies should periodically conduct a cost analysis if the difference in contract and federal labor and benefits costs are close to, or exceed, 20 percent. According to OMB officials, a difference of less than 20 percent would likely be obliterated through (1) a process that allows contractors to resubmit lower bids and (2) the 10-percent conversion penalty for unforeseen costs that federal agencies must add to their estimated in-house costs.

For five of the nine facilities shown in table 4.1, the estimated costs of a contract force were at least 20 percent higher than a federal force; four

[3]Contracting of Guard Services At Oak Ridge Will Spiral Costs (GAO/PLRD-82-71, Apr. 30, 1982).

were less than 20 percent. Yet, DOE has not reanalyzed the cost differences between contract and federal forces since the early 1980s. According to the Chief, Management Systems Development/Evaluation Branch, DOE has not done so because the operations offices have more pressing problems, such as the billions of dollars of environmental cleanup, and do not have the staff to initiate multiple cost comparison studies.

Some Aspects of Contract and Federal Security Forces Offset Each Other

According to DOE officials and others with whom we met, either contract or federal security forces can protect DOE facilities. According to a 1976 Nuclear Regulatory Commission report, neither option offers an overall advantage over the other; therefore, the deciding issue is cost. One of the major disadvantages of a contract force is that it can strike, which generates security concerns and increases costs. The Los Alamos strike cost about $1.6 million over and above the almost $17 million fiscal year 1989 contract cost. On the other hand, a federal force would eliminate contract administration costs, which vary according to the force size.

Although several strike prevention mechanisms exist, they also carry a price tag. For example, a never-strike provision that extends beyond the contract expiration date and through renewal negotiations would provide DOE a mechanism to eliminate work stoppages. According to an Albuquerque Office of General Counsel official, no legal obstacles exist to DOE's negotiating a never-strike provision in its security force contracts, but the official believed that such a provision would be costly and estimated that the union might require a 25-percent increase in wages before agreeing not to strike.

A number of other differences exist between federal and contract forces. For example:

- Federal protective forces may experience less turnover. During the 26 months before the strike, Mason and Hanger experienced turnover rates of between 11 and 15 percent. Albuquerque's federal guard force experienced no turnover during the same period. Also, DOE's nuclear materials couriers experienced turnover rates as low as 8 and 10 percent during 1987 and 1988 even though the employees worked more overtime (about 75 percent) than the Los Alamos force (about 40 percent).
- A contract force can more rapidly respond to changes in workload demands. According to officials, one reason that DOE contracted for security services at Los Alamos was that OMB did not authorize additional personnel as security demands increased. Although the federal

personnel register included individuals wanting to be on the Los Alamos security force, DOE could not get additional positions approved in the early 1980s.

- A contract force can more easily terminate an employee who does not meet the required qualifications and skills. A member of DOE's security task force study said that a federal force has built-in protection and terminating an employee is a slow and cumbersome process.

Although costs and turnover rates may be lower for a federal force, DOE has never converted a contract force to a federal function. Some DOE and Los Alamos officials believe that federalizing the Los Alamos security force would traumatize employees and cause political turmoil in the local community but cited no specific examples to support their opinions. In addition, DOE noted that its operations offices do not have personnel slots to manage federal security forces, and OMB would require DOE to staff such positions from existing slots. OMB officials told us that they would work with DOE through the budget review process to help get the necessary positions if DOE can demonstrate that conversion is cost-effective. However, DOE officials said that the budget process is very time consuming and cumbersome and has not been responsive to their prior requests for additional federal personnel positions.

Conclusions

Contractors provide security services for all but one DOE facility. At nine facilities, we found that selected federal force costs may be at least $15 million less costly than contract forces. Believing that little or no cost difference exists, DOE has not reexamined analyses conducted in the early 1980s nor conducted additional ones to determine whether using contract forces today is cost-effective and, therefore, still warranted.

DOE says that both a federal and contract force are equally capable of protecting its facilities. However, a federal force may offer financial and other unquantifiable benefits that are not, nor are they required to be, considered in weighing the costs and benefits of obtaining security services. For example, a federal force cannot legally strike—the Los Alamos strike cost about $1.6 million over and above the almost $17 million contract costs. Also, a federal force may be more stable. High turnover rates, such as the 11 to 15 percent that occurred at Los Alamos before the strike, increase hiring, training, and security clearance costs. DOE would have to weigh these benefits against other factors, such as its ability to terminate employees. Nevertheless, taken together, a federal force may be able to offer numerous advantages across the board for DOE.

Recommendation to the Secretary of Energy

In this era of scarce budget resources, DOE needs to obtain protective services in the most cost-effective manner. Because significant savings may be realized by having federal rather than contract employees provide security services, we recommend that the Secretary of Energy conduct an in-depth analysis of the relative costs of federal and contract security services across the nuclear weapons complex and convert to federal forces at locations where it is cost-effective to do so.

Views of Los Alamos Security Force Members

The following summarizes the views expressed by 14 Los Alamos security force members concerning the (1) causes of the strike; (2) adequacy of security before, during and after the strike; (3) actions that could improve security; (4) quality and quantity of training; (5) usefulness of DOE's inspections, and (6) advantages and disadvantages of federalizing the security force. The views of these individuals cannot be projected to all the Los Alamos security force.

Strike Causes

All said the strike was caused by a combination of excessive, mandatory overtime, a restrictive sick leave policy, and a punitive disciplinary policy that increased stress because demerits could result in job loss. A common complaint was that the company gave demerits for minor reasons (eating at a desk, picking up a newspaper, and minor vehicular damage). Some also said that sometimes the company required employees to take annual leave in lieu of sick leave, even if they had a doctor's statement and sick leave time was available. Some acknowledged that Mason and Hanger instituted such a policy because of reported past sick leave abuses by the Los Alamos force. All but one said that the strike could have been prevented if Mason and Hanger had been more flexible and understanding with its employees and exhibited better human relations skills.

Adequacy of Security Before, During, and After the Strike

- About half said that security was poor before the strike because of fatigue and low morale caused by excessive overtime; the other half said security was good to adequate.
- Twelve said that security was poor or marginal during the strike because the replacements did not meet the physical fitness and medical requirements and were not trained in using the same weapons as the regular Los Alamos force. Also, several said that the replacements were unfamiliar with the site, and some posts were not staffed because not enough replacements were available.
- Thirteen said that security has improved since the strike. Some security inspectors also noted that an "open campus" atmosphere prevents them from fully implementing DOE's requirements because laboratory personnel complain when security inspectors do their jobs correctly. Also, some claimed that Los Alamos allows its personnel to circumvent the policies established.

Actions That Could Improve Security

The security force members offered various suggestions to improve security. Some examples follow.

- Increase training, especially to qualify with new weapons, increase firing range time, and provide more communications training.
- Obtain better equipment, such as 4-wheel drive vehicles, clothing, and holsters.
- Improve safety and health conditions that will decrease sick leave and injuries. For example, when a security inspector fell from a guard tower, Los Alamos made changes to make it safer but did not take the same actions to improve other towers. Guard posts should be improved: concrete floors are cold and some traffic islands are "falling apart," which allows exhaust fumes to enter the buildings and affect their health.
- Allow Mason and Hanger to manage security instead of Los Alamos and encourage labor relations training for Los Alamos, Mason and Hanger, and security force members.

Quality/Quantity of Training

Some security force members said that they were adequately trained to perform their jobs. One said that some members need more training on using weapons, but the firing range is seldom open. About 50 percent said that more training is needed on using the baton and arrest procedures. Some suggested that training classes should be smaller so the security force could receive more individual attention, and Mason and Hanger should use trained instructors rather than field supervisors. They also expressed concerns that training is often canceled, usually because of lack of funds.

Usefulness of DOE's Inspections

Eight said that DOE's inspections are useful because they help identify problems. On the other hand, some noted that the limited-scope performance tests do not represent real-life situations because DOE announces when the exercises will be held, training increases right before the tests, and some force members are preselected to participate. For these reasons, some force members did not believe that the tests appropriately assessed their competencies.

Federalizing

- Almost all said that they would like to be in the federal system because the benefits (sick and annual leave, health plan, and retirement) are better, and military service counts toward retirement. They also said that a federal force would take security more seriously, receive better training, and employee problems would be resolved in a timely manner.

- Many said that the major disadvantage would be a reduction in the salary received. However, some noted that the benefits were more important than salary.

Comparison of Six Facilities' Compliance With Albuquerque's Draft Contingency Plan Requirements

Requirements	1	2	3	4	5	6[a]
1. Identify number of posts needed during emergencies.	N	Y	Y	Y	Y	Y[b]
2. Identify number of nonstriking protective force individuals that would be available during strike on all shifts.	N	Y	Y	Y	Y	Y
3. Identify posts that could be shut down, curtailed, and/or consolidated.	Y	Y	Y	N	Y	N
4. Determine the priority of site operations that can be shut down or curtailed.	N	N	N	N	Y	N
5. Identify functions that could be accomplished by other staff.	N	N	Y	Y	Y	N
6. Describe how auxiliary guard uniforms will be idenfified.	N	Y	N	N	N	N
7. Describe how nonstriking security inspectors would be identified.	N	N	N	Y	N	N
8. Identify inventories and inspections to be made upon departure of striking employees.[c]						
a. weapons	N	N	N	N	N	Y
b. keys	N	N	N	N	N	N
c. emergency response vehicles/ equipment	N	N	N	N	N	Y
d. perimeter posts, radio, telephone, and alarms.	N	N	N	N	N	Y
9. Identify a plan to notify management and auxiliary guards in the event of a strike.	N	Y	Y	Y	N	N
10. Estimated amount of time required to implement the site contingency plan.	Y	N	N	N	N	N
11. Identify how, and for how long, local law enforcement agencies will provide assistance during a strike.	N	N	N	N	Y	N
12. Identify training to be held upon the arrival of augmentees.	N	N	N	N	N	N

(continued)

Requirements	1	2	3	4	5	6[a]
13. Identify training for auxiliary guards to be held prior to duty assignment.	Y	Y	N	Y	N	Y
14. Identify a point of contact to coordinate logistics, and explain how you will meet logistical needs.	N	Y	N	N	N	Y
15. Identify and discuss transition plans when the strike is terminated.	N	Y	N	N	N	N

[a]1=Pantex, TX.
2=Los Alamos, NM.
3=Pinellas, FL.
4=Kansas City, MO.
5=Mound, OH.
6=Rocky Flats, CO.

[b]Y=yes; N=no.

[c]Counting each of these items as separate topical areas results in a total of 18 requirements.

Major Contributors to This Report

Resources, Community, and Economic Development Division, Washington, D.C.

Judy England-Joseph, Associate Director, Energy Issues
Mary Ann Kruslicky, Assistant Director
Philip A. Olson, Assignment Manager

Denver Regional Office

John D. Gentry, Regional Manager's Representative
Craig D. Richards, Evaluator-in-Charge
Lois J. Curtis, Site Senior
Sarah A. Narvaez, Evaluator
Pamela K. Tumler, Report Analyst