The Sum of All Fears:

Security Gaps at Department of Energy Nuclear Weapons Facilities

Staff Summary of Responses by the
Department of Energy
to Correspondence from
Rep. Edward J. Markey (D-MA)
Member, Energy and Commerce Committee
Co-Chair, Bipartisan Task Force on Nonproliferation
U.S. House of Representatives
August 20, 2002

EMBARGOED UNTIL AUGUST 20, 2002

Table of Contents

Heading	Page
Introduction	3
DOE Reduced the Numbers of Security Guards at Nuclear Facilities Nearly In the Past Ten Years	6
DOE Has Consistently Told Congress, the Press and the Public That There Is No Security Problem, While Simultaneously Requesting More Emergency Funds to Meet "Urgent Security Needs," but the White House Has Twice Refused These Funds	9
DOE Design Basis Threat Security Upgrades And Implementation Are Taking Too Long to Complete And Are Inadequate	10
Two Yemeni Citizens Who Participated in a DOE Anti-Terrorism Training Program Disappeared in the U.S. After The Program Ended	12
DOE Force-on-Force Exercises Have Revealed Security Flaws, and DOE's Response Contains Inconsistencies	12
Successful Cyber-Attacks Have Taken Place at DOE Facilities	14
Results of the Los Alamos Safeguards and Security Survey Conducted by DOE in Summer 2001 Found Security Problems	17
Appendix A: Partial List of Reports Critical of DOE Security	20

Introduction

Following the terrorist attacks on the World Trade Center Towers and the Pentagon on September 11, 2001, Rep. Markey began to examine issues related to the adequacy of security at Department of Energy (DOE) nuclear facilities. The possibility of a terrorist attack on one of these facilities is not new, and Rep. Markey has long been concerned that the security requirements and implementation of these requirements is inadequate[1].

Moreover, numerous Congressional, independent and Executive Branch investigations have concluded that DOE security is gravely lacking[2]. For example, on June 15, 1999, the President's Foreign Intelligence Advisory Board (PFIAB) issued a report entitled Science at its Best, Security at its Worst: A Report on Security Problems at the U.S. Department of Energy which concluded that: security at DOE was "responsible for the worst security record on secrecy that the members of this panel have ever encountered," that the "Department has devoted far too little time, attention, and resources to the prosaic but grave responsibilities of security and counterintelligence in managing its weapons and other national security programs," and that DOE had essentially ignored 25 years worth of reports recommending improvements in security.

More recently, a September 2001 report entitled U.S. Nuclear Weapons Complex: Security at Risk by the Project on Government Oversight (POGO) described its eight-month investigation that used unclassified documents and credible whistleblower sources to establish that nuclear weapons material at DOE sites remains vulnerable to theft or onsite construction and detonation of dirty bombs or homemade nuclear weapons. In particular, the POGO report described repeated failures by DOE contractor security personnel to protect DOE facilities from attack by mock "terrorists" who were testing security, repeated failures by DOE and its contractors to address and correct identified security problems, and weak and ineffective oversight of security by DOE headquarters personnel.

Ten DOE sites, some of which are located near urban areas such as Denver Colorado and the Bay Area of California, reportedly contain enough weapons-grade plutonium (reportedly about 10 kg of metallic plutonium) and highly enriched uranium (reportedly about 50 kg of metallic uranium) to build a crude nuclear bomb (i.e. a bomb that does not require the use of sophisticated technologies such as neutron reflectors).

---

[1] See http://www.house.gov/markey/iss_terrorism_971014.pdf, a 1997 letter from Rep. Markey to then-DOE Secretary Pena on the threat of attacks on DOE nuclear facilities. The letter cited reports of improper storage of nuclear weapons materials in broken vaults, the possibility that terrorists who gained access to nuclear weapons materials could quickly construct a dirty bomb or crude nuclear bomb that could achieve criticality and produce nuclear yield, reports that anti-government militia groups attempted to recruit members from within the Rocky Flats security guard force, and that DOE reports on Safeguards and Security repeatedly downplayed and ignored security risks. Please also see http://www.house.gov/markey/iss_terrorism_ltr971125.pdf, a 1997 letter from Rep. Markey to the House Commerce Committee requesting that hearings be held on the topic.

[2] See Appendix A.

In addition, the DOE Transportation Security Division regularly transports nuclear weapons materials on public highways from site to site within the DOE complex.

On January 23, 2002, Rep. Markey sent a 23-page letter to DOE Secretary Spencer Abraham expressing his concerns that a group of suicidal terrorists might not bother to attempt to steal nuclear weapons materials from these sites; instead, they might attempt to gain access to the nuclear materials located within them by killing the security guard forces, and, once inside the facility, proceed to construct and detonate dirty bombs or homemade nuclear bombs[3]. Many reports in past months have detailed both Al Qaeda members' attempts to obtain nuclear materials as well as their desire to attack U.S. nuclear facilities.

A radiological dispersion device or "dirty bomb" could be created by surrounding nuclear weapons material with conventional explosives and then detonating the conventional explosives, or by detonating a large truck bomb adjacent to a facility used to store nuclear material. The amount of damage done would depend on the amount of radioactive materials (and how small the particles of those materials were made and dispersed) as well as on the amount of conventional explosives used to detonate the device. Such a device could be constructed quickly once terrorists gained access to the nuclear materials, and could result in deaths, cancer and widespread contamination of the surrounding community.

Even more alarming is the possibility that terrorists could rapidly construct and detonate an improvised nuclear device[4], or "homemade nuclear bomb," which could achieve criticality and release nuclear yield. Criticality occurs when the minimum amount of fissile nuclear material necessary to cause a chain reaction is brought together, either deliberately or accidentally. The first-ever fatal criticality accident took place at Los Alamos National Laboratory during the Second World War, when a Manhattan Project scientist accidentally dropped a metal block near a plutonium sphere and caused a chain reaction to begin, which delivered a fatal dose of radiation before he was able to move the metal block. A recent example of a criticality accident took place in 1999 in Tokaimura, Japan when too much highly-enriched uranium was allowed in a tank. The materials delivered fatal doses of radiation to two people and high doses of radiation to others before the chain reaction was halted.

If, instead of trying to stop a chain reaction, a group of suicidal terrorists tried to start one by rapidly propelling two masses of weapons-grade plutonium or uranium towards one another to create a critical mass (conventional explosives or propellants can be used to propel the masses towards one another), several independent security and nuclear weapons experts have suggested that the result could be equivalent to that of a detonation of a nuclear weapon.

---

[3] See http://www.house.gov/markey/iss_terrorism_ltr020122.pdf

[4] According to Department of Defense documentation, an improvised nuclear device is defined as "a device incorporating radioactive materials designed to result in the dispersal of radioactive material or in the formation of a nuclear-yield reaction. Such devices may be fabricated in a completely improvised manner or may be an improvised modification to a U.S. or foreign nuclear weapon."

On May 3, 2002, Secretary Abraham responded to Rep. Markey's letter with a 200+ page document (hereafter to be referred to as the DOE Response), some of which DOE requested not be released publicly. Other portions of the response were marked classified and kept at DOE headquarters[5]. Rep. Markey also obtained two classified briefings related to these documents and other security issues from DOE.

This analysis represents a summary of the unclassified material in the DOE Response provided to Rep. Markey. Secretary Abraham's letter stated that he considers "this Department's responsibilities to national security to be my number one priority,[6]" and that "our weapons complex remains safe and secure and the protection systems at our sites are robust, reliable, and responsive to evolving security challenges.[7]" However, the DOE Response indicates that security at U.S. nuclear weapons facilities continues to be inadequate, particularly in light of the events of September 11. Specifically, the DOE Response to Rep. Markey indicates that:

- DOE Reduced the Numbers of Security Guards at Nuclear Facilities Nearly 40 Percent In the Past Ten Years
- DOE Has Consistently Told Congress, the Press, and the Public That There is no Security Problem, While Simultaneously Requesting More Emergency Funds to meet "Urgent Security Needs," but the White House Has Twice Refused These Funds
- DOE Design Basis Threat Security Upgrades And Implementation Are Taking Too Long to Complete And Are Inadequate
- DOE Admitted That Two Yemeni Citizens Who Participated in a DOE Anti-Terrorism Training Program Disappeared in the U.S. After The Program Ended
- DOE Force-on-Force Exercises Have Revealed Security Flaws, and DOE's Response Contains Inconsistencies
- Successful Cyber-Attacks Have Taken Place at DOE Facilities
- Results of the Los Alamos Safeguards and Security Survey Conducted by DOE in Summer 2001 Found Security Problems, Despite Limitations

---

[5] Pages 3-9 of the DOE Response. Information that was kept classified includes: a) Information about the nature of the vaults used to store nuclear materials, the ability of the storage vaults to withstand aircraft impact or large truck bomb, and the worst-case consequences of such an attack. b) Information on specific changes to the Design Basis Threat, the regulations used to determine the level of security required at each site. c) Information about specific security measures taken by DOE after September 11. d) Information related to facilities that will be used for temporary storage of plutonium at the Savannah River Site. e) Information related to force-on-force exercises at DOE facilities. f) Information on why the public road that runs next to the Los Alamos buildings used to store weapons-grade nuclear materials was reopened and the distance between these buildings and vehicle barriers. While Rep. Markey has reviewed these classified materials, this staff report is based entirely on the unclassified materials provided by DOE, as well as other information available from open sources.

[6] Page 1 of the DOE Response

[7] Page 2 of the DOE Response

DOE Reduced the Numbers of Security Guards at Nuclear Facilities Nearly 40 Percent In the Past Ten Years

The DOE Response indicated that the numbers of security guard forces for the DOE complex have been reduced in the past 10 years. The total number of protective force personnel in the DOE complex went from 7091 in 1992 (of which 5640 were uniformed and 1451 were support staff), to 4262 in 2001 (of which 3500 were uniformed and 762 were support staff). This represents a 40% decline in the overall size of the guard force and a 38% decline in the number of uniformed guard forces.[8]

While almost all DOE sites reported significant cuts to the numbers of security guard forces between 1992-2001, these cuts may have an even higher impact on security than what might be apparent at first glance. This is because the cuts have been focused on armed guards who can actually do something to stop a terrorist attack on the facility. DOE has chosen to reduce the numbers of guards that carry firearms and have arrest powers more drastically than it has unarmed guards. Security guard forces at DOE labs contacted by Rep. Markey's staff indicated that unarmed guards are paid less than armed guards, have more limited promotion potential, and are not required to meet the same physical fitness standards.

This trend is shown in Table 1[9]. The numbers of unarmed guards were found by examining the columns marked "Security Officer" in the tables provided by DOE[10]. The numbers of armed guards were found by adding the numbers in the columns marked SPO I, SPO II and SPO III in the tables provided by DOE. Supervisors were not included in this process since it is unclear whether the supervisors are armed or unarmed.[11] For some of these sites, the mission and amount of materials that needed to be guarded changed dramatically over the reporting period, which could partially explain the reduction in security forces. However the scope of the reductions seem far greater than those which might reasonably be expected to accompany changes in mission or amount of materials in most cases.

For example, the WIPP facility, which was not even open in 1992, had 17 armed guards, all of which had been eliminated by 2001 – after the facility was open and being used to store radioactive waste. While the amount of radioactive materials at sites such as Rocky Flats may have decreased between 1992-2001, the missions and sizes of Sandia, Los Alamos and Livermore have not changed dramatically – yet there has been a 24%, 21% and 12% (respectively) decrease in the numbers of armed forces used to

---

[8] Page 205 of the DOE Response
[9] Pages 189-204 of the DOE Response
[10] Page 189 of the DOE Response indicates that a "Security Officer" is an "unarmed individual assigned the responsibility to accompany persons who lack need to know or access authorization within a security area in order to ensure adherence to security measures."
[11] Page 189 of the DOE Response indicates that an SPO I, II and III is an "armed and uniformed PF [protective forces] officer authorized to carry firearms and make arrests who is employed for, and charged with the protection of classified information and DOE assets..." and who is employed in various capacities at DOE sites.

guard those facilities. In addition, since nuclear materials are being shipped to the Savannah River Site from other facilities such as Rocky Flats, the 39% reduction in armed forces at the Savannah River Site simply cannot be justified.

An analysis of Table 1 shows that:

- Five of 31 sites (Grand Junction, Ames Lab, Fermi Lab, Princeton Lab and Fernald) never had armed security officers during the reporting period. One plant (Pinellas) had been deactivated during the reporting period.
- Seventeen of the remaining 25 sites had higher reductions in armed security officers than the average DOE complex-wide reduction of 38% (that included both armed and unarmed personnel).
- Ten of the remaining 25 sites had higher reductions in armed security officers than the total site-wide reduction in security officers. This means that they cut a higher percentage of their guard forces that could provide armed response and make arrests than guard forces that could not provide armed response or make arrests.
- Twelve of the remaining 25 sites either cut the same (within 2%) percentage of their guard forces that could provide armed response or make arrests as the total cuts made, or did not report having unarmed guard forces at any point during the reporting period.
- One site (Hanford) reported a 47% cut in armed security forces, an 84% cut in unarmed security forces, and a 51% cut overall.
- Only two sites (Pantex and Argonne West) reported an increase in numbers of armed security forces.

TABLE 1: Numbers of Security Guard Forces at DOE Sites

DOE Site	# armed forces in 1992	# armed forces in 2001	% change armed forces	# unarmed forces in 1992	# unarmed forces in 2001	% change unarmed forces	% change all guard forces
Kansas City Plant	76	37	- 51%	17	45	+ 165%	- 12%
Los Alamos	322	255	-21%	0	43	NA	- 8%
Pantex Plant Amarillo, TX	293	381	+ 30%	18	2	- 89%	+ 23%
Sandia Labs New Mexico	165	106	- 36%	12	5	- 58%	- 37%
Sandia Labs California	42	32	- 24%	0	0	0	- 24%
WIPP New Mexico	17	0	- 100%	7	14	+100%	- 42%
Grand Junction Colorado	0	0	0	13	5	- 62%	- 62%
Tonopah Test Range Nevada	58	33	- 43%	8	3	- 63%	- 45%
Pinellas Plant Florida[12]	73	0	-100%	0	0	0	-100%
Argonne East, Illinois	33	0	-100%	11	18	+ 64%	- 59%
Argonne West, Idaho	34	42	+ 23.5%	0	0	0	+ 23.5%
Brookhaven Lab, New York	60	37	- 38%	0	0	0	- 38%
Ames Lab, Iowa	0	0	0	4[13]	6	+ 50%	+ 50%
Fermi Lab, Illinois	0	0	0	35[14]	19	- 46%	- 46%
Princeton Lab, New Jersey	0	0	0	15[15]	15	0	0
Idaho Operations Office facilities	267	89	- 67%	25	20	- 20%	- 59%
Nevada Test Site	276	115	- 58%	17	4	- 76%	- 59%
Lawrence Livermore Lab	141	124	- 12%	8	4	- 50%	- 14%
Y-12 plant, Tennessee	473	248	- 48%	41	15	- 63%	- 49%
ETTP, Tennessee	101	43	- 57%	8	4	- 50%	- 57%
Oak Ridge Office, Tennessee	47	17	- 64%	0	0	0	- 64%
Portsmouth Plant, Ohio	202	34	- 83%	6	3	- 50%	- 82%
Paducah Plant, Kentucky	56	21	- 63%	1	2	+ 100%	- 60%
Mound Plant, Ohio	95	0	-100%	7	17	+ 143%	- 83%
Fernald, Ohio	0	0	0	17	26	+ 53%	+ 53%
West Valley, New York	10[16]	0	- 100%	9[17]	12	+ 33%	- 37%
Hanford Site, Washington	319	168	- 47%	37	6	- 84%	- 51%
Rocky Flats, Colorado	380	154	- 59%	26	8	- 69%	- 60%
Savannah River Site, South Carolina	698	423	- 39%	44	30	- 32%	- 39%
Strategic Petroleum Reserve, Texas and Louisiana	233	113	- 52%	0	9	NA	- 48%
DOE HQ, DC	156	33	- 79%	0	77	NA	- 29%

[12] Page 194 of the DOE Response states that "Pinellas protective force discontinued with plant deactivation."
[13] Page 195 of the DOE Response – the first year provided for Ames Lab is 1994.
[14] Page 196 of the DOE Response – the first year provided for Fermi Lab is 1994.
[15] Page 196 of the DOE Response – the first year provided for Princeton Lab is 1994.
[16] Page 202 of the DOE Response - the first year reported for West Valley was 1995.
[17] Page 202 of the DOE Response - the first year reported for West Valley was 1995.

DOE Has Consistently Told Congress, the Press, and the Public That There is no Security Problem, While Simultaneously Requesting More Emergency Funds to meet "Urgent Security Needs," But the White House Has Twice Refused These Funds

On January 23, 2002, then NNSA-director General John Gordon issued a press release in response to Rep. Markey's letter and the POGO report. It stated that he "personally reviewed our [security] posture immediately following the terrorist attacks in September," that "allegations that the Department of Energy has lax security at its nuclear weapons facilities are false and misleading," that "we aggressively protect our people, facilities, and materials, and we display a formidable security posture to potential attackers," and that "nuclear material is not at risk at Department of Energy facilities." General Gordon also wrote a letter to the editor of the Washington Post on February 16, 2002, in which he stated that the POGO report "needlessly and dangerously suggests an attacker or terrorist could have a chance of success, potentially creating danger when none exists," and that the DOE sites "are not places a terrorist could attack with any real expectation of success."

The May 3 DOE Response states that it "has extensive protection measures in place to mitigate against the remote possibility that a terrorist organization could construct or detonate a device. The way we store, handle and transport nuclear weapons and other strategic materials results in the most highly protected assets in this nation. There are no places that a terrorist could attack with any real expectation of success." [18] The DOE Response also stated that the answer to Rep. Markey's question regarding the amount of additional funding requested for security upgrades taken after September 11 was classified[19].

However, on March 14, 2002, DOE submitted an unclassified supplemental appropriations budget request to the White House Office of Management and Budget (OMB) requesting $379.7 million in additional funds "to meet urgent and compelling requirements for safeguards and security, emergency response, and energy security and assurance activities.[20]" The funds were requested after "security vulnerabilities were assessed on a site-by-site basis and immediate action was taken to mitigate many of the concerns,[21]" and DOE stated that it "is unable to meet the next round of critical security mission requirements.[22]" The funding request also noted that "Failure to support these urgent security requirements would be unwise.[23]"

---

[18] Page 176 of the DOE Response
[19] See Page 3 of the DOE Response indicating that the response to question 2 on Page 4 of Rep. Markey's January 23, 2002 letter is classified. See http://www.house.gov/markey/iss_terrorism_ltr020122.pdf for Rep. Markey's January 23, 2002 letter.
[20] See http://www.house.gov/markey/iss_terrorism_ltr020314.pdf
[21] See http://www.house.gov/markey/iss_terrorism_ltr020314.pdf
[22] See http://www.house.gov/markey/iss_terrorism_ltr020314.pdf
[23] See http://www.house.gov/markey/iss_terrorism_ltr020314.pdf

Inexplicably, the White House failed to include the vast majority (all but $26 million was rejected) of this request in its own supplemental appropriations request to Congress. On March 28, 2002, DOE sent another letter to OMB[24] expressing disappointment at the rejection, stating that DOE is "not operating, nor can it operate, under the pre-September 11 Design Basis Threat. Until that is revised, we must operate under Interim Implementing Guidance, and you have not provided resources to enable us to do so." Congress passed the Supplemental Appropriations bill in July 2002, and included about $360 million for emergency security and nonproliferation activities at DOE sites. On August 13, 2002, President Bush declined to use $5.1 billion of emergency supplemental funds appropriated by Congress. All but $26 million of the $360 million for DOE security has been refused by the White House, now for the second time this year.

DOE appears determined to maintain a sanguine public face, telling the public and Congress that there is nothing to worry about, while insisting in private that it cannot guarantee the security of DOE facilities at the funding levels approved by OMB.

DOE Design Basis Threat Security Upgrades And Implementation Are Taking Too Long to Complete And Are Inadequate

The Design Basis Threat (DBT) is the policy document that serves as the foundation used to determine the risk facing DOE facilities and therefore the security levels needed to protect these facilities from acts of terrorism, theft of nuclear materials or sabotage. After September 11, DOE began to reexamine its DBT, to determine what changes would be needed. According to the DOE Response, DOE and DOD have developed a draft "Interim Joint Threat Policy Statement" (IJTPS) which is still in review and which is expected to be finalized in the summer, almost a full year after September 11.[25] It is unclear why an "interim" statement is taking so long to prepare. The new DBT, however, will be based on a new Postulated Threat, a draft for which was completed by the intelligence community in late Spring 2002, and finalized by Fall 2002. According to the DOE Response, the new DOE DBT will be issued 90 days after the Postulated Threat is completed, by the end of 2002.[26]

Once the new DBT is issued, DOE nuclear facilities will have an entire year – until late 2003, if all proceeds according to schedule – to complete and submit their Site Safeguards and Security Plans (SSSPs) that will detail how they will implement the new security policy. After the draft plans are completed, DOE program offices will have 60 days in which to respond, until early 2004. The DOE Response says the implementation period will vary from site to site, but even if the plans were immediately implemented after the DOE program office review, the earliest any DOE facility would

[24] See http://www.house.gov/markey/iss_terrorism_ltr020422c.pdf
[25] Page 13, 181 of the DOE Response
[26] Page 13, 181 of the DOE Response

be required to implement the new security requirements would be almost 2.5 years after the September 11 attacks.[27]

DOE also reported delays in its security reporting requirements. DOE has yet to complete its 2000/2001 (the two reports are being combined into one) Report to the President on Safeguards and Security. [28]

Rep. Markey's staff has also been informed of some disturbing information regarding the progress of the DBT: According to several knowledgeable individuals, DOE has inexplicably decided to eliminate many of the resources that have provided its expertise in this area. In the past, the DOE has reportedly relied on Science Applications International Corporation (SAIC) and subcontracts thereto for its security expertise in developing threat assessments and the Design Basis Threat. Instead of increased reliance on these subcontractors for their expertise as DOE proceeds to revise the DBT, the DOE Office of Security (SO) has instead reportedly chosen to eliminate them entirely. For example, RETA Security was removed from its role as security analyst for DOE in late 2000. In June, 2002, DOE SO decided that it no longer required anyone to perform the threat assessment work that is used to help define the DBT, and deleted the task from its contract with SAIC. As a result, the SAIC subcontract held by Eagle Research Group Inc., which has advised DOE since 1993 on terrorism and terrorism protection, developed threat guidance used by DOE facilities nationwide for security planning, and prepared analyses of domestic and international terrorism threat issues and insider threats, was recently terminated (effective July 19, 2002). There is no in-house expertise at DOE that can provide the same level of assistance as these consultants provided as DOE continues to evaluate its security needs post-September 11.

DOE reportedly has also decided to proceed with a DBT that follows a "dual-track" approach, according to several knowledgeable sources. Level 1 facilities, which have been accorded an elevated interim threat level and have higher security levels, are reported to include the DOE entities that handle fully-assembled nuclear weapons (Pantex Plant in Amarillo Texas and the Office of Transportation Safeguards), while Level 2 facilities include the rest of the sites in the DOE complex that store large quantities of weapons-grade uranium and plutonium. DOE appears to have ignored the threat that a terrorist could break into one of the so-called Level 2 facilities, access the weapons-grade materials, and construct and detonate a dirty bomb or improvised nuclear weapon. Such a "dual-track" approach would seem to ignore or minimize both the serious consequences of such a scenario and the relative ease of assembling and detonating an improvised nuclear device as compared to successfully operating a fully-assembled nuclear weapon.

---

[27] Page 181 of the DOE Response
[28] Page 178 of the DOE Response

Two Yemeni Citizens Who Participated in a DOE Anti-Terrorism Training Program Disappeared in the U.S. After The Program Ended

In the DOE Response, the Department admitted that two Yemeni citizens who were attending a DOE training program (run by DOE for the State Department) designed to "assist delegations of foreign countries to harden their facilities to the many threats[29]" disappeared after the program was completed, and that the investigation into their disappearance was turned over to the FBI.

According to the DOE, one of the threats the program is designed to educate attendees about is "the threat posed by the terrorist. Information in this course has a heavy emphasis on physical security systems, with additional topical areas covering contingency planning, terrorist methodology, non-technical perimeter security, incident command, and the supervisory role in handling incidents involving explosive ordinance[30]." Would-be terrorists could find this training useful, as it would provide them with insight on how to spot the security systems in place at particular buildings as well as how to identify security vulnerabilities. The DOE Response did not reveal the results of the FBI investigation into the Yemenis' disappearance. DOE stated that it believed this program should be continued in order to ensure that terrorist attacks in other countries can be thwarted, and that prospective attendees are screened by DOE's Foreign Access Central Tracking System database, which feeds into the U.S. Counterintelligence Analytical and Research System.

DOE Force-on-Force Exercises Have Revealed Security Flaws, and DOE's Response Contains Inconsistencies

DOE periodically conducts force-on-force security exercises in order to assess the adequacy of security at its sites. Rep. Markey's letter requested general information about these exercises, and raised questions about specific exercises that reportedly resulted in the mock terrorists gaining access to weapons-grade uranium or plutonium.

The DOE Response revealed several inadequacies in and failures of past force-on-force exercises. In response to questions related to an exercise at Los Alamos National Laboratory (LANL), DOE concurred that protective forces that had already been "killed" by the mock "terrorists" got up and followed the mock "terrorists" back into the facility, but that the remaining guard forces could not have recaptured the facility had it been a real attack[31]. DOE also noted that in a 1998 force-on-force exercise at Rocky Flats near Denver, CO, mock "terrorists" were able to use speed, firepower and concealment smoke to penetrate the facility[32]. Finally, DOE found that during force-on-force exercises at Rocky Flats, Sandia National Laboratories in Albuquerque NM and at

[29] Page 14-17 of the DOE Response
[30] Page 14-17 of the DOE Response
[31] Page 37 of the DOE Response
[32] Page 165 of the DOE Response

the Savannah River Site 321-M facility in South Carolina, security guard forces fired on "civilians" during the exercises.[33]

However, the DOE Response also contains numerous inconsistencies and puzzling obfuscations:

- The DOE Response indicates that some responses to questions related to whether it had conducted force-on-force exercises at DOE facilities since September 11 are classified. [34] However, at a March 1, 2002 unclassified meeting with DOE security personnel, Rep. Markey's staff were informed that at least one force-on-force test had occurred at Lawrence Livermore National Lab (LLNL) since September 11. It is unclear why the DOE Response said this information was classified.

- DOE admitted that in a 1998 force-on-force exercise at Rocky Flats near Denver, CO, mock "terrorists" were able to use speed, firepower and concealment smoke to penetrate the facility. However, DOE stated that at the time it planned this exercise, it "was not aware of any credible improvised nuclear device or comparable radiological dispersal threat associated with the facility in question." [35] This was intended to justify DOE's decision to plan the exercise designed around whether the mock "terrorists" were able to steal weapons-grade materials from the facility, rather than their demonstrated ability to take over the facility and detonate an improvised nuclear device or comparable radiological dispersal threat onsite. It is unclear why DOE said it was unaware of this threat in 1998. Rep. Markey, for example, made DOE aware of it in October 1997 in correspondence to then-DOE Secretary Pena[36]. Moreover, Edward McCallum, then head of DOE's Office of Safeguards and Security, discussed this issue in 1997 during a highly publicized telephone conversation with Jeff Peters, Former Operational Security Manager, Wackenhut Services, Inc., at the Rocky Flats nuclear site near Denver, CO.[37]

- The DOE Response states that "the very concept of a "win/lose" percentage for such testing reflects a profound misunderstanding of the way in which DOE uses force-on-force performance testing, a misunderstanding that trivializes the real value of

---

[33] Page 166-169 of the DOE Response

[34] Page 3 of the DOE Response indicating that the response to Question 4 on Page 4 of the January 23, 2002 Markey letter to DOE is classified. For the January 23 2002 Markey letter, see http://www.house.gov/markey/iss_terrorism_ltr020122.pdf

[35] Page 165 of the DOE Response

[36] See http://www.house.gov/markey/iss_terrorism_971014.pdf

[37] See http://www.whistleblower.org/www/mccallum1.htm **Jeff Peters:** Yeah, well, they allow you with that new strategy unlimited time in the vault! And there's some scenarios out there that we can't even re-enact when I was there -- you couldn't re-enter the building if you had to. Well, you give the adversary that long with that kind of material, you know the result. That's just -- **Ed McCallum:** A little mushroom shaped cloud over – **Jeff Peters:** [Laughs] Exactly. You don't wanna' -- well, maybe you do wanna' be real close to it. At least it's fast. I think you'd probably rather go fast than the slow residual effects of radiation.

such testing."[38] It also states that the artificialities in the tests "argue strongly against treating apparent successes in penetrating to a target as reflecting the actual likelihood that a real adversary might successfully apply the same scenario."[39] In addition, it states that because DOE performs four exercise scenarios per force-on-force inspection, that "to argue that a single "win" or "loss" in such circumstances should be taken as indicative of overall protection effectiveness flies in the face of reason."[40] It appears from these arguments that DOE does not accept traditional notions of success or failure in the conduct of security force-on-force exercises – such as "would the terrorists likely have succeeded in accomplishing their mission, or not?" – but would rather use less well-understood and equivocal methods of assessing the adequacy of security at DOE nuclear facilities. However, DOE did not volunteer what its preferable assessment system might be.

- DOE believes that the Composite Adversary Team (CAT), which is made up of DOE protective force personnel, is the best group to perform the force-on-force exercises for the DOE Office of Independent Oversight and Performance Assurance, even though the team does not have as high a level of military skills as military special forces teams. DOE says this is because military special forces teams can be called up for overseas duty at any time, and because special forces teams wouldn't know as much about DOE sites as the CATs. DOE believes that using military special forces teams would pose a conflict-of-interest because DOE line management uses them to develop security plans, so using them to assess the adequacy of the same plans would be a conflict. It is not clear why using the CAT itself does not pose a conflict-of-interest, since the individuals are all DOE protective forces personnel, and are therefore charged with assessing their colleagues' performance.[41]

- Although there were several force-on-force exercises that resulted in the protective force's inappropriate use of deadly force and "killing" civilians or bystanders (specifically, at Rocky Flats, Sandia National Laboratories and the Savannah River Site), the DOE Response stated that "there is not a specific requirement for a site to separately report incidents of inappropriate use of deadly force during FOF [force-on-force] exercises.[42]"

Successful Cyber-Attacks Have Taken Place at DOE Facilities

Cyber-security has become an increasingly high profile concern since September 11. For example, a June 27, 2002 article in the Washington Post reported that groups of individuals located in the Middle East and South Asia were attempting to explore the computer systems used to operate emergency telephone systems, electrical generation and transmission, water storage and distribution, nuclear power plants and gas facilities.

---

[38] Page 11 of the DOE Response
[39] Page 12 of the DOE Response
[40] Page 12 of the DOE Response
[41] Page 4, 31-32 of the DOE Response
[42] Page 169 of the DOE Response

The article stated that some of the probes "homed in on a class of digital devices that allow remote control of services such as fire dispatch and of equipment such as pipelines. More information about those devices -- and how to program them -- turned up on al Qaeda computers seized this year, according to law enforcement and national security officials."

Rep. Markey requested information related to the number of successful hacking attempts that had taken place since an individual hacked into the Lawrence Livermore National Laboratory (LLNL) computer system in 1999 in order to cause damage. A list of all intrusions, compromises, or web defacements that were detected and reported to DOE's Computer Incident Advisory Capability that occurred from October 1999 – January 2002 was provided in Pages 218-226 of the DOE Response and is compiled in Table 2.

The total number of intrusions, compromises, or web defacements dropped from 130 in FY 1999 to 64 in FY 2001.[43] DOE attributed the decline to an increase in the number of firewalls and active email scanning capabilities. The security violations ranged from root-level compromises (which occur when a hacker is able to enter the computer system, and perhaps install viruses or software that would allow them to return to or damage the site, etc.), to compromises to the server, to an intruder sending email from an AOL account while making it appear as though it came from the White House, to viruses and other software installed. In each case, DOE reports that remediation steps such as patching the system or changing the password were taken.

[43] Page 217 of the DOE Response.

Table 2 – List of Successful Hacking Attempts at DOE Facilities[44]

DOE Site	# Root-Level Compromises	# FTP Server Compromises	# Email/User Server or Personal Computer Compromises	# Software/ Virus/ Directory/ Internet Chat Installations	# Web compromises/ defacements
Nevada Operations	0	1	0	1	1
Los Alamos	1	1	0	0	1
Lawrence Livermore	2	0	2	0	0
Sandia New Mexico	7	0	0	1	2
Sandia California	2	0	1	0	0
WIPP New Mexico	0	0	1	0	0
Chicago Operations	0	0	0	0	1
Oak Ridge Operations	0	0	1	1	1
Ames Lab	Multiple systems in 1 incident, 3 incidents total	0	0	0	0
Argonne National Lab	9	0	0	0	1
Brookhaven National Lab	3	0	1	0	multiple
Fermi Lab	Multiple systems in 1 incident, 3 incidents total	0	1	4	1
GAT	1	0	0	1	0
Lawrence Berkeley Lab	16 incidents total, 2 systems in 1 incident	0	4	4	1
Oak Ridge	4	0	5	5	1
DOE Office of Scientific and Technical Information	0	0	0	0	1
Princeton Plasma Physics	1	0	0	0	0
Thomas Jefferson National Accelerator Facility	1	0	2	0	1
Hanford Environmental Health Foundation	0	0	0	0	1
Idaho Engineering and Environmental Laboratory	1	0	0	0	1
Pacific Northwest Lab	3	0	0	0	1
Golden Field Office	1	0	0	0	0
National Renewable Energy Lab	1	0	0	0	1
DOE Headquarters	1	0	0	1	1
Energy Information Administration	Unspecified compromise	0	0	0	0

[44] In some cases, a hacking incident may have involved, for example, a server compromise AND the installation of software or a virus – this situation would be tabulated twice in Table 2 to indicate that both of those security violations occurred.

Results of the Los Alamos Safeguards and Security Survey Conducted by DOE in Summer 2001 Found Significant and Disturbing Security Problems

Rep. Markey's January 23 letter requested copies of the Inspection Plans for LANL for 2000 and 2001 because there had been allegations that the security ratings associated with earlier such surveys had been altered with no justification and that relevant documentation was destroyed. These were provided.[45] The Plan was supposed to assess the following subcategories:

- physical security (protective lighting, physical barriers, lock and key control, personnel and vehicle access control, and property protection)
- security systems (i.e. closed circuit TV, alarm systems)
- protection program operations (strategies for protecting each safeguards and security interest, security guard forces, security badges, credentials and shields, transportation security)
- classified matter protection and control, operational security program (the process designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive Departmental activities or information and to prevent the unauthorized disclosure of such information)
- special nuclear material control and accountability
- incident reporting and management
- personnel security (including the insider threat possibility, visits by foreign nationals, security clearances, etc.)

Some of the documents provided stated that it is DOE policy "not to write Findings against the Facility being inspected if previously identified in a Self-Assessment," but that findings would be included if milestones in the Corrective Action Plans were not being met or if "the finding identified during the Survey has major implications to the overall protection program system effectiveness for the facility and would significantly affect the "Rating" for a sub-topic, a topic or the overall Composite Rating for the facility."[46] Perhaps as a result of this policy to omit "self-assessment" security findings, only a few 2001 security findings were provided in response to Rep. Markey's request. However, these indicate that even after the 1999 security problems revealed at Los Alamos, there remain serious concerns:

- The survey found that LANL was not marking all classified material with the classification level and classification category in accordance with DOE requirements.[47] In one case, hundreds of classified parts that had not been marked classified had recently been inventoried by a custodian.

---

[45] Pages 53-143 of the DOE Response
[46] Page 83, 84 of the DOE Response
[47] Page 144-145 of the DOE Response

- The survey found that LANL had no system in place to determine which information systems security officers had completed required annual training. This weakness was considered to have a "high impact" because if the personnel don't have the right training, "there is little assurance that all required protections and controls have been properly implemented."[48]

- The survey found that the LANL information security policies and procedures Cyber Security Handbook was not kept up to date, and "contains conflicting, contradictory and outdated information. In addition, program documentation referenced in the handbook also contains conflicting and contradictory information, and does not reflect current program requirements."[49] The DOE reviewers said this could have a high impact because of the "potential for compromise of classified information."

- The survey found that there was no current disaster recovery plan in the Central Computing Facility, and that when a plan was found, "it was dated 1997 and did not contain the names and phone numbers of current responsible personnel." The impact was judged to be medium, because "incorrect information delays reporting and responding to disasters."[50]

- The survey found that there was no documentation indicating that the required annual TEMPEST (telecommunication emission security) threat assessments and special review were conducted. For some facilities, no reviews had been performed since 1999.[51]

- The survey found that security features of the Basic Rapid Alarm Security System (BRASS) and Los Alamos Integrated Communication System (LAICS) were not tested prior to the features being accredited. This also was judged to have a high impact because "if security features are not tested, there is no assurance that protection mechanisms are functioning as expected."[52]

- The survey found that contingency plans for BRASS and LAICS had not been tested as required, and that "there is little assurance that BRASS or LAICS could recover from a catastrophic loss if the contingency plans are not tested."[53]

- The survey found that the Protection Program Plan (which describes the standards of protection for unclassified information at LANL) does not accurately describe required protections for unclassified information. The impact was judged to be high,

---

[48] Page 146 of the DOE Response
[49] Page 147 of the DOE Response
[50] Page 148 of the DOE Response
[51] Page 149 of the DOE Response
[52] Page 150 of the DOE Response
[53] Page 151 of the DOE Response

because "if accurate information is not provided, there is little assurance that information is protected in a consistent manner."[54]

- The survey found that "formal, documented, inspections of inaccessible, aerial and unexposed classified distributive information network runs are not conducted." Apparently, the Site Manager was not aware of this annual requirement. The finding stated that it was possible that "a modification could be made to the CDIN [classified distributive information network], providing for unauthorized access to classified information through wiretapping."[55]

The ratings for this 2001 survey indicated that LANL received satisfactory ratings in all but 2 categories, and received marginal ratings in the areas of Classified and Unclassified Automated Information Systems Security because of the risk that both classified and sensitive information could be compromised.[56] Even though only some security findings were allowed to be included in the survey, these still indicate that serious security shortfalls still exist at LANL.

[54] Page 152 of the DOE Response
[55] Page 153 of the DOE Response
[56] Page 154-157 of the DOE Response

Appendix A
Partial List of Reports Critical of DOE Security[57]

1. "*Department of Energy: Fundamental Reassessment Needed to Address Major Mission, Structure, and Accountability Problems*," General Accounting Office, December 21, 2001.
2. "*Management Challenges at the Department of Energy*," DOE Inspector General, December 2001.
3. "*Inspection of Lawrence Livermore National Laboratory Protective Force and Special Response Team*," DOE Inspector General, December 2001 (Classified).
4. "*U.S. Nuclear Weapons Complex: Security At Risk*," POGO Report, October 2001.
5. "*The Department's Unclassified Cyber Security Program*," DOE Inspector General, August 2001.
6. "*Control of Classified Matter at Paducah*," DOE Inspector General, July 2001.
7. "*Government at the Brink: Volume II, An Agency by Agency Examination of Federal Government Management Problems Facing the Bush Administration*," Chairman Senator Fred Thompson, Committee on Governmental Affairs, June 2001.
8. "*Department of Energy: Views on the Progress of the National Nuclear Security Administration in Implementing Title 32*," General Accounting Office, April 2001.
9. "*Information Security: Safeguarding of Data in Excess Department of Energy Computers*," General Accounting Office, March 2001.
10. "*Eleventh Annual Report to Congress*," Defense Nuclear Facilities Safety Board, February 2001.
11. "*High Risk Series: An Update*," General Accounting Office, January 1, 2001.
12. "*Major Management Challenges and Program Risks: Department of Energy*," General Accounting Office, January 2001.
13. "*Management Challenges at the Department of Energy*," DOE Inspector General, November 2000.
14. "*Inspection of Selected Aspects of the Department of Energy's Classified Document Transmittal Process*," DOE Inspector General, November 2000.
15. "*Security Incident at Technical Area 18, Los Alamos National Laboratory*," DOE Inspector General, November 2000.
16. "*Establishing the National Nuclear Security Administration: A Year of Obstacles and Opportunities*," Special Oversight Panel on Department of Energy Reorganization, House Committee on Armed Services, October 13, 2000.
17. "*Summary Report on Allegations Concerning the Department of Energy Site Safeguards and Security Planning Process*," DOE Inspector General, September 2000.
18. "*Weaknesses in Classified Information Security Controls at DOE'S Nuclear Weapon Laboratories*," Hearing before the House Committee on Commerce Subcommittee on Oversight and Investigations, July 11, 2000.
19. "*Computer Insecurities at DOE Headquarters: DOE's Failure to Get Its Own Cyber House in Order*," Hearing before the House Committee on Commerce Subcommittee on Oversight and Investigations, June 13, 2000.
20. "*Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research*," General Accounting Office, June 9,2000.
21. "*Department of Energy: National Security Controls Over Contractors Traveling to Foreign Countries Need Strengthening*," General Accounting Office, June 2000.
22. "*Inspection of Surplus Computer Equipment Management at the Savannah River Site*," DOE Inspector General, June 2000.
23. "*Whistleblowers at Department of Energy Facilities: Is There Really 'Zero Tolerance' for Contractor Retaliation?*" Hearing before the House Committee on Commerce Subcommittee on Oversight and Investigations, May 23, 2000.
24. "*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*," DOE Inspector General, May 2000.
25. "*Legislation to Improve Safety and Security in the Department of Energy*," Hearing before the House Committee on Commerce Subcommittee on Energy and Power, March 22, 2000.

---

[57] This list was prepared by the Project on Government Oversight

26. "*Department of Energy: Views on Proposed Civil Penalties, Security Oversight, and External Safety Regulation Legislation*," General Accounting Office, Statement of Gary L. Jones, Associate Director, Energy, Resources, and Science Issues, Resources, Community, and Economic Development Division, March 22, 2000.
27. "*Safety Security Oversight of the New National Nuclear Security Administration*," Joint Hearing before the House Committee on Commerce Subcommittees on Energy & Power and Oversight & Investigations, March 14, 2000.
28. "*Status of the National Nuclear Security Administration, Department of Energy*," Hearing before the Special Oversight Panel on Department of Energy Reorganization, House Armed Services Committee, March 2, 2000.
29. "*Department of Energy: Views on DOE's Plan to Establish the National Nuclear Security Administration*," General Accounting Office, Statement of Gary L. Jones, Associate Director, Energy, Resources, and Science Issues, Resources, Community, and Economic Development Division, March 2, 2000.
30. "*Nuclear Security: Security Issues at DOE and Its Newly Created National Nuclear Security Administration*," General Accounting Office, March 2000.
31. "*Inspection of the Department of Energy's Export License Process for Foreign National Visits and Assignments*," DOE Inspector General, March 2000.
32. "*Unclassified Computer Network Security at Selected Field Sites*," DOE Inspector General, February 2000.
33. "*Nuclear Security: Improvements Needed in DOE's Safeguards and Security Oversight*," General Accounting Office, February 2000.
34. "*Draft Statement of Facts, Nuclear Security: Improvements Needed in DOE's Safeguards and Security Oversight*," General Accounting Office, December 14, 1999.
35. "*An Inspection of the Sale of a Paragon Supercomputer by Sandia National Laboratories*," DOE Inspector General, December 1999.
36. "*The State of Security at the Department of Energy's Nuclear Weapon Laboratories*," Hearing before the House Committee on Commerce Subcommittee on Oversight and Investigations, October 26, 1999.
37. "*Results of Security Inspections at the Department of Energy's Lawrence Livermore National Laboratory*," Hearing before the House Committee on Commerce Subcommittee on Oversight and Investigations, July 20, 1999.
38. "*Restructuring the Department of Energy*," Joint Hearing of the House Committees on Commerce Subcommittee on Energy & Power and the Science Subcommittee on Energy & Environment, 106th Congress, July 13, 1999.
39. "*Department of Energy: Need to Address Longstanding Management Weaknesses*," General Accounting Office, Statement of Victor S. Rezendes, Director, Energy, Resources, and Science Issues, Resources, Community, and Economic Development Division, July 13, 1999.
40. "*Retaliation at the Departments of Defense and Energy: Do Advocates of Tighter Security for U.S. Technology Face Intimidation?*" Hearing before the House Committee on Government Reform, June 24, 1999.
41. "*Science at its Best, Security at its Worst: A Report on Security Problems at the U.S. Department of Energy*," A Special Investigative Panel, President's Foreign Intelligence Advisory Board, June 1999 (Rudman Report).
42. "*The Rudman Report: Science at its Best, Security at its Worst*," Hearing before the House Committee on Commerce, June 22, 1999.
43. "*Cox Committee Report*" aka "*U.S. National Security and Military/Commercial Concerns with the People's Republic of China*," House Select Committee; Rep. Christopher Cox, Chairman, May 25, 1999 (Classified).
44. "*Security at the Department of Energy's Laboratories: The Perspective of the General Accounting Office*," House Committee on Commerce Subcommittee on Oversight and Investigations, April 20, 1999.
45. "*Key Factors Underlying Security Problems at DOE Facilities*," General Accounting Office, Statement of Victor S. Rezendes, Director Energy, Resources, and Science Issues, Resources, Community, and Economic Development Division, April 20, 1999.

46. "*Internal Report to the Secretary: Special Security Review*," Roger Hagengruber Report, January 21, 1999 (Classified).
47. "*Balancing Scientific Openness & National Security Controls at the Nation's Nuclear Weapons Laboratories*," Committee on Balancing Scientific Openness & National Security, National Academy of Sciences, National Academy of Engineering, Institute of Medicine, 1999.
48. "*Admiral Jeremiah report*," aka "*Intelligence Community Damage Assessment of China's Acquisition of U. S. Nuclear Weapons Information*," Report of the panel chaired by Admiral David Jeremiah.
49. Hearing of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, House of Representatives, October 14, 1998.
50. "*DOE Needs To Improve Controls Over Foreign Visitors To Its Weapons Laboratories*," General Accounting Office, Statement of Keith O. Fultz, Assistant Comptroller General, Resources, Community, and Economic Development Division, October 14, 1998.
51. Hearing of the House Committee on National Security Subcommittee on Military Procurement, October 6, 1998.
52. "*Department of Energy: Problems in DOE's Foreign Visitors Program Persists*," General Accounting Office, Statement of Keith O. Fultz, Assistant Comptroller General, Resources, Community, and Economic Development Division, October 6, 1998.
53."*Assessment Report: Department of Energy Nuclear Weapons-Related Security Oversight Process*," U.S. Nuclear Command and Control System Support Staff, March 1998.
54. "*DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories*," General Accounting Office, September 1997.
55. "*The Organization and Management of the Nuclear Weapons Program*," Paul Richanbach, Institute for Defense Analyses, March 1997.
56. 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.