The Project On Government Oversight

Back to POGO Main Page
For more information on
Energy and Environment Investigations

U.S. Nuclear Weapons Complex: Security At Risk

October 2001

Table of Contents

Foreword

"*And we will operate from a few basic principles. First, candor. No one should be wary of coming forward when they see a problem. It's the only way to define a solution. The urgency of our task dictates candor about our challenges and confidence in our ability to solve them.*"
Director of Homeland Security Tom Ridge, October 8, 2001

This report presents the results of an eight-month investigation initiated when more than a dozen insiders contacted POGO with unclassified evidence that the U.S. Department of Energy's nuclear bomb complex is vulnerable to terrorist attack. We were in the final stages of editing on September 11th. We immediately took our information to policy-makers, briefing the National Security Council, the Pentagon and Congressional Committees. During that process, our report was made public and began to receive media attention. Because of the extraordinary demand for this report, we are now making it available on POGO's website.

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 Metropolitan Areas Within 100 miles of Nuclear Weapons Facilities chart below). 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." (Emphasis added)1

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 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])

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)

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 DOE (Appendix F) 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

DOE Map of Plutonium Inventories (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)

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. (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." (Appendix T) 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 Sreet 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 in the Field Operations Office annual surveys section of this report below. (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 citizens11. 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.

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 earlier in this report , 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 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 Inspector General chart in Appendix C reveals the changes made by the Field Operations Office management from ratings of "unsatisfactory" to ratings of "marginal" or "satisfactory".

- *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 before in this report 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 draft GAO table in Appendix EE page 11, 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.

- 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 1½ 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 worse17.

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 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]

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.

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 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 (Appendix U and Appendix MM) to *USA Today* and the *Washington Post*. 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 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.

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

FOOTNOTES

Footnote and Document Note

Some of the Footnotes are links to actual documents on other web sites. You will not leave POGO's frame as you go to these links. Please use the back button on your browser to return to the report.

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

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 Appendix T, Appendix V, and Appendix BB.

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

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

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-t3/tab03.pdf - Downloaded as of September 17, 2001.

10. www.whistleblower.org/www/grafexcerpt.htm – Downloaded on September 17, 2001.

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.

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

14. Ibid.

15. Ibid.

16. Ibid.

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

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

19. Ibid.

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

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

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.

Click to the left to let POGO know! Please contact us if you have inside information concerning abuse of power, mismanagement or subservience to powerful special interests by the federal government.