2 May 2005

From: Richard W. Mies, Admiral USN (Retired)

To: NNSA Administrator, Ambassador Linton Brooks

Subject: Independent NNSA Security Review

Enclosure (1) NNSA Security - An Independent Review

1. Background. Since President Franklin Delano Roosevelt created the American nuclear weapons program by informal directive in October 1939, preserving nuclear security has been a national imperative. It also has been an exceptional challenge. Many of the difficulties inherent in nuclear security - creating an open yet secure atmosphere for world-class nuclear weapons science, managing contact with foreign scientist, securing and accounting for minute quantities of special nuclear materials - have been part of the program since its birth. Modem technology keeps bringing new challenges. Cyber security is one example; the proliferation of microelectronic devices – cellular, telephones, personal data assistants, increasingly powerful laptop computers, and high capacity computer memory devices – has created a new array of security challenges.

Federal oversight of the nuclear weapons program has evolved through the years beginning with the Uranium Committee in late 1939; transitioning to the National Defense Research Committee, then the Office of Scientific Research and Development, and then the Manhattan Project during World War II; residing in the newly created Atomic Energy Commission (AEC) in 1947; transferring to the Energy Research and Development Administration in 1975; and finally shifting to the newly created Department of Energy (DOE) in 1977.

In 1999, Congress, reacting in part to security lapses, transferred responsibility to a semiautonomous agency, the National Nuclear Security Administration (NNSA). Section 3212 of NNSA's Title XXXII legislative charter gave the NNSA Administrator authority over, and responsibility for, all programs and activities of NNSA, including safeguards and security (S&S). In practice, although NNSA is closely involved in security policy development, separate DOE offices outside NNSA develop security policy and conduct independent security audits and inspections.

Nuclear security, always important, has become even more critical in the aftermath of September 11. A previous commission highlighted a problem in the entire nuclear weapons complex - the aging federal and contractor scientific and technical workforce - which also pertains to the approximately 150 federal security professionals in NNSA. In

2002, another commission report identified the new challenges facing DOE in operating premier scientific instructions in the 21" century in a manner that fosters scientific excellence and promotes the missions of the Department, while protecting and enhancing national security. Finally, a series of well-publicized security incidents had, by the summer of 2003, led Energy Secretary Spencer Abraham to direct NNSA to aggressively and broadly improve nuclear security.

2. Against this background, NNSA Administrator Linton Brooks established two groups to assess long-range issues affecting security management and protection. The first study group analyzed the federal security workforce; this study, broader in scope, examines a multitude of factors that affect NNSA's security programs. For the past 18 months, we have independently reviewed security at NNSA sites. This report describes our analyses, summarizes our findings, and recommends ways to improve NNSA's security. We interviewed professionals who directly manage and indirectly support the security programs throughout the NNSA complex, including those at Los Alamos, Pantex, Oak Ridge, Livermore, Sandia, Nevada, and Savannah River and DOE and NNSA headquarters. We also reviewed past reports and numerous other documents relating to the nuclear security program and received briefings on topics germane to this study from responsible officials in DOE and NNSA.

We were given a very broad charter to take a strategic look at how security within DOE/NNSA is organized and structured, the interrelationships between various security disciplines, and the existing security policies, procedures, and practices in place to recommend possible improvements. We were specifically not chartered to look at specific security incidents and individual NNSA organizations in isolation.

3. Enclosure (1) forwards the detailed observations and recommendations of our study group. Because of the comprehensive nature and sensitivity of the security issues addressed in our review, enclosure (1) has been classified.

4. Our review consists of 13 sections which address specific areas of security within DOE/NNSA. An unclassified summary of our general observations in each of these areas follows:

Culture: NNSA is plagued by a number of cultural problems that, until addressed, will erode its ability to establish and provide security consistent with the gravity of its mission:

- Lack of a team approach to security
- Disparate views and an underappreciation of security across the enterprise, such that security is not fully embraced as integral to mission

- Ingrained organizational relationships that inhibit an enterprise approach to security
- A bias against training
- An over-reliance on a compliance-based approach to security rather than a more balanced approach using performance-based standards
- Lack of trust in the security organization
- An absence of accountability.

Roles, Responsibilities, and Relationships: The small size of the NNSA organization greatly impedes its effectiveness with the DOE headquarters bureaucracy. Although NNSA has made good progress by consolidating security functions, responsibility for security as a process is still fragmented and, along with authority and accountability for security, is not adequately embedded in individual and line management responsibilities. Until recently, staffs were organizationally misaligned. Security personnel with sufficient certification, training, rotation, and broad experience are lacking. Security collaboration between DOE/NNSA and DoD and among individual security disciplines within DOE is lacking. NNSA headquarters has inappropriately delegated virtually all security oversight, review, and assistance responsibilities to the site offices, divorcing itself from day-to-day oversight.

Security Policy: The NNSA enterprise lacks a comprehensive strategic security plan. Policy collaboration is lacking between DOE and DoD, internally within DOE/NNSA headquarters, between headquarters and the sites, and among sites. NNSA does not have adequate staffing to direct policy to the field or facilitate site implementation. In general, security policy is not sufficiently prescriptive and is open to too much individual interpretation in implementation. No effective system is in place for verifying documented security guidance and direction.

Cyber System Security: DOE/NNSA cyber security policies, procedures, and practices are less mature than their counterparts in other security disciplines. NNSA is resource poor in terms of secure or classified networks and access terminals. Insufficient resources have been devoted to address many of its cyber security issues, particularly the insider threat. Cyber security implementation varies widely throughout NNSA because of the lack of an enterprise approach, inadequate funding, insufficient cyber security personnel and expertise, and inadequate collaboration among DOE and NNSA cyber security organizations. Cyber security is not sufficiently integrated with other security disciplines, such as physical, personnel, material control and accountability, counterintelligence, and intelligence. This stovepipe approach to security has hindered the development of a more comprehensive coordinated approach to securing NNSA information assets.

Counterintelligence: The DOE/NNSA counterintelligence program suffers from a dysfunctional relationship between counterintelligence offices, insufficient collaboration with the other security disciplines, lack of a proactive approach to protection of information, and insufficient emphasis on the insider threat. Counterintelligence budget allocations do not appear to be aligned with program priorities. Finally, performance objectives designed to promote counterintelligence initiatives to deter, prevent, and preempt espionage activities are lacking.

Site Safeguards and Security Plans (SSSP). Vulnerability Assessments NA). and Performance Testing: A number of factors -the shortage of experienced VA analysts, increase in work-load resulting from the new design basis threat (DBT), lack of a comprehensive VA training program, overreliance on a few VA tools, and lack of a rigorous, institutionalized VA approach -detract from the validity and consistency of VAs across the NNSA complex. In addition, weaknesses and wide variations in SSSP limited scope performance testing and force-on-force exercises distort physical security assessments across the complex, promote a false sense of security in selected areas, and complicate prudent allocation of security resources to address potential vulnerabilities.

Protective Force: NNSA lacks a consistent approach for validating protective force manning; because of wide variations in site approaches, determining whether site protective force can adequately meet the requirements of the new DBT remains problematic. Protective force performance is degraded by an excessive backlog in security clearances, inadequate guidance and training in several significant areas (such as adversary pathways, chemical and biological weapon defenses, and recapture, recovery and pursuit), and a lack of collaboration with vulnerability assessment experts, FBI, and local law enforcement officials. Response plans, target folders, and central alarm station systems need upgrading to improve protective force readiness.

Security Incidents and Inquiries: The reporting, investigation, monitoring, and analysis of security incidents within NNSA are hindered by inconsistent practices, redundant reporting, and inadequate reviews. More formal and disciplined processes are needed to ensure the underlying causes of incidents are identified and addressed, appropriate corrective action is effectively implemented, and lessons learned are disseminated within NNSA to mitigate against recurrence.

Design Basis Threat (DBT) Implementation: There has been insufficient collaboration between DOE and DoD and among NNSA sites in translating the intelligence community's postulated threat into security requirements. As a result, NNSA security standards differ:

- from those of DoD nuclear weapons facilities, because DOE/NNSA has taken a different approach to dealing with the postulated threat than that of DoD, and

- ♦ from site to site, because sites interpret terms such as insider threat, mission-critical facilities, escorting policies, and improvised nuclear devices differently.

Determining whether NNSA will meet DBT implementation objectives by FY06 is difficult: the process for managing the program and funding requirements largely depend on the sites' interpretations of DBT requirements.

Security Research and Development (R&D) Programs: DOE/NNSA lacks a strategic vision and plan for R&D, procurement, and installation of technologies to improve security across the enterprise. There is no centralized technology component with the department to oversee such a plan. As a consequence, security upgrade initiatives to employ new technologies are inconsistent. Sites are independently engineering upgrades without benefit of expert headquarters oversight and complex-wide collaboration. There is no robust technology R&D foundation for an advanced protection strategy.

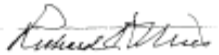
Nuclear Materials and Waste Storage: DOE/NNSA lack an enterprise-wide plan for consolidation of Special Nuclear Material (SNM). A lack of collaboration between NNSA and other elements of DOE, such as EM and NE, may preclude some secure and cost effective alternatives for consolidation from consideration. DOE /NNSA should seek to make greater use of underground storage. Some radiological waste storage areas may 1ack adequate protection against sabotage which could cause wide-area radiological dispersal.

Security Resources and Requirements: NNSA has made good progress in implementing a planning, programming, budgeting and evaluation (PPBE) process, but much remains to be done. The lack of an enterprise approach to security planning, inconsistent site-to-site interpretation and implementation of security resource requirements, lack of collaboration among the participants in the budget process, lack of a centralized budget validation process, and a cumbersome and unresponsive reprogramming process complicate rational resource planning, programming, budgeting, and evaluation to meet evolving security needs.

Security Contracting: The contractual relationships for security which NNSA has inherited are varied and adverse. Current and past security contracts insufficiently delineate performance expectations. The NNSA move to emphasis on broad, performance-based contracting-with appropriate focus on security as a key element of maintenance and operations (M&O) contractor performance-is a very positive, overdue step. NNSA has been operating under the Department of Energy Acquisition Regulation (DEAR); however, NNSA requires a unique set of tailored acquisition regulations and a common, standardized policy and practices to enable greater consistency and discipline across its breadth of national security missions.

5. Our panel has provided a number of detailed recommendations to address each of our specific concerns outlined in general terms above. Of greatest concern, our panel finds that past studies and reviews of DOE/NNSA security have reached similar findings regarding the cultural, personnel, organizational, policy and procedural challenges that exist within DOE and NNSA. Many of these issues are not new; many continue to exist because of a lack of clear accountability, excessive bureaucracy, organizational stovepipes, lack of collaboration, and unwieldy, cumbersome processes. Robust, formal mechanisms to evaluate findings, assess underlying root causes, analyze alternative courses of action, formulate appropriate corrective action, gain approval, and effectively implement change are weak to non-existent within DOE/NNSA. Accordingly, our panel strongly recommends that NNSA continue to work within DOE to develop, with urgency, a more robust, integrated DOE/NNSA-wide process to provide accountability and follow-up on security findings and recommendations.

6. Additionally, our panel fully supports the findings and recommendations of the Chiles panel on the need for improved career development, assignment rotation, training, professional qualification, and certification of NNSA security personnel. All security systems ultimately depend on trust. Committed, well trained, and experienced people can overcome organizational deficiencies; but no organizational improvements can overcome uncommitted, poorly trained, or inexperienced people.



Richard W. Mies
Admiral, US Navy (Retired)

NNSA SECURITY

An Independent Review

April 2005

CONTRACT NUMBER DEAM5204NA99608

Contents

Figures

Tables

Acknowledgments

This study was conducted under the leadership of ADM Richard W. Mies USN (Retired). Sage Systems Technologies, LLC, and LMI supported the effort. The primary contributors to this report include the following:

- ADM Richard W. Mies USN (Retired), Study Director
- Mr. Paul Grimm
- Mr. Gregory R. English
- Mr. Victor A. Lambson
- Mr. Fremont G. Mortensen
- Mr. Scott W. Patrick
- Mr. Matthew R. Pincock
- Mr. John F. Seward

The study team is grateful for the support of numerous individuals at both NNSA and DOE, who provided the information that allowed us to develop our findings and recommendations. Other contributors to the effort include Mr. Bill Coleman, Mr. David Dietz, and Mr. Ronnie Edge.

Section 1
Introduction

1.1 BACKGROUND[1]

Since President Franklin Delano Roosevelt created the American nuclear weapons program by informal directive in October 1939, preserving nuclear security has been a national imperative. It also has been an exceptional challenge. Many of the difficulties inherent in nuclear security—creating an open yet secure atmosphere for world-class nuclear weapons science, managing contact with foreign scientists, securing and accounting for minute quantities of special nuclear materials—have been part of the program since its birth. Modern technology keeps bringing new challenges. Cyber security is one example; the proliferation of microelectronic devices—cellular telephones, personal data assistants, increasingly powerful laptop computers, and high capacity computer memory devices—is another.

Federal oversight of the nuclear weapons program has evolved through the years, beginning with the Uranium Committee in late 1939; transitioning to the National Defense Research Committee, then the Office of Scientific Research and Development, and then the Manhattan Project during World War II; residing in the newly created Atomic Energy Commission (AEC) in 1947; transferring to the Energy Research and Development Administration in 1975; and finally shifting to the newly created Department of Energy (DOE) in 1977.

In 1999, Congress, reacting in part to security lapses, transferred responsibility to a semiautonomous agency, the National Nuclear Security Administration (NNSA). Section 3212 of NNSA's Title XXXII legislative charter gave the NNSA Administrator authority over, and responsibility for, all programs and activities of NNSA, including safeguards and security (S&S). In practice, although NNSA is closely involved in security policy development, separate DOE offices outside NNSA develop security policy and conduct independent security audits and inspections.

Nuclear security, always important, has become even more critical in the after-math of September 11. NNSA is reorganizing its structure and its approach to managing the contracts for its government-owned nuclear facilities it supervises. A former commission highlighted a problem in the entire nuclear weapons complex—the aging federal and contractor scientific and technical workforce—which also pertains to the

[1] Because it also pertains to this study, we included the entire "Background" subsection from the following report: NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

approximately 150 federal security professionals in NNSA[2]. In 2002, another commission report identified the new challenges facing DOE in operating premier scientific institutions in the 21st century in a manner that fosters scientific excellence and promotes the missions of the Department, while protecting and enhancing national security[3]. Finally, a series of well-publicized security incidents had, by the summer of 2003, led Energy Secretary Spencer Abraham to direct NNSA to aggressively and broadly improve nuclear security.

1.2 APPROACH

Against this background, NNSA Administrator Linton Brooks established two groups to assess long-range issues affecting security management and protection.[4] The first study analyzed the federal security workforce;[5] this study, broader in scope, examines a multitude of factors that affect NNSA's security program.

For the past 18 months, we have independently reviewed security at NNSA sites. This report describes our analysis, summarizes our findings, and recommends ways to improve NNSA's security. We interviewed professionals who directly manage and indirectly support the security programs throughout the NNSA complex, including those at Los Alamos, Pantex, Oak Ridge, Livermore, Sandia, Nevada, and Savannah River and DOE and NNSA headquarters. We also reviewed past reports and numerous other documents relating to the nuclear security pro-gram and received briefings on topics germane to this study from responsible officials in DOE and NNSA.

We were given a very broad charter to take a strategic look at how security within DOE/NNSA is organized and structured, the interrelationships between various security disciplines, and the existing security policies, procedures, and practices in place to recommend possible improvements. We were specifically not chartered to look at specific security incidents and individual NNSA organizations in isolation.

[2] The Commission on Maintaining United States Nuclear Weapons Expertise was created pursuant to the National Defense Security Acts of 1997 and 1998 and delivered its report to Congress and the Secretary of Energy on March 1, 1999. The chairman of that commission, retired Navy Admiral Henry G. Chiles Jr., also directed the companion study on nuclear security personnel expertise (see Note 1).

[3] The Commission on Science and Security, chaired by former Deputy Secretary of Defense John J. Hamre, delivered its report, *Science and Security in the 21st Century*, to the Secretary of Energy in April 2002.

[4] National Nuclear Security Administration, "NNSA Announces Security Initiatives for Weapons Laboratories," Press Release, July 8, 2003.

[5] See Note 1.

1.3 REPORT ORGANIZATION

We begin the study by describing the culture of security at DOE and NNSA. We then describe the roles, responsibilities, and relationships of various security organizations and the security policy that governs them. We then discuss, in order,

- cyber systems security;
- counterintelligence;
- site safeguards and security plans, vulnerability assessments, and performance testing;
- protective forces;
- security incidents and inquiries;
- design basis threat implementation;
- security research and development programs;
- nuclear materials and waste storage;
- security resources; and
- security contracting.

We then close with a brief discussion of past studies concerning NNSA security.

Section 2
Culture

2.1 BACKGROUND

Previous studies of DOE have repeatedly criticized its cultural approach to security. In 1999, the President's Foreign Intelligence Advisory Board (PFIAB) found that DOE and the weapons laboratories have a "deeply rooted culture of low regard for and, at times, hostility to security issues."[1] The long-standing culture of the DOE organization affects NNSA security practices at all levels, from the enterprise to the individual.

In February 2002, NNSA's *Report to Congress* detailed the agency's plan to "integrate security and counterintelligence into NNSA Mission Activities."[2] In fact, NNSA has accomplished many of its stated goals in this area, but its culture still reflects many of the long-standing negative attributes of DOE. As a relatively new agency, NNSA has had little time to develop a unique culture, and its semi-autonomous nature makes changing the culture—to institutionalize security as integral to mission and individual responsibility—difficult.

2.2 SUMMARY

NNSA is plagued by a number of cultural problems that, until addressed, will erode its ability to establish and provide security consistent with the gravity of its mission:

- Lack of a team approach to security
- Disparate views and an underappreciation of security across the enterprise, such that security is not fully embraced as integral to mission
- Ingrained organizational relationships that inhibit an enterprise approach to security
- A bias against training
- An over-reliance on a compliance-based approach to security rather than a more balanced approach using performance-based standards

[1] President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.
[2] National Nuclear Security Administration, *Report to Congress on the Organization and Operations of the NNSA*, February 2002.

- Lack of trust in the security organization
- An absence of accountability.

2.3 OBSERVATIONS

2.3.1 Lack of Team Approach

Complex-wide, the views of security are many and varied. The DOE/NNSA white-collar professional and managerial ranks tend to underappreciate it. The security culture in the production environment differs from that of the scientific and research community; production sees security as an integral part of the mission, and the researchers tend to see it as an additional or contracted service. Thus, DOE/NNSA has no team approach to security, instead struggling to succeed in an atmosphere of conflicting viewpoints, e.g., headquarters versus the field, lab versus lab, site office versus contractor, academic versus operational, union versus management, and non-NNSA elements of DOE.

This divisiveness—stemming from the strong cultural identities of the individual sites and lack of team approach—impedes effective security enterprise-wide. This cultural framework is reinforced by the lack of a career development and rotation plan, which promotes remaining in a single organization rather than taking a wider, more diverse range of assignments[3]. As a consequence NNSA tends to view security issues as site-unique rather than addressing their complex-wide implications.

2.3.2 Cultural Opposition

Numerous reports have criticized DOE security management, and repeated attempts at reform have failed or faltered. Congressional micro-management, geographic decentralization, layers of bureaucracy, frequent changes in leadership, low morale, competition among the laboratories and sites, and an inherent tension between the openness of scientific inquiry and need for governmental secrecy have all been cited as contributing causes. However, underlying these factors is the low regard for security—set in a deeply rooted culture of ingrained behavior, attitudes, and values—which has permeated DOE for many years.

The PFIAB report of 1999 saw "a department saturated with cynicism, an arrogant disregard for authority, and a staggering pattern of denial."[4] Elements of that cultural environment persist today and significantly restrict NNSA's ability to institutionalize a different cultural environment, where security is valued as integral to mission.

[3] NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.
[4] See Note 1.

The ingrained cultural environment and long-established organizational relationships within DOE/NNSA inhibit an enterprise approach to security:

- The sites have historically enjoyed significant autonomy and are reluctant to surrender this independence for a more centralized approach. A common saying that reflects this field-to-headquarters relationship is "Negotiations begin when the order is issued."

- The fragmented and stovepiped security process within DOE/NNSA has resulted in a lack of process ownership and accountability, which complicates NNSA headquarters' assertion of centralized authority.

DOE/NNSA has tried to "manage the contract and not the contractor" to avoid micromanagement, but, under this philosophy the organization views its day-to-day oversight responsibility in a narrow contractual frame of reference rather than a broader national security one.

The NNSA-stated philosophy that headquarters will develop the "what" (security policy) and the field will develop the "how" (security policy implementation) reflects both the strong autonomy of the individual sites and NNSA headquarters reluctance to assert a stronger day-to-day oversight role.

The stovepiped culture and lack of sufficiently trained and qualified security professionals (as cited in Chiles report) promotes an overreliance on compliance checklists, rather a broader, more balanced focus on meaningful performance objectives.[5] This culture, and the overly bureaucratic organization, also limits staff members' understanding and appreciation of the broader security program objectives and their role in achieving them.

2.3.3 Bias against Training

A bias against training is evident, stemming from:

- an older workforce that believes training is more appropriate for younger recruits,

- inadequate training budgets,

- poor quality training, and

- lack of training relevance to job assignments.

The Office of Independent Oversight and Performance Assurance (OA) acknowledges the lack of white-collar security training and the need for a "security community."

[5] See Note 3.

2.3.4 Lack of Trust

Employees lack trust that the DOE/NNSA security organization is capable of dealing forthrightly, expeditiously, and responsively with security issues. As a consequence, they have a greater propensity than those in other organizations (such as DoD) to use alternative channels (such as leaking to media or seeking whistle blower protection) as a first course of action, rather than relying on the normal chain of command for resolution.

As noted in the Commission on Science and Security report[6]

> Two competing forces within DOE tear at the delicate fabric of trust among scientists, laboratory management, security professionals, and field and headquarters officials. The first is the inherent tension between the interests of science and the interests of security. The second force is the long-standing tension between headquarters and field elements. Managers and staff at headquarters question whether they can trust the systems that the laboratory directors create. Laboratory directors do not feel that they can always trust headquarters to back them up when security problems arise that could benefit from mutual problem solving…
>
> Trust is reciprocal. Employees need to trust their supervisor to manage a security system that protects them. This entails appropriate verification. Once an individual has earned trust, through the granting of a security clearance, that person should in fact be trusted. Yet that trust must be periodically verified. One must never lose sight of the fact that sometimes trust is misplaced, and the system must be able to effectively handle that inevitability. Trust must be embedded in a system that is designed to deter and prevent betrayal and, failing prevention, that provides for early detection.

2.3.5 Absence of Accountability

Historically, security responsibility within DOE/NNSA has been spread thin and is fragmented. There is no single proponent under the Secretary of Energy who "owns" the security process and ensures consistent application of security standards. Headquarters views security as primarily a field responsibility. Responsibility for security is diffused among a number of stovepiped organizations. This institutionalized fragmentation results in weak integration of security programs and functions. Roles and responsibilities have not been clarified to ensure security is embedded as a line management and individual responsibility. Many line and program managers do not view security as integral to their mission.

[6] Commission on Science and Security, *Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories*, John J. Hamre, Commission Chair, Anne Witkowsky, Project Director, April 2002. Executive summary available from http://www.csis.org/css/ExecSummary.pdf.

Diffused responsibility undermines meaningful accountability. There is a reactionary cultural approach to security which relies on external reviews and audits rather than internal management oversight and critical self-assessment to drive the security agenda. Lack of accountability breeds weak follow-up on identified security deficiencies which in turn breeds further external reviews.

2.4 RECOMMENDATIONS

1. Continue to promote greater collaboration and team building within NNSA with the goal of an enterprise approach to security. Support the Chiles panel recommendations on improved career development, assignment rotation training, professional qualification and certification, etc.[7]

2. Establish a more extensive security training program designed for white-collar professionals.

3. Make an unequivocal commitment to upgrade the quality, relevance, and ownership of security training programs and professional certification.

4. Emphasize a balance of compliance and performance objectives designed to incentivize and embed security improvement throughout NNSA, as part of an enterprise approach to security.

5. Create a stronger climate of trust in the security program. Differentiate honest human security errors from malicious, grossly negligent ones.

6. Adopt a more proactive approach to security through stronger accountability. Promote greater ownership of security through clarified roles and responsibilities, greater emphasis on security in performance assessments, and increased reliance on healthy self-assessment programs.

[7] See Note 3.

Section 3
Roles, Responsibilities, and Relationships

3.1 BACKGROUND

Congress established NNSA in March 2000 as a separately organized semi-autonomous agency within DOE,[1] to maintain and enhance the safety, reliability, and performance of the nation's nuclear weapons; maintain the nation's ability to design, produce, and test nuclear weapons; prevent the proliferation of weapons of mass destruction; and design, build, and maintain naval nuclear propulsion systems.

The enabling statute established a Chief, Defense Nuclear Security (CDNS), reporting directly to the Administrator, to implement security policies directed by the Secretary and Administrator and develop and implement security programs for NNSA. Separately, the Office of Safeguards and Security Programs (NA-55), reporting to the Associate Administrator for Infrastructure and Security, was charged with overall coordination and implementation of NNSA security programs.

In May 2003, NNSA issued its first *Functions, Responsibilities, and Authorities Manual* (FRAM) for safeguards and security (S&S).[2] The manual assigns responsibility to NNSA headquarters, the service center, or site offices for various aspects of S&S policy, oversight, approval, program management, financial management, survey, and training.

On December 4, 2003, DOE established a new Office of Security and Safety Performance Assurance (SSA), which reports directly to the Secretary and develops and implements the Department's S&S policies.[3] DOE tasked SSA with working closely with NNSA,

- through the Office of Security Policy (SO), to ensure that NNSA security policies align with Department security policies, and

[1] Title 32 of the National Defense Authorization Act for Fiscal Year 2000 (Public Law 106-65) created NNSA. The National Defense Authorization Act for Fiscal Year 2001 (PL 106-398) amended Title 32 to require additional information on NNSA's organization, planning, program-ming, and budgeting.

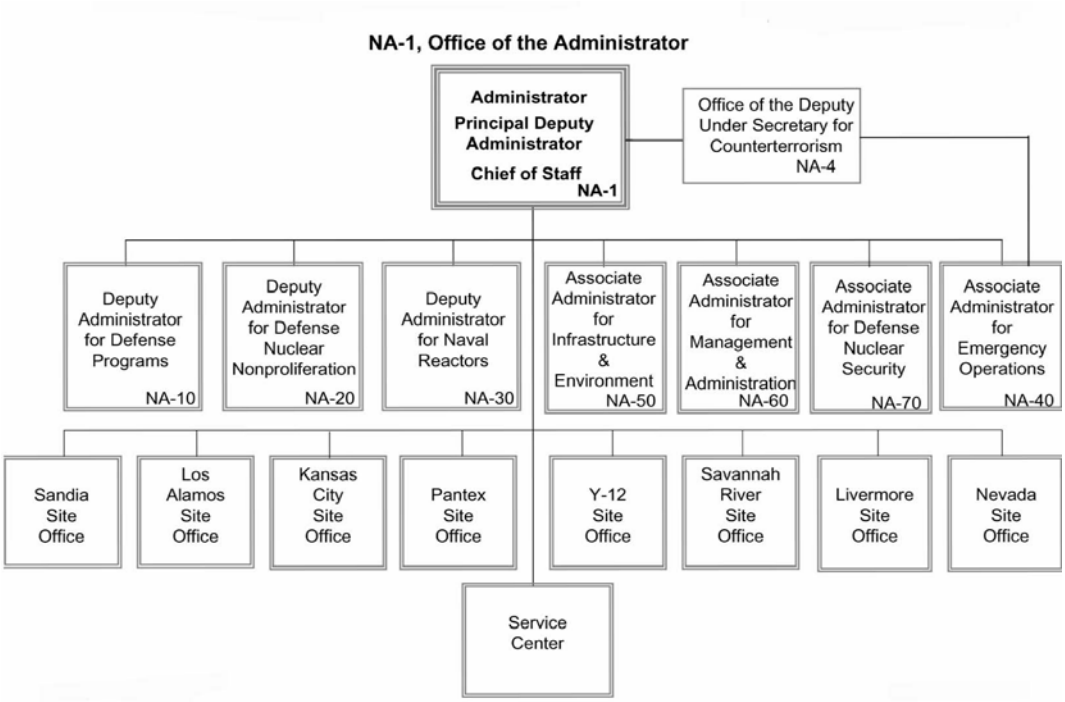
[2] National Nuclear Security Administration, *Functions, Responsibilities and Authorities Man-ual*, May 2003; Change 1, August 2003.

[3] U.S. Department of Energy, "DOE Establishes Office of Security and Safety Performance Assurance for Effective Implementation of Safeguards & Security Policies," *Press Release*, December 2003. Available from http://www.energy.gov/engine/content.do?PUBLIC_ID=14545&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE.

- through the Office of Independent Oversight and Performance Assurance (OA), to continue the independent oversight of NNSA's S&S, cyber security, environment, safety and health, and emergency management pro-grams.

In June 2004, during this study, the Administrator consolidated the CDNS and the NA-55 NNSA security functions into one office under the management of a new office of Associate Administrator for Defense Nuclear Security (NA-70). The cyber security function moved from the former NA-55 to the Office of the Chief Information Officer (NA-65). Figure 3-1 shows the new NNSA organization.

Figure 3-1. NNSA Organization



3.2 SUMMARY

The small size of the NNSA organization greatly impedes its effectiveness within the DOE headquarters bureaucracy. Although NNSA has made good progress by consolidating security functions, responsibility for security as a process is still fragmented and, along with authority and accountability for security, is not adequately embedded in individual and line management responsibilities. Until recently, staffs were organizationally misaligned. As identified in the Chiles report, security personnel with sufficient certification, training, rotation, and broad experience are lacking.[4]

[4] j NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Inde-pendent Analysis*, Henry G. Chiles Jr. et al., March 2004, pp. 2-3 and 2-4

Security collaboration between DOE/NNSA and DoD and among individual security disciplines is lacking. NNSA headquarters has inappropriately delegated virtually all security oversight, review, and assistance responsibilities to the site offices, effectively divorcing itself from day-to-day oversight.

3.3 OBSERVATIONS

3.3.1 Disparity in Staff Size

As the steward of the nation's nuclear stockpile, NNSA has a heavy responsibility, but the size of its organization is dwarfed by that of DOE overall. The NNSA portion of the FY05 budget request is $9 billion, or about 37 percent of the DOE FY05 budget request of $24.3 billion. However, the NNSA staff size is about 10 percent of DOE's. This disparity greatly impedes its effectiveness within the headquarters bureaucracy. For example, DOE SO and NNSA share responsibility for security policy, but, due to the staff size disparity, SO predominates in policy development. The disparity is even more skewed when one considers the large number of headquarters contractors employed by DOE relative to NNSA. Ironically, despite the current disparity in the staff size, NNSA was in the final phases of a 17 percent workforce reduction during the study period.

Beyond these overall numbers, as identified in the Chiles report, qualified security personnel—with sufficient certification, training, rotation, and broad experience—are lacking. Both headquarters and the site offices lack security depth and competency.[5]

3.3.2 Responsibility Fragmentation

Responsibility for security as a process is fragmented within DOE/NNSA. No single person beneath the Secretary has overall responsibility for the security process from policy formulation to implementation and oversight. Security policy is formulated predominantly outside of NNSA. NNSA headquarters has insufficient qualified people to conduct oversight reviews of site security organizations. As a consequence NNSA relies heavily on OA for support. The lack of security process "ownership" contributes to a lack of accountability within the DOE/NNSA security disciplines. As a result of diffused responsibility, a large DOE headquarters bureaucracy, and a turf-oriented culture, decision-making is often consensus driven, compliance based, and unresponsive.

3.3.3 Organizational Misalignment

The Office of Safeguards and Security Programs (NA-55), since realigned, lacked true line management authority, appropriate security expertise, and meaningful security responsibility. This organizational alignment did not serve

NNSA well and inhibited the day-to-day awareness of key security issues and concerns among senior DOE/NNSA decision makers. Elevating NA-55 to the Associate Administrator for Defense Nuclear Security (NA-70) is a step toward achieving increased NNSA security staff access and influence with senior DOE/NNSA leadership.

As discussed in Section 5, the head of NNSA cyber security was inappropriately assigned to NA-55 under the physical security experts rather than working directly for the NNSA CIO equivalent. This organizational alignment inhibited the development and integration of cyber security policies and implementing guidance with information technology policies.

3.3.4 Decentralized and Inadequate Oversight

NNSA headquarters has inappropriately delegated virtually all security oversight, review, and assistance responsibilities to the site offices, effectively divorcing itself from day-to-day oversight. The FRAM assigns an overwhelming majority of oversight functions—123 of 165—to the site offices; however, the site offices generally do not have enough appropriately qualified or certified personnel to perform this function effectively.

NNSA's ability to exercise comprehensive, day-to-day security oversight—to monitor security policy implementation, provide critical guidance and advice, assist in the identification of deficiencies and initiation of corrective action, and promulgate lessons earned and best practices across the enterprise—is problematic for a number of reasons:

- Security expertise is lacking at all levels of the oversight process.[6] Personnel with limited security experience and expertise accomplish much of the day-to-day oversight. For example, NNSA headquarters does not have sufficient oversight expertise for protective force, material control and accountability vulnerability assessments (VAs), and personnel security.

- As highlighted in a 1998 report, the oversight of nuclear weapons security is "a shared responsibility which encompasses numerous assumptions, offices, and echelons of management."[7] This diffused responsibility creates confusion and results in a lack of clear authority and accountability. For example, NNSA headquarters and many managers say that responsibility for site security oversight rests with OA. In reality, that office has little if any direct responsibility, authority, and accountability for day-to-day supervision of the NNSA complex. Its principal role is one of

[5] See Note 4.
[6] See Note 4.
[7] President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf

periodic independent performance assessment. Although independent oversight is a necessary, integral function of NNSA's security organization, it is only a small part of an effective approach to security oversight. Other NNSA line managers believe that site oversight responsibility rests with the local site S&S offices and don't see security as integral to their supervisory responsibilities.

- The NNSA philosophy of centralized guidance and decentralized execution has evolved into a narrow interpretation of responsibilities described as, "headquarters does policy, and the field does implementation." NNSA has advocated decentralized day-to-day oversight without sufficient de-centralized resources. In effect, under this approach, NNSA has surrendered its responsibilities for day-to-day oversight to the field, which is inadequately manned and qualified to perform that function consistently and effectively. Additionally, the lack of centralized clarification of policy interpretation and centralized guidance on policy implementation impedes an enterprise-wide approach to security.

- The oft-quoted DOE/NNSA philosophy, "Manage the contract and not the contractor," has been narrowly interpreted by many NNSA officials to limit their oversight responsibilities to those of contract administrators.

- As a result of numerous outside influences (such as congressional mandates and independent reports), oversight responsibilities have been routinely realigned and modified. This regular restructuring has inhibited the maturation of cohesive oversight processes. For example, the effectiveness of the new Albuquerque Service Center has been hindered by "absentee leadership" (several key positions filled by people who do not reside in Albuquerque) and the unwillingness of employees of the field offices being disestablished to accept new positions and relocate to Albuquerque.

- Some oversight processes have been discontinued or fallen into neglect. For example, DOE's site safeguards and security plan (SSSP) validation and verification (V&V) process has been discontinued, so contractor vulnerability assessments (VAs) do not receive an independent external review. In addition, until recently, NNSA lacked sufficient resources to review the sites' incident reports of concern and verify appropriate corrective actions.

Effective oversight consists of several interdependent elements:

- Day-to-day line management oversight

- Periodic or continuous annual self-assessment survey programs

- Independent oversight.

These elements are intended to operate synergistically. In practice, however, they do not:

- Day-to-day NNSA oversight is lacking as described above
- NNSA guidance is vague on the administration of self-assessment programs. As a consequence, NNSA self-assessment programs vary widely in concept and quality. Self-assessment reports range from none to comprehensive. At present the safeguards and security self-assessment program can be characterized as marginally effective at most sites.
- The survey program has not lived up to its envisioned role. As federal and contractor staffs have been downsized, support for survey programs have diminished. The quality of both surveys and the analytical review of corrective actions have suffered. As a result, analysis of the root cause of deficiencies is often ineffective and corrective actions often address only the most obvious symptoms rather than correcting the underlying fundamental weaknesses. Weak survey programs tend to breed weak self-assessment programs.

3.3.5 Lack of Collaboration

Security collaboration between DoD and DOE/NNSA is lacking, despite the recommendations of a comprehensive independent review.[8] No formalized, established mechanisms exist for sharing security lessons learned, best practices, technological improvements, tactics, and procedures among the security organizations of the two departments.

Individual security disciplines—physical, cyber, personnel, material control and accountability (MC&A), intelligence, and counterintelligence—are not well integrated into a cohesive security program. Conceptually, the benefits of seamless integration are readily apparent. In reality, the various security disciplines do not sufficiently collaborate, despite their growing interdependence, and no single body within DOE oversees and integrates them. The lack of collaboration and cooperation, often results in uncoordinated, inconsistent, and, in some cases, vague or conflicting guidance.

The quality panel system, established to ensure maximum field element participation in and input to DOE security policy, is not effective. In general, there are too many panels (25 as of June 2004) for the sites to support, and the system has become excessively bureaucratic. The leadership of some panels is viewed by some members as “tyrannical.”

Field assistance visits, which offered sites the opportunity to obtain policy clarification and other assistance from headquarters in a non-inspection format, have lain dormant for a number of years.

3.3.6 Lack of Individual and Line Management Responsibility, Authority, and Accountability

Responsibility, authority, and accountability for security are not adequately embedded in line management responsibilities. Security is not viewed as a mission-integral responsibility. In NNSA headquarters, the two principal program deputy administrators (NA-10 and NA-20) do not have significant direct responsibility for security, although they control almost all of the nuclear weapons program re-sources.

Additionally, many site, line, and program managers lack clearly delineated individual responsibilities for security. As a result, security is not viewed as an integral part of their mission, but rather as a service that others provide. Several factors contribute to this perception:

- The FRAM only focuses on safeguards and security staff and does not assign any significant security responsibilities to line and program managers.
- The fact that security is treated as a separate, direct-funded line item, administered separately from the stockpile stewardship programs also reinforces the perception that security is not integral to the programs and is often seen as a resource competitor.

In general, security falls into two categories: security common to all programs in a given facility (such as site perimeter security) and program-unique security. Line and program managers do not have sufficient responsibility for the program-unique elements of security. This separation of responsibility often impedes the ability of line and program managers to make appropriate resource allocation decisions to effectively administer their programs. Programs are often delayed because of security-related issues that line and program managers are not empowered to influence.

The Integrated Safeguards and Security Management (ISSM) program, was implemented in March 2001 for all NNSA federal and contractor offices and sites. The ISSM program was patterned after the successful Integrated Safety Management (ISM) program. As such, ISSM was designed to include core values and principles and rely on line management ownership of safeguards and security within their work scope, as well as individual employee commitment to conducting all work in a secure manner. ISSM was clearly intended to embed security as an individual responsibility; however ISSM was "stillborn." It has not been institutionalized into day to day management or embraced as an individual responsibility.

[8] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System* (U), Final Report, April 2002 (Secret).

3.4 RECOMMENDATIONS

1. Conduct an independent staffing assessment of NNSA relative to DOE. Rebalance staffing and expertise commensurate with the significance of the national security assets NNSA manages.

2. Give greater autonomy and authority to the NNSA Administrator to oversee the elements of the security process, from policy formulation to implementation and oversight, which directly affect security of the NNSA complex.

3. Implement the recommendations of the Chiles report to improve the federal security workforce, including developing and executing a comprehensive human capital management program; improving the training, qualifications, and stature of the NNSA security workforce; reengaging in national markets to hire security professionals; instituting a long-term practice of security staff rotation; identifying options for accelerating the security clearance process; improving security information flow; revising the *NNSA Safeguards and Security Strategic Plan*; and providing specific budget support for and tracking the progress of these recommendations.[9]

4. Continue to elevate security program visibility and importance through initiatives such as the June 2004 organizational realignment, to ensure security is commensurate with other line management responsibilities.

5. Have NNSA headquarters assume greater responsibility for day-to-day supervision and oversight of site activities to promote an enterprise-wide approach to security, more consistent interpretation of security policy, and more standardized and coherent implementation. The new Associate Administrator for Defense Nuclear Security should be assigned responsibility for day-to-day security oversight. Responsibility for implementation needs to reside at all levels.

6. Establish formal mechanisms to enable DOE/NNSA to regularly collaborate with DoD (and other appropriate federal agencies) on security policy issues, lessons learned, best practices, technological improvements, tactics, and procedures as recommended by a previous study.[10] This collaboration should be more frequent and at lower management levels than [REDACTED] the current guidance requires. The Nuclear Weapons Council may be an appropriate organization to sponsor this activity.

7. Establish forums and procedures to promote greater coordination and collaboration among the various security disciplines, such as the following:

[9] See Note 4.
[10] See Note 8.

- Consider establishing a security "board of directors" comprising NNSA prime security contractors and like-asset protection experts.

- Add to the responsibilities of the existing management council a requirement to convene periodic meetings to address security concerns. These meetings should include SSA, Counterintelligence (NNSA and DOE), Intelligence, CDNS, and the Cyber Security Manager.

- Consider establishing a DOE/NNSA security panel at headquarters and each NNSA site that requires key leadership representatives from physical security, cyber security, counterintelligence, and intelligence, as appropriate, to meet regularly to share knowledge and coordinate activities.

8. Embed greater security planning and programming responsibilities in the two Program Deputy Administrators (NA-10 and NA-70), for example, development of plans for consolidation of special nuclear material (SNM). Consider promoting greater line and program manager accountability for security by establishing a direct funding line to integrate the resourcing of program-unique security elements with their respective programs.

9. Streamline the quality panel system; reduce the number of panels, establish more discipline and a well-defined focus, and increase higher management participation to reduce bureaucracy.

10. Revitalize the ISSM program. (The NNSA Administrator has already taken action to implement this initiative.)

11. Promote greater reliance on continuing security self-assessment programs to better inculcate security as every individual's responsibility and integral to mission. Consider changing the annual survey and self-assessment program to a year-round program of in-depth assessments in specific areas.

Section 4
Security Policy

4.1 BACKGROUND

In May 2002, NNSA defined a formal system for development and codification of its policy, directives, and business management practices.[1] This policy letter system codifies how NNSA establishes policy and provides direction and guidance to all elements. The system establishes new policy for directives unique to NNSA, supplements or indicates how NNSA will cost-efficiently implement a departmental directive, and provides business and operating guidance. NNSA policy letters include directives, policy letters, and business and operating policy (BOP) letters.[2] The former describe "what" will be done, and the latter describe "how."

DOE develops and communicates its policies, requirements, and responsibilities throughout the Department by means of its directives system. The system informs, directs, and guides employees in the performance of their jobs, enabling them to work effectively within the Department and with agencies, contractors, and the public.[3] The five general types of directives are policies, orders, manuals, guides, and notices.

DOE Order 470.1 establishes the responsibilities, authorities, and requirements of the DOE Safeguards and Security Program.[4] Draft 470.1A, which has been distributed for review and comment, requires the Director, Office of Security, to establish "security policies, requirements, standards, and guidance, including the DOE Design Basis Threat (DBT) for use in designing and implementing the safeguards and security programs."

DOE vets policy by two methods—the Field Management Council (FMC) and the Review and Comment (RevCom) Process—before finalizing and distributing it:

- The FMC issues policy that has to get out to the field quickly. Since 1999, the FMC has taken 481 actions, 15 to 20 percent of which are security related. Although the actual council has not met since the Clinton Administration, DOE still employs the review process, which involves field sites and headquarters elements.

[1] NNSA defined this system under the authority of Section 3212(b)(2) of Public Law 106-65, the National Defense Authorization Act for Fiscal Year 2000.
[2] As of June 2004, NNSA had issued nine directives policy letters and eight BOP letters.
[3] U.S. Department of Energy, Office of Management Communications, "Department of Energy Directives Checklist," *Directives, Regulations, and Standards,* August 2004. Available from http://www.directives.doe.gov/cgi-bin/currentchecklist#POLICY.
[4] U.S. Department of Energy, *Safeguards and Security Program*, DOE Order 470.1, September 1995.

- RevCom is the DOE coordination system for the development of administrative directives.[5] DOE employees and prime contractors use the system to comment on draft directives.

A July 2002 working group report stated,

> The Department's current coordination process is considered unnecessarily elaborate and bureaucratic by directives owners and customers. The group determined that the directives processed through the directives system during 2001 took an average of 295 days to coordinate and pro-vide the Deputy Secretary with a final directive for approval.[6]

In part, on the basis of this report, DOE's Office of Security and Safety Performance Assurance (SSA) is streamlining the Department's security policy. In March 2004, the Office of Management, Budget and Evaluation (ME) issued for comment a 1200-page draft on streamlining, and it plans to issue the final in fall 2004.[7]

4.2 SUMMARY

The NNSA enterprise lacks a comprehensive strategic security plan. Policy collaboration is lacking: between DOE and DoD, internally within DOE/NNSA headquarters, between headquarters and the sites, and among sites. NNSA does not have adequate staffing to direct policy to the field or facilitate site implementation. In general, security policy is not sufficiently prescriptive and is open to too much individual interpretation in implementation. No effective system is in place for verifying documented security guidance and direction.

4.3 OBSERVATIONS

4.3.1 Lack of Enterprise Vision

The NNSA enterprise lacks a comprehensive strategic security plan that charts a course for the organization, strives to achieve better efficiency and effectiveness in security programs, and provides a unifying vision for the nuclear weapons complex.

[5] U.S. Department of Energy, Office of Management, Budget and Evaluation, *RevCom Re-view and Comment System*, August 2004. Available from http://www.revcom.doe.gov/.
[6] U.S. Department of Energy, DOE Directives System Working Group, Office of Management, Budget and Evaluation, *Report on Streamlining Directives System*, presented to the DOE Management Council, July 23, 2002
[7] ME issued the draft as Official Use Only (OUO), so it is not widely available for comment.

The Department of Energy's Strategic Security Plan is a well written document with 14 specific objectives[8]—divided into near, mid, and long term—with specific strategies designed to achieve desired intermediate goals and long-term outcomes. It also delineates qualitative and quantitative measures of success to assess progress toward meeting these objectives. In contrast, the *NNSA Safeguards and Security Strategic Plan* is more general, consisting of only 4 goals, which lack the specificity and the time frames of those in the DOE plan.[9] Although issued at about the same time, the two plans do not appear to be linked. The stark differences in the plans reflect a lack of collaboration between NNSA and DOE.

Of greater concern, the NNSA sites have adopted neither the DOE plan nor the NNSA plan. The safeguards and security plans of most NNSA sites reflect little linkage to either plan and vary widely in structure and content.

4.3.2 Lack of Collaboration in Policy Formulation and Implementation

Security policy collaboration between DOE/NNSA and DoD is lacking. The two departments differ greatly in their approaches to security policy and implementation.[10] No integrating process or overall management ensures the equivalence of their respective security approaches. At a minimum, the same nuclear weapon or material located within DoD or NNSA should be protected at an equivalent level against an equivalent threat on the basis of the intelligence community's postulated threat. As outlined in Section 10, this is not the case today. Prior drug use policy (peyote, for example) is also not standardized between DOE/NNSA and DoD.

Within DOE/NNSA headquarters, security policy formulation lacks appropriate collaboration. In general, SO formulates security policy, except for cyber security, which either the DOE Office of the Chief Information Officer (OCIO) or NNSA cyber security office formulates separately; collaboration between these offices is minimal. NNSA has little involvement with SO in policy formulation and interpretation, in part because of staffing limitations.

Appropriate security policy collaboration between the DOE/NNSA headquarters and field is also lacking. This has resulted in significant inconsistencies in policy interpretation and implementation throughout the NNSA complex. In recent history, DOE/NNSA had unnecessarily restricted SO from communicating with the field concerning the impact of safety and security policy on its operations. (Increased collaboration resulting from a recent DOE initiative to restore SO communication with the field should improve the formulation and implementation of effective

[8] U.S. Department of Energy, *The Department of Energy's Strategic Security Plan*, March 2003.
[9] National Nuclear Security Administration, *NNSA Safeguards and Security Strategic Plan*, June 2003.
[10] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Con-trol System* (U), Final Report, April 2002 (Secret).

security policy.) The RevCom system also has not been effective as a collaboration tool; the sites perceive that headquarters does not consider their inputs.

Collaboration among sites is also lacking. Most sites perceive that early collaboration in the formulation of security policy is lacking.

Peer review is a critical element of the NNSA scientific process; yet, safety and security appear to be excluded from peer review. Although a number of forums and other groups have focused on security, they have not been effective in promoting meaningful collaboration.

4.3.3 Inadequate Staffing

NNSA does not have adequate staffing to direct policy to the field and to address, clarify, and interpret policy to facilitate site implementation. It also does not have the experience and expertise needed in key security disciplines, such as vulnerability assessments (VAs), to assist the field. Because of staffing limitations, NNSA has little effective involvement in policy formulation and interpretation.

4.3.4 Inconsistent Implementation

NNSA has not provided sufficient clarification and interpretation of security policy to facilitate more consistent site-to-site implementation. In general, security policy is not sufficiently prescriptive and is open to too much individual interpretation in policy implementation. One headquarters employee stated, “Policy which is issued is not the best policy that can be written; it is the best policy that can be negotiated.”

The prevalent philosophy of centralized guidance and decentralized execution, while commendable in purpose, suffers from a lack of centralized collaboration and clarification of policy intent, insufficient decentralized oversight expertise (at the site offices), and lack of enterprise standards and criteria. The abolishment of a previously effective security standards and criteria manual, and decentralized interpretation, undermine consistency of policies. Examples are as follows:

- Security policy on chemical and biological defenses is not well defined, particularly in regard to use of protective suits and gloves, (which at one site at least are still in the warehouse).

- The focus on exit security policy (for items people take or send from a facility) is weak compared with entrance security policy (for items people bring into a facility).

- Sites have differing interpretations of fundamental concepts such as "critical facilities" and "nuclear threat" as discussed in Section 7.

As a consequence, no coherent NNSA-wide security standards and criteria exist and an enterprise-wide vision is lacking.

Local site security policies have proliferated through a reactionary approach to implementing headquarters policies that are subject to wide interpretation. In one site's perspective, "Security policy has 50 years of band-aids; the bureaucratic band-aids have become the problem." This situation has contributed to a compliance-based (checklist) approach to security policy implementation and oversight, rather than a risk-based approach focused on outcomes, which better ties compliance to mission performance.

The DOE security policy streamlining initiative is commendable, but it is still in review. Because the draft streamlining initiative document is OUO, it is not available electronically.[11] The lack of access means fewer staff members can review, comment, and ultimately follow the guidelines.

4.3.5 Documentation

DOE/NNSA has no effective system in place to ensure organizations or staff can verify they hold a complete, up-to-date file of all security guidance and direction. No database or centralized program (other than the quality panels) identifies current supplemental directives for field offices and contractors to ensure that applicable memorandums, order changes, and guidance are followed. No consolidated listing of all effective security policy guidance or direction is available to ensure appropriate accountability.

All DOE security directives are unclassified as a matter of policy (for reasons not fully understood). As a consequence, classified policy guidance or direction (such as the new DBT security requirements) has not been incorporated into the directives system, but issued in the form of policy memorandums or letters.

The SO initiative to consolidate all unclassified policy in CD format, including an umbrella document and seven underlying manuals, is a step in the right direction, but it does not fully integrate cyber security policy or classified policy.

[11] U.S. Department of Energy, *Identifying and Protecting Official Use Only Information*, DOE Order 471.3, April 2003.

4.4 RECOMMENDATIONS

1. Formulate an NNSA-wide strategic security plan, similar in level of detail and content to DOE's, to create a unifying security roadmap for the NNSA enterprise. Use this plan as a cornerstone for the creation of other interdependent enterprise-wide plans, such as special nuclear material consolidation, infrastructure recapitalization, technology investment, information systems modernization, and the foundation for individual security discipline plans (physical, cyber, personnel, and material control and accountability).

2. Establish effective, formal forums to:

   - promote greater DOE/NNSA-to-DOD, DOE-to-NNSA, headquarters-to-site, and site-to-site collaboration between security policymakers and policy implementers,
   - promote more consistent interpretation and application of security policy,
   - foster adoption of best practices,
   - help formulate a more coherent, NNSA-wide security plan,
   - institutionalize the principles of the ISSM initiative in daily practice (the NNSA Administrator has already taken steps to implement this recommendation), and
   - consider making peer review an inherent element of security policy formulation and implementation.

3. Review and streamline local site compliance-based quick fixes to ensure security oversight is appropriately focused on performance objectives.

4. Provide greater centralized clarification and interpretation of security policy to promote more consistent and standardized implementation. Consider repromulgation of a security standards and criteria manual. As part of this initiative:

   - establish more definitive policies for biological and chemical defenses, and
   - better balance entry and exit security policies (both cyber and physical) to deter inappropriate or illegal removal of items from sites as well as entry.

5. Periodically promulgate a consolidated listing of all effective security policy (directives, letters, memorandums, manuals, etc). Consider establishing a single, integrated (unclassified and classified, cyber and physical) directives system with appropriate distribution controls.

6. Consider clarifying the DOE Order 471.3 so that OUO information can be placed on the unclassified network.

7. Reconcile security policy differences with DOD such as the policy on the use of hallucinogenic drugs (e.g. peyote).

Section 5
Cyber System Security

5.1 BACKGROUND

The security of NNSA information systems is an integral element of its mission. The rapid advances in information system technologies and increasing reliance on electronic networks and media call for evolving cyber security policies that ensure adequate management, operational, and technical security controls.

NNSA is operating in a highly interactive environment of powerful computing devices and interconnected systems of systems across global networks. These systems cross a variety of boundaries—both federal and commercial. The complexity of these cross-connected systems and networks presents great security challenges for NNSA.

Much of NNSA information requires some level of protection. Loss or compromise of this information, whether held directly by NNSA or its contractors, could directly affect U.S. economic, environmental, and national security interests. Implementing a broad, comprehensive program of information assurance to satisfy the NNSA information security requirements is critical.

5.2 SUMMARY

DOE/NNSA cyber security policies, procedures, and practices are less mature than their counterparts in other security disciplines. NNSA is resource poor in terms of secure or classified networks and access terminals. Insufficient resources have been devoted to address many of its cyber security issues, particularly the insider threat. Cyber security implementation varies widely throughout NNSA because of the lack of an enterprise approach, inadequate funding, insufficient cyber security personnel and expertise, and inadequate collaboration among DOE and NNSA cyber security organizations. Cyber security is not sufficiently integrated with other security disciplines, such as physical, personnel, material control and accountability, counterintelligence, and intelligence. This stovepipe approach to security has hindered the development of a more comprehensive coordinated approach to securing NNSA information assets.

5.3 OBSERVATIONS

NNSA lacks sufficient classified voice (STU 3-like) and data (SIPRNet-like) network access terminals; thus, personnel transmit a large volume of very sensitive information via mail or unclassified networks, with only the key elements (which would make the information classified) removed. Significant potential vulnerabilities result from:

- outsider access to a large volume of sensitive, though unclassified, data, which can create a classified "mosaic," and

- inadequate secure voice and data network access terminals which force people to use unclassified media to address sensitive, though unclassified, matters or talk around classified subjects.

In general, DOE/NNSA cyber security has focused almost exclusively on network perimeter security (such as firewalls and intrusion detection), leaving inadequate cyber security safeguards against the insider threat. Sufficient resources have not been committed to internal security controls and monitoring to both deter and detect inappropriate activities; periodic performance assessments have primarily evaluated perimeter security at the expense of internal security controls.

Despite NNSA Policy Letter (NAP) 14.1,[1] which defines the NNSA Cyber Security Program, implementation varies widely across NNSA, perpetuated by a lack of consistent minimum standards, wide differences in policy interpretation by individual sites, and lack of collaboration among sites. Site-level cyber security program plans radically differ from each other due to this lack of standardized criteria. A lack of standardization inhibits an enterprise-wide approach to cyber security. As one consequence, NNSA has not comprehensively assessed the risk to its information systems end to end as required by FISMA.

Federal staffing of cyber security positions within NNSA is inadequate. At present, only two employees and two contractors in NNSA headquarters, supplemented by very limited cyber security expertise at each site, are responsible for day-to-day cyber security. Several sites have an extremely low level of federal cyber security expertise relative to the sensitivity of their mission.

DOE/NNSA lacks an effective cyber security training and qualification program. Many federal and contractor cyber security personnel lack IT security professional certifications, such as CISSP, CISM, and GSEC.[2] Additionally, many line and program managers are unfamiliar with the basic elements of an effective cyber security program.

DOE/NNSA lacks a consolidated, accurate inventory of their information systems. While some information systems are known to lack certification and accreditation, the accreditation of others is questionable in light of the professional qualifications of the site accrediting officers.

[1] National Nuclear Security Administration, NNSA Policy Letter 14.1, *Cyber Security Pro-gram*, September 2003.
[2] CISSP = Certification for Information System Security Professional; CISM = Certified Information Security Manager; and GSEC = Global Information Assurance Certification (GIAC) Security Essentials Certification

NNSA cyber security is not sufficiently integrated with other security disciplines, such as physical, personnel, material control and accountability, counterintelligence, and intelligence. Accordingly, determining whether the resource allocation between cyber and the other security disciplines is appropriately balanced to en-sure the highest priority vulnerabilities are being addressed is difficult. For example, some cyber security personnel perceive that their inputs were ignored during budget preparations because of overriding concerns with physical security funding.

Collaboration between NNSA and DOE headquarters in setting cyber security policy is lacking. As a consequence, the policy is fragmented and inconsistent. For example:

- DOE/NNSA has no standardized cyber security architecture or standards and criteria
- There is virtually no collaboration between NNSA sites and the DOE Cyber Security Office. (Although legislation prevents a DOE officer from directing an NNSA officer, it does not preclude collaboration.)
- The NNSA initiative to establish the cyber equivalent of a design basis threat (DBT) is a positive step. However, DOE has yet to accept or adopt this "cyber DBT" approach to the rest of the department
- The Office of Environmental Remediation and Waste Management (EM) and NNSA cyber security policies are not fully consistent.

Cyber security incident reporting policies have not been adequately integrated into the incidents of security concern program. At present, no meaningful metrics are available to NNSA leadership to monitor and assess cyber security performance.

In the NNSA scientific and research community, cultural resistance to implementation of, and adherence to, individual cyber security policies (such as configuration control, patch management, and root access control) is long-standing and unresolved.

Field cyber security personnel perceive the new cyber security directives, NAPS 14.1–14.11, as increasing the administrative workload with little corresponding increase in security protection.

NNSA cyber security management does not have a seat on key cyber security forums, such as the following:

- Committee on National Security Systems (CNSS), http://www.nstissc.gov/
- Information Assurance Technical Framework Forum (IATFF), http://www.iatf.net/
- The Center for Internet Security, http://www.cisecurity.org.

No one in DOE/NNSA headquarters is qualified and certified as a transient electromagnetic pulse surveillance technology (TEMPEST) technical authority to direct the telecommunication security programs for TEMPEST, communications security (COMSEC), and protected distribution systems (PDS).

5.4 RECOMMENDATIONS

1. Expand classified voice and data network access terminals throughout NNSA. Shift sensitive information to secure networks to the maximum ex-tent possible.

2. Devote more emphasis and cyber security resources to the insider threat. Implement an internal NNSA-wide network architecture and security policies, including:

   - more robust identification, authentication, and access controls
   - more robust audit trail, auditing, and archiving capabilities
   - automated patch management
   - 24×7 staff to monitor for abnormal and unusual network activity
   - improved security awareness, training, and education
   - improved contingency and incident response capability.

   In addition, expand the independent verification and validation program and performance assessment programs to better evaluate cyber safeguards against the insider threat.

3. Develop more consistent standards, guidelines, and procedures to promote a more integrated, comprehensive, uniform implementation of cyber security policies across the NNSA complex, including:

   - formulation of an enterprise cyber security program plan

- development of an enterprise architecture that encompasses all NNSA networks.

4. Assess NNSA's cyber security program end to end to clearly establish the interrelationships of information technology assets, threats, vulnerabilities, and safeguards.

5. Increase the number and professional qualifications of federal cyber security personnel across the NNSA complex. Require key federal and con-tractor cyber security personnel to achieve certain IT security professional certifications before or as part of their assignment to critical positions.

6. Require screening of all sensitive network system administrators as part of the Human Reliability Program.

7. Establish a white-collar cyber security training program to appropriately train key line and program managers.

8. Develop a comprehensive, accurate inventory of information systems and validate their certification and accreditation status. In the absence of appropriate site accreditation expertise, NNSA should centralize network accreditation to promote greater uniformity in information assurance and explicit acceptance of risk across the NNSA complex.

9. Better integrate cyber systems security with other security disciplines (as addressed in Section 3).

10. Establish a cyber security policy panel in DOE/NNSA headquarters to improve the consistency, specificity, and adequacy of cyber security policies within NNSA.

11. Fully integrate cyber security incident reporting into the incidents of security concern program and establish meaningful metrics to enable leader-ship to monitor and assess the NNSA cyber security program performance.

12. Encourage DOE to adopt the NNSA cyber DBT initiative and continue to refine this approach.

13. Increase NNSA's national-level visibility of national level information security issues through assignment of NNSA cyber security representatives as DOE representatives to the following forums (and others as appropriate):

- Committee on National Security Systems (CNSS), http://www.nstissc.gov/

- Information Assurance Technical Framework Forum (IATFF), http://www.iatf.net/

- The Center for Internet Security, http://www.cisecurity.org.

14. Establish a position within NNSA for a certified TEMPEST technical authority to support the NNSA chief information officer (CIO) and cyber security manager.

.

Section 6
Counterintelligence

6.1 BACKGROUND

As the repository of the crown jewels of our nation's nuclear secrets, the NNSA complex will continue to be a major target of foreign (friendly as well as hostile) government and terrorist collection activities.

The National Defense Authorization Act for fiscal year 2000 established the NNSA and, with it, an Office of Defense Nuclear Counterintelligence (ODNCI). The act also codified the existence of the DOE Office of Counterintelligence (OCI). For approximately a year following enactment, the Director, OCI, also served as Chief, ODNCI. Subsequent congressional action prohibited these dual responsibilities, and, as a result, the Secretary appointed a Chief, ODNCI, in October 2000.

Thereafter, DOE and NNSA tried to establish a clearly defined working relationship between the two counterintelligence offices, culminating in a secretarial policy memorandum.[1] The counterintelligence organizational concepts embodied in the memorandum established the two managers and a shared headquarters program staff approach, with DOE/OCI managing counterintelligence activities at DOE sites, and NNSA/ODNCI managing counterintelligence activity at NNSA sites.

The Secretary recently notified congressional committees that he wants to combine the two programs into the Office of Counterintelligence, within DOE, reporting directly to him. The congressional legislative process will determine the outcome of this proposal.

6.2 SUMMARY

The DOE/NNSA counterintelligence (CI) program suffers from a dysfunctional relationship between OCI and ODNCI, insufficient collaboration with the other security disciplines, lack of a proactive approach to protection of information, and insufficient emphasis on the insider threat. CI budget allocations do not appear to be aligned with program priorities. Finally, performance objectives designed to promote CI initiatives to deter, prevent, and preempt espionage activities are lacking.

[1] U.S. Department of Energy, memorandum from Bill Richardson, Secretary of Energy, to John T. Conway, subject: *Providing Revision 1 of the 2000-1 Implementation Plan*, January 19, 2001.

6.3 OBSERVATIONS

6.3.1 Counterintelligence Organization

The relationship between OCI and ODNCI is dysfunctional. Both the OCI and ODNCI managers agree that the offices should be combined. Coordination and collaboration among DOE/NNSA counterintelligence officials and DOE/NNSA intelligence and security officials is insufficient. For example:

- OCI has issued a large number of intelligence information reports to the intelligence community without coordination with ODNCI or the DOE Intelligence Office.
- OCI and ODNCI have not been adequately involved in red-teaming activities in the vulnerability assessment (VA), performance testing, and site safeguards and security plan (SSSP) processes to help NNSA sites:
  - assess how potential adversaries could exploit information, particularly from open sources, to plan attacks against site assets;
  - identify and mitigate vulnerabilities; and
  - improve the quality of protection strategies reflected in VAs, performance testing, and SSSPs.
- OCI and ODNCI were not adequately involved in the iterative site analysis (ISA) process.
- Most security and intelligence people interviewed criticized the counterintelligence program as a one-way receptor of information.

6.3.2 Counterintelligence Approach

DOE takes a reactive, investigation-based approach to counterintelligence rather than having a broad, comprehensive, and proactive philosophy designed to prevent, deter, and preempt foreign intelligence collection and espionage activities. The principal purpose of the counterintelligence program should be the protection of DOE/NNSA information rather than the successful prosecution of people who engage in activities on behalf of a foreign government or terrorist group. The existing approach narrowly focuses on investigating potential illegal activity and has as a principal measure of program success the number of active investigations open.

The existing program does not sufficiently emphasize protecting DOE information from the insider threat. For example:

- Red-teaming initiatives to determine how a potential insider threat could do the most damage to national security, prioritize potential vulnerabilities, and develop protection strategies are weak to non-existent.
- Polygraphs, computer searches, and other analysis and inspection techniques are not adequately utilized in a random (or even targeted) manner to serve as a deterrent.
- The counterintelligence program lacks sufficient cyber security expertise at headquarters to adequately oversee IT-based counterintelligence activities against the potential insider threat.

6.3.3 CI Resources

In general, the sites perceive that DOE/NNSA has devoted insufficient resources to a CI strategy of "defense in depth" which DOE envisions. The three nuclear weapons laboratories are specifically concerned with a "systemic failure to align CI budget allocations with program realities" and the inadequacy of budgetary resources allocated to their resident CI programs.[2]

6.3.4 Performance Measures

The counterintelligence *Program Inspection Standard* is very compliance oriented and does not adequately focus on performance objectives designed to deter, pre-vent, and preempt foreign government or terrorist espionage activities.[3]

NNSA lacks an enterprise-wide approach to contractor counterintelligence performance measures. The FY04 counterintelligence performance measures ODNCI delineated vary widely in both detail and scope among the NNSA maintenance and operations (M&O) contractors without appropriate justification. Federal site managers have apparently been given wide latitude in the formulation of performance measures, which are incorporated into the performance evaluation of the M&O contractors. The wide variation in counterintelligence contractor performance measures reflects both a lack of collaboration among NNSA federal site managers and a lack of centralized guidance from DOE/NNSA headquarters.

[2] Letter, from G. Peter Nanos et al, Laboratory Directors, to Kyle McSlarrow, Deputy Secretary, October 10, 2003.
[3] U.S. Department of Energy, ODNCI, *Program Inspection Standard*, March 2002. We understand that this standard is being revised.

Counterintelligence performance metrics focus almost exclusively on quantitative measures—such as the percentage and number of people receiving awareness training, percentage and number of intelligence information reports (IIRs) issued, and, particularly, the number of active investigations—as the measures of pro-gram success, without equivalent focus on the quality or effectiveness of those elements.

6.4 RECOMMENDATIONS

1. Reunify the OCI and ODCNI organizations in a single office. Because the preponderance of vital national security information foreign governments and terrorist entities seek from DOE resides within NNSA—and because of the gravity to national security of the loss of nuclear weapons information—strong consideration should be given to a merged office working directly under the NNSA Administrator.

2. Adopt a broader, more comprehensive, and proactive counterintelligence approach that gives primacy to deterring, preventing, and preempting foreign intelligence and terrorist espionage activities over investigation and prosecution of offenders.

3. Place greater emphasis on the insider threat through increased:

   - red-teaming to assess and prioritize potential internal vulnerabilities,
   - use of surveillance techniques (such as polygraphs and computer searches) to serve as a deterrent, and
   - cyber security expertise within the NNSA headquarters counterintelligence offices.

4. Improve coordination and collaboration among counterintelligence, intelligence, and various security disciplines across the NNSA complex to better integrate counterintelligence in red-teaming security activities, such as the ISA, VA, performance testing, and SSSP processes. Devote more resources to analyzing open-source information from potential adversaries' perspectives. Coordinate IIRs with the DOE Intelligence Office before their submission.

5. Independently validate the allocation of CI resources to ensure scarce resources are focused on the areas of greatest risk to national security.

6. Standardize the counterintelligence performance measures where appropriate for M&O contracts across the NNSA enterprise.

7. Develop counterintelligence performance metrics that enable DOE/NNSA leadership to better evaluate the quality and effectiveness of program elements

as well as quantitative measures. Add qualitative performance-related objectives to the counterintelligence program inspection standard to subjectively evaluate initiatives to deter, prevent, and preempt espionage activities.

Section 7
Site Safeguards and Security Plans, Vulnerability Assessments, and Performance Testing

7.1 BACKGROUND

The effectiveness of NNSA protective systems is supposed to be formally and regularly examined through the conduct of vulnerability assessments (VAs). A VA is a systematic evaluation process in which qualitative and quantitative techniques are applied to identify vulnerabilities and arrive at effective protection of specific assets, such as special nuclear material (SNM). To conduct such assessments, DOE uses a number of different DOE-developed VA software programs, tabletop analyses, and performance testing.

The results of these assessments are documented at each site in a classified document known as the site safeguards and security plan (SSSP). In addition to identifying known vulnerabilities, risks, and protection strategies for the site, the SSSP formally acknowledges how much risk the contractor and DOE are willing to accept.

The SSSP process, including the VA and performance-testing programs, serves as the foundation for protection of weapons and weapon grade materials in NNSA. These plans define risk to the most critical NNSA assets, influencing site protective posture and directly affecting the resources and funding allocated across the complex. Site-specific limited scope performance tests and force-on-force exercises help identify risks and influence the accuracy of VAs.

7.2 SUMMARY

A number of factors—the shortage of experienced VA analysts, increase in work-load resulting from the new design basis threat (DBT), lack of a comprehensive VA training program, overreliance on a few VA tools, and lack of a rigorous, institutionalized VA approach—detract from the validity and consistency of VAs across the NNSA complex. In addition, weaknesses and wide variations in SSSP limited scope performance testing and force-on-force exercises distort physical security assessments across the complex, promote a false sense of security in selected areas, and complicate prudent allocation of security resources to address potential vulnerabilities.

7.3 OBSERVATIONS

7.3.1 Vulnerability Assessments

INADEQUATE STAFFING AND SKILLS

NNSA has a shortage of VA analysts because of retirements, exits to consulting and higher-paying positions, reserve duty activations, and other reasons. Increased workload—stemming from the modified DBT, additional targets, VA policy changes, and analysis of security upgrades—exacerbates the shortage problem.

The experience and skills of VA analysts vary widely. The cadre of experienced, expert personnel available in NNSA to perform VAs is very small, so VAs are often performed by less experienced analysts, delayed, or not performed at all. As a consequence, sites are submitting budgets for costly security upgrades without the benefit of completed VAs, which can result in inadequate upgrades, upgrades exceeding needs, and inappropriate funding amounts.

DOE/NNSA does not have a mature, comprehensive VA training program. VA analysts new to the process are expected to make major decisions on system effectiveness and upgrades. In addition, they need training for numerous different responsibilities, including modeling that uses as many as a dozen different software programs.[1] Although the recent effort to train VA analysts complex-wide is a step in the right direction, its success hinges on a well-defined, institutionalized approach, which DOE/NNSA lacks.

At individual sites, the number and expertise of VA personnel is inconsistent with the work scope. For example, one site, which has only two inexperienced VA analysts, has more work than another site, which has 10 experienced VA analysts. These two analysts will have difficulty meeting the VA milestones required to support major construction projects, DBT implementation, and other needs.

INAPPROPRIATE RISK ASSESSMENT

Some NNSA sites are not appropriately assessing security risk. The *NNSA Safeguards and Security Strategic Plan* calls for revising VAs and SSSPs to ensure consistency with the new DBT, and it cites updated VAs, SSSPs, and site security plans (SSPs) as an indicator of success.[2] However, the risk associated

[1] These include Analytic System and Software for Evaluating Safeguards and Security (ASSESS), Joint Conflict and Tactical Simulation (JCATS), Joint Tactical Simulation (JTS), Adversary Timeline Analysis System (ATLAS), ASSESS Query Tool, Access Knowledge Database System (AKDBS), Antiterrorist (AT) Planner, radiological dispersal programs, chemical and bio-logical weapon (CBW) software, and blast effects software, such as Blast Effects Estimation Model (BEEM), Explosive Effects Analysis Software (Blast FX), Blast Effects for Internal Detonations (Blast X), and Conventional Weapons Effects (ConWep)

[2] National Nuclear Security Administration, *NNSA Safeguards and Security Strategic Plan*, June 2003, p. 4.

with some VAs does not reflect current operations because the VAs are based on future security upgrades that are not yet operational or an SSSP has not been recently writ-ten, approved, and submitted. At some sites, VA analysts have submitted vulnerability assessment reports (VARs) to site offices based on a number of security upgrades that have not yet been implemented and with risk inappropriately defined as if these upgrades were fully operational.[3] Some site offices have inappropriately accepted risk on the basis of these misleading reports. Although analyzing post-upgrade risk is beneficial, official VA risk for a given site should reflect existing security conditions.

In contrast, some sites' VAs are outdated. They show an obsolete site configuration, based on a security posture and operations from years past, and lack the data—existing status of site operations, threats, and protective measures—to accurately assess prevailing risk. Some sites tend not to complete VAs unless an SSSP needs to be submitted and approved. Meanwhile, they routinely use these VAs for major security system and budgeting decisions even though they no longer accurately reflect the existing configuration or include newer threats.

In addition to the above concerns, the majority of NNSA sites have not submitted SSSPs for approval as required in the last 3 to 5 years, and thus, new DBT guidance has not been incorporated. (Appendix A shows the status of safeguard and security plans for the NNSA sites.)

The shortage of VA expertise and other resources, along with the greater workload stemming from the new DBT and upgrade analyses are principal reasons why these VAs are outdated. The discontinuance of the VA validation and verification (V&V) process, as discussed below, has also exacerbated this situation.

COMPLEX-WIDE INCONSISTENCY

The VA program—approach, process, rigor, and tools—is inconsistent complex-wide, primarily because adequate policy, guidance, and training are lacking. To some degree, the different VA approaches at each site appropriately represent varying geographies, missions, and other factors. Although site-specific differences are justified, rationalizing the foundations of the VAs is difficult: more standardization, consistency, and rigor is needed. Each site has a different approach to conducting VAs, and in most cases the full process is not documented at the site level, leaving any entity outside of each VA program on its own to interpret the process and method used. In addition, determining the justification for the different sites' bases for analysis is difficult because of the dearth of process documentation.

[3] Even if these not-yet-operational upgrades pertained to the current risk, NNSA will not know their effectiveness until they are performance tested, especially since some are procedural.

Examples of inconsistencies include the following:

- Some sites use the worst-case position of the protective force to determine their response force times (RFTs), and others use an average or 80th percentile.

- Some sites use "pictures in time" to help determine RFT data, and others don't.[4]

- Some sites heavily rely on a single VA software tool. For example, to determine the probability of neutralization, some sites use ASSESS BATLE only,[5] some use JCATS analyses only, and some use iterative site analysis (ISA) results. In other cases, where applicable exercises have been con-ducted, the sites have not incorporated results in the neutralization probability.

- Some sites rely on ISA as the primary method of identifying risk. [REDACTED]

ONE-TIME ISA PROCESS

In response to the events of September 11, 2001, the Chief, Defense Nuclear Security, developed the ISA process. It was designed to conduct site-by-site analyses of today's most realistic threats at the sites, as determined by a team of outside experts. It was a one-time event of great value—value that has yet to be duplicated by any other VA software tool or method when evaluating a single attack in depth.[6] Some sites want to continue to conduct ISAs and incorporate the results in their VA and SSSPs. However, NNSA has not disseminated guidance on incorporating the ISA process in the VA and SSSP, and additional ISAs have not been planned.

Although the ISA process takes a detailed approach in its evaluation of a single target, it is not designed to address all targets at a given site. The process is an

[4] Pictures in time are random, unannounced observations of protective force positions and configurations, which are duplicated during force-on-force exercises or JCATS analyses to ensure realism.

[5] The Brief Adversary Threat Loss Estimator (BATLE), an older computer model, was incorporated into ASSESS.

[6] This ISA process includes in-depth planning and information gathering meant to simulate the activities of real-world adversaries, such as collecting open source information for adversary attack planning, using active duty special operations personnel, and documentation of attack plans through an operations order format supported by real world combat experience.

"inch wide and a mile deep" in that it evaluates a specific target using a specific scenario. Other DOE/NNSA VA tools and methods tend to be more encompassing in analyzing a variety of threats and adversary scenarios to determine system effectiveness. The ISA process provides specific insights that other VA tools are not capable of providing, but other tools provide insights that ISA is not designed to accommodate. Two sites heavily rely on the ISA process as the foundation of their VA, without utilizing other VA modeling software; as a consequence they have incomplete target and scenario coverage.

JOINT CONFLICT AND TACTICAL SIMULATION (JCATS) ANALYSES INCONSISTENCY

The accuracy of the risk that sites are reporting is questionable. The inherent limitations of JCATS as a modeling tool, the lack of incorporation of exercise results in the probability of neutralization, the absence of existing standards and protocol rigor, and JCATS use as the sole tool for determining the probability of neutralization within the risk equation all contribute to this questionable accuracy.

The use of JCATS analyses varies complex-wide:

- Some sites use it as the sole method for determining the probability of neutralization.
- Some sites use a terrain file that only depicts the portion of the site to be analyzed instead of showing the entire menu of targets available to the adversary force. The limited JCATS terrain model alerts the protective force ahead of time as to which target will be attacked.
- JCATS software updates, reflecting the full weapons capabilities of the new DBT, are not centrally managed or issued to the sites. [REDACTED]
- Sites are increasingly using JCATS to dictate exercise scenarios, prohibiting the adversary force from deviating from the attack plan on the basis of the battlefield situation—thus negating its tactical advantage—because the change doesn't match the computer simulation.
- JCATS is not capable of analyzing some potential adversaries' weapons capabilities. As a consequence, some sites limit the adversary weaponry for exercises to match the weapon systems that can be evaluated by JCATS; thus, some DBT weapon capabilities do not undergo an evaluation by means of any performance test.
- Some sites have noted mistakes in the JCATS software terrain file. One site modeled a potential upgrade where a fence was used to simulate a

wall. Unknown to the JCATS system administrator, the fence allowed the protective force to shoot the adversary force through the fence when they would have realistically been behind a wall. In another JCATS analysis, instead of several adversaries traversing through the same breach point, each was required to breach a separate hole, adding an unrealistic delay time and putting the adversary force at a disadvantage.

Both exercises and JCATS have strengths and weaknesses; however, DOE/NNSA has not determined the extent to which they should be used to influence the probability of neutralization. DOE/NNSA has also not issued policy that provides each site a standard or minimum level of rigor for conducting exercises or JCATS analyses.

UNDERUTILIZED SOFTWARE TOOLS

DOE/NNSA has not provided guidance on the use of software tools in the VA process. Consequently, a number of tools developed by Sandia National Laboratory—such as AKDBS, ASSESS Query Tool, and ATLAS—are not being utilized in the field.[7] Blast effects software also has not been widely used; again, DOE/NNSA has issued no guidance regarding the standard to be used (such as AT Planner, Blast FX, Blast X, or BEEM).

INCONSISTENT CRITICAL SYSTEM ELEMENTS

NNSA lacks a standardized process for identifying critical system elements when conducting VA analyses. DOE Order 470.1 discusses critical system elements in general;[8] however, NNSA policy and guidance does not specify identification methods, testing methods, and how to incorporate test results in VAs. The sites' VAs identify critical system elements in broad terms and often do not identify all of them. The broad, general identifications make it difficult to determine the criticality of the item identified, such as protective force awareness. In other cases, testing focuses on protective force personnel and does not consider the two-person rule,[9] Personnel Security Assurance Program (PSAP), and other components of the protective system, which should be defined as critical.

INSUFFICIENT VA PROTOCOL DOCUMENTATION

Protocol documents that depict the sites' VA methods and processes are lacking.

---

[7] See Note 1.

[8] U.S. Department of Energy, *Safeguards and Security Program*, DOE Order 470.1, September 1995.

[9] The two-person rule is a system designed to prohibit access by an individual to nuclear weapons and certain designated components by requiring the presence at all times of at least two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task to be performed. Source: http://www.dtic.mil/doctrine/jel/doddict/data/t/05538.html.

Some sites have operating procedures for conducting JCATS analyses, limited scope performance tests, and force-on-force exercises, but these documents fall short of identifying how rigorous or detailed the analyses should be. For example, a procedure might identify administrative assignments for force-on-force exercises (such as armorer issuance of MILES gear),[10] but it does not describe the difference between validation and training exercises, the minimum amount of time the adversary force has to plan its attack, how picture-in-time data are utilized, controller training requirements, or how weapon effects are controller called if the MILES gear systems are incapable of representing a certain weapon (such as 40 mm grenade launchers). Exercise protocol documents serve more rudimentary functions, such as (in the case of JCATS) describing the rotation of what is termed in DOE/NNSA a "puck" driver or setting the minimum number of JCATS runs to determine neutralization.

Sites that use JCATS results as the only method for determining the probability of neutralization do not have a documented process that identifies such actions as how picture-in-time data are incorporated in the JCATS analyses and whether each crew is tested.[11] For example, no protocols exist to prevent a site from using a mixture of selected protective force personnel from all the crews, which would not represent a single, site-specific operational protective force crew. The results of this type of analysis do not reflect each crew's capability.

INSIDER THREAT INTERPRETATION VARIANCE

Interpretations of the insider threat under the new DBT differ from site to site, resulting in an inconsistent approach to VAs throughout the NNSA complex. An unclassified portion of the DBT defines an insider as someone who is unescorted. This wording has caused some NNSA sites to interpret someone who is escorted as not an insider and hence not requiring VA analysis. As a consequence, many non-PSAP insiders who were escorted have not been included in VA analyses.

[REDACTED]

LACK OF VA OVERSIGHT

DOE/NNSA headquarters and site office VA oversight is lacking. The Chiles re-

[10] MILES (Multiple Integrated Laser Engagement System) gear enables force-on-force training through a system of lasers and sensors.

[11] See Note 4.

port, *Strengthening NNSA Security Expertise*, observed that the federal security workforce rated VAs as "highly important," but also stated, "Discussions pointed out the ability to expertly review and critique the contractor's vulnerability assessment as a particularly weak area of NNSA security personnel."[12]

The oversight of VAs also suffers from a conflicting perception of responsibility as well as a lack of resources. DOE has discontinued the SSSP V&V process. NNSA headquarters representatives have expressed a desire to review and approve site-submitted SSSPs, but they are not currently doing so. Within DOE/NNSA there is a fundamental disconnect in the understanding of the role of the DOE Office of Independent Oversight and Performance Assurance (OA) in the VA oversight process. OA conducts a relatively short VA review during its 18-month desired rotation inspection process for all DOE and NNSA sites. OA representatives stated that they do not extensively review site VAs during the OA inspection, that they don't fully validate VAs (only a sample thereof), and that OA should not be viewed as the organization that validates VAs. In contrast, NNSA representatives stated that they rely on OA for oversight of VAs.

7.3.2 VA Performance Testing

INCONSISTENT LIMITED SCOPE PERFORMANCE TESTING

Protocol documents delineating the method and process of site VAs and performance testing are either nonexistent or lack depth. Existing documents lack any detail regarding how tests are identified, approved, conducted, documented, and analyzed and thus are inconsistent across the complex. Very few limited scope performance testing programs have documentation that describes the evaluation of test results and their integration back into the VA process. Many tests do not provide the data that should be sought by the VA analysts.

The documentation that does exist is generally not intended for effectiveness testing but for operability testing only. For example, site personnel may test the operability of a set of alarm sensors—waving a hand in front of a motion sensor to ensure the alarm activates at the central alarm station (CAS)—but do not conduct tests that attempt to circumvent or spoof the alarm sensor.

The methods and processes for identifying and conducting limited performance tests, and integrating them into the VAs, are inconsistent and lack rigor. The

[12] NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004, p. D-7.

strategic plan cites "Internal and Independent evaluations and performance tests document system performance and capabilities" as a success indicator.[13] However, the tests stop short of obtaining the most important pieces of site-specific performance data.

The tests conducted focus narrowly on the protective force instead of the two-person rule, PSAP, and other aspects of personnel adhering to procedure, which in some cases are more prone to failure because of their heavy reliance on the human element, as opposed to an automated sensor system. Tests that attempt to conduct an unauthorized activity to actually determine a site-specific probability of detection for various defeat strategies are almost nonexistent. When all DOE/NNSA site VAs are based on predefined detection probabilities within the various computer VA models used, there is little confidence in the accuracy of the risk reported if controlled, site-specific tests of unauthorized activities are never conducted.

Examples of other testing shortfalls are as follows:

- Some narrowly focused tests don't include critical elements or components of the protective system. For example, protective force alertness to detect airborne intrusion is excluded from evaluation when protective force supervisors, who were notified of a helicopter overflight in advance, are allowed to detect and report the intrusion.

- A site gives a 90 percent VA probability of detection credit to a specific protected area perimeter, but this same intrusion detection perimeter has 800 to 900 false and nuisance alarms per month.

- Most sites do not rigorously test adherence to the two-person rule, but rather simply observe whether the two people keep each other in line of sight. Tests designed to distract someone or simulate performance of an unauthorized activity to actually determine the probability of detection for various defeat strategies are practically nonexistent.

- [REDACTED]

- Tests measure how quickly a responder can traverse from point A to point B but fail to account for the time it takes to don fighting equipment or traverse the distance while under fire.

Because the VA software tools rely on these data, the inadequate testing results strongly influence the overall risk reported for each NNSA site.

[13] See Note 2, p. 4

INADEQUATE FORCE-ON-FORCE EXERCISES

Like limited scope performance testing, force-on-force exercises are inconsistent and lack rigor. It is not clear whether force-on-force exercises provide an accurate assurance of protective forces' capabilities to meet the new DBT because of several factors:

- exercise scenarios are constrained by many mandated restrictions such as routes of ingress/egress for safety, prescribed weapons and tactics
- adversary forces used in most of the force-on-force exercises are not fully representative of the new DBT
- NNSA lacks a testing regime similar to DoD's Mighty Guardian exercise program. Under this DoD program, a team of experts trained to think and act like potential adversaries and patterned on the postulated threat are used to evaluate DoD's nuclear security forces and protection strategies in free-play, realistic scenarios. The exercises are designed to stress forces to their limits while ensuring that the results are not treated as an inspection.

Insufficient distinction is made between DOE/NNSA exercises, designed to train people and explore new tactics and technologies, and evaluations that are designed to assess performance. In general, security force contractors are not incentivized to conduct rigorous exercises that really stress protective forces because the lack of a distinction between exercises and evaluations creates the potential of an exercise failure adversely impacting the assessment of contract performance. The pressure to not fail a force-on-force exercise inhibits useful training and promotes some inappropriate behavior. For example, some sites:

- identify administrative assignments but don't specify important practices or internal methods that significantly influence the exercise rigor and accuracy of the results
- conduct training exercises that are scaled down to the point that they don't test the overall protective system capabilities, instead of comprehensive validation exercises that do
- practice the exact exercise scenario just days before the exercise
- give the adversary force minimal time to plan its attack
- don't use a picture-in-time concept, detracting from the realism of the

starting point and configuration of the protective force[14]

- use the same crew, a combination of the best protective force members from all the crews, or selectively hire the protective force on an overtime voluntary basis (typically, the best qualified protective force members participate as volunteers) instead of rotating representative crews
- script the adversary's tactics to the point of predefining weapons, rather than letting the adversary force choose the weapons most advantageous for the scenario and terrain
- don't use exercise results to validate or otherwise influence the probability of neutralization reported in the VA because of sole reliance on the results of the JCATS computer simulations
- inconsistently use exercise (validation, training, stress exercises, etc.) results. For example, a site uses the results of a training exercise to support an assessment of low risk but omits validation exercises that may have resulted in negative outcomes.

Sites seldom use special operations personnel as adversary force team members during exercises, preferring to rely on their protective force personnel. For example, one site has refused to use "Grizzly Hitch" personnel as adversaries because, it perceives, they do not play fairly or by the rules proposed by the site.[15]

Although it is impractical to employ special operations personnel for most exercises, the use of protective force members in most cases can't duplicate the realistic operating experience associated with a professional adversary force. Exercises that use protective force personnel as adversaries often have unrealistic results because these personnel are primarily trained as defenders and lack experience in heavy weapons, explosives, airborne assets, etc. Continued overreliance on the use of protective force personnel as exercise adversaries—rather than more realistic terrorist planning and modus operandi unforeseen by the site—has the potential to create a false sense of security.

Some sites fail to comply with DOE policy, which requires at least one exercise quarterly. Some sites conduct several exercises over a year's time, falling short of the quarterly testing requirement. These situations stem in part from scheduled overtime and the manning of higher security condition levels, which have limited the availability of the protective force to train and participate in exercises. Interpretation and application of the quarterly exercise policy vary widely throughout the NNSA complex because of a lack of clear guidance. Some sites interpret "exercise" as a scaled-down test involving only a portion of the protective force and a less-than-full DBT adversary threat in a training setting; other sites interpret an exercise as a full-scale test involving an entire protective force crew and a full DBT adversary force.

[14] See Note 4.
[15] Grizzly Hitch is a trained intruder force drawn from DOD Special Operations community.

Because the quarterly exercise requirement doesn't specify how often each category I SNM facility is to be exercised, some sites conduct repeated exercises on the same target for years rather than testing a different on-site SNM facility.

The current quarterly testing requirement can contribute to an imbalance in the exercise frequency of the Category I SNM targets complex-wide. For example, site X has 50 different targets and site Y, only two. Each has the same exercise requirement. Site Y can exercise each category I SNM target several times per year, but site X takes much longer (many years) to exercise each target. Therefore, each site should rotate the types of targets that undergo an exercise to have a representative sample of the target set at each site; for example, sites should test various types of targets, varying them to test response and personnel that may be excluded if only a specific section of the facility continues to undergo an exercise.

Some sites need exercises that are more realistic. The "telegraphed" awareness that the site is about to be attacked (from an opened exercise window or a scheduled JCATS analysis) can tempt the protective force to assume a position or configuration that does not represent its day-to-day operations. To preclude this situation, a few sites capture pictures in time—a relatively new aspect of the VA process—as a verifiable method for determining protective force posture, armament, etc.[16] Security management may not know how the protective force is truly configured day to day. At present, the picture-in-time concept is one of the better methods of providing a semblance of realistic randomness, and sites can integrate it into the neutralization process, such as exercises and JCATS analyses, however it is not currently a DOE/NNSA requirement.

Many sites do not have pictures in time, raising concerns as to the accuracy of protective force positions for JCATS simulations or force-on-force exercises. When sites do use pictures in time, they often don't try to gather all the needed information—such as visiting the Central Alarm Station (CAS) to find out where the CCTVs are pointed or determining the locations of backup communication equipment (pagers and cellular telephones). Individually, these pieces of information may seem unimportant, but collectively they can significantly influence the overall protective system effectiveness. For example, not knowing the CCTV monitors that are observed within the CAS on a random basis makes it difficult to ensure the realism of detecting an adversary by CCTV in JCATS or during an exercise. Gathering all pertinent information ensures that realism and day-to-day operations are replicated in the testing process.

Training to one particular type of scenario also detracts from realism: although it may begin as a VA worst-case scenario, the more it is exercised, the less worst-case it becomes. When training and the response plan narrowly focus on a scripted scenario, slight variations can challenge the protective force.

[16] See Note 4.

7.4 RECOMMENDATIONS

1. Establish clear day-to-day oversight responsibility and accountability for the VA, SSSP, and performance testing programs within NNSA headquarters. Ensure plans and programs are current and reflect the new DBT. Periodically utilize OA resources to independently assess the performance of these programs.

2. Improve the recruitment and training of VA analysts, and balance VA expertise across the NNSA complex. Address the near-term shortage of VA expertise at selected sites through temporary reassignment. Continue development of a comprehensive VA program of instruction to:

   - better train and certify VA analysts
   - promote a more standardized VA method
   - foster greater knowledge of the strengths and limitations of various tools.

3. Develop policy and guidance for standardizing the VA, SSSP and performance testing processes and establishing more rigor and consistency across the complex. Develop standards that accomplish the following:

   - Document a consistent VA protocol.
   - Set a minimum level of rigor for all VA tools and methods used to define risk.
   - Limit the extent to which a single software tool can be used in determining the probability of neutralization and balance software tool usage with field-testing results (which require the entire protective system to actually perform). For example, provide guidance on using JCATS to complement performance testing results, not substitute for them. Use force-on-force exercises to contribute more to the foundation of a site's probability of neutralization.
   - Provide guidance for performance testing to help standardize how VA analysts identify protection elements and components that should be tested and how the results should be calculated and integrated into the VA process. Prepare detailed protocol documents for force-on-force exercises to capture the aspects—preplanning, conduct, and after-action tasks—that influence exercise realism and value.
   - Adopt true free-play, force-on-force testing for the exercise program, in which the threat force is not artificially limited in its ability to apply known terrorist tactics or weaponry. The threat force should routinely comprise expert adversaries, who, by their training and operational background, can think and act like terrorists.

- Clearly identify and delineate critical system elements and specify how the elements should be tested and the results incorporated into VAs, SSSPs, and performance testing

- Clarify the DBT policy related to the insider threat to ensure consistent interpretation.

- Provide policy and guidance to those responsible for identifying, writing, conducting, documenting, and analyzing VA performance tests to ensure a higher level of rigor and standards. Ensure that site exercise programs evaluate a broad range of components that span the site's protective system (detection, delay, and response force times), including insider-type defeat strategies (two-person rule, etc.).

- Establish policy and guidance for force-on-force exercises and their utilization in the VA process. Provide guidance that ensures each site is conducting exercises and JCATS analyses in a manner that precludes the protective force from intentionally or unintentionally knowing the adversary tactics, strategies, and target selection. Guidance will result in greater consistency and standardization among NNSA sites, including the rigor with which a validation exercise should be con-ducted and how exercise data can be used to support the site's probability of neutralization.

- Provide guidance on the use of the external special operations team (such as Grizzly Hitch) as the aggressor force or establish a trained aggressor force that does not comprise protective force members from the same site.

- Provide specific policy on the quarterly exercise requirement, including the degree to which different protective force crews and targets are tested. Provide a balanced policy approach, which requires rotation of exercised target areas to reflect the diversity of site-specific targets.

- Require pictures in times to be conducted for each site so that normal protective force configurations can be documented and serve as a preparatory step for force-on-force exercises and JCATS analyses.

4. Consider creating an NNSA-wide core VA team that routinely assists sites in the conduct of VAs and ensures a greater consistency and quality in VAs across the NNSA enterprise. The core team would also provide a mobile VA training function as it rotated from site to site.

5. Ensure that approved site SSSPs and the risk acceptance inherent in these SSSPs are based on VAs that evaluate existing operational conditions. Do not allow risk acceptance to be based on planned or projected security up-grades. Encourage sites to use the VA and SSSP process to analyze the effectiveness of potential security upgrades and project future risk.

6. Reinstitute the ISA process on a recurring basis in the conduct of VAs and development of SSSPs.

7. Promote more rigorous, realistic exercises that really stress protective forces (to understand their limits) by providing greater immunity to security contractors, such that exercise results are distinct from periodic performance assessments and do not affect contract performance.

8. Adopt a force-on-force exercise program for NNSA sites similar to the DoD Mighty Guardian exercise program, or expand the Mighty Guardian exercise program to include NNSA sites. Under this program, a team of experts trained to think and act like potential adversaries, patterned after the DBT, would conduct the exercises. NNSA would use the results of these exercises to rationalize past differences in DoD and NNSA performance testing and more accurately validate protection strategies.

Section 8
Protective Force

8.1 BACKGROUND

Each NNSA site hires and maintains its own protective force (PF) personnel to protect special nuclear material (SNM), classified material, and NNSA assets and employees. The PF, which includes approximately 2,400 officers nationwide, comprises several contractors and unions and is divided into the following categories:

- Security Officer—unarmed officers
- Security Police Officer I and II (SPO I and II)—armed defensive officers and offensive responders
- Security Police Officer III (SPO III)—special response teams (SRTs) and offensive responders.[1]

Each category of officers has its own physical fitness, weapons, and training qualifications.

8.2 SUMMARY

NNSA lacks a consistent approach for validating PF manning; because of wide variations in site approaches, determining whether site PFs can adequately meet the requirements of the new Design Basis Threat (DBT) remains problematic. PF performance is degraded by an excessive backlog in security clearances, inadequate guidance and training in several significant areas (such as adversary pathways, chemical and biological weapon defenses, and recapture, recovery and pursuit), and a lack of collaboration with vulnerability assessment (VA) experts, FBI, and local law enforcement officials. Response plans, target folders, and central alarm station systems need upgrading to improve PF readiness.

8.3 OBSERVATIONS

8.3.1 Staffing

PF staffing is not based on clear, well-defined policies and a consistent NNSA-wide methodology. Although the NNSA strategic plan states, "We will use a systems

[1] We did not visit the Office of Transportation Security, which consists of federal officers

engineering approach to identify and implement best combination of systems and PF personnel to most effectively protect our security interests,"[2] and "We will use a risk management approach to identify that level of security protection that provides an acceptable and managed level of risk,"[3] the approach to staffing varies widely from site to site.

Without an NNSA policy that sets standardized criteria for validating PF operations, determining whether site PFs can adequately protect DOE SNM and critical assets will remain problematic. Each site has different methods and rationales for determining PF staffing, equipment, and training and for gauging whether protection is effective or adequate. The lack of a standardized, specific policy (formerly found in the superseded *Standards and Criteria Manual*) has led to this ad hoc approach.

Sites increase or decrease PF staffing with little documented analysis as to its effect on other projects or contingencies. For example, the shortage of personnel in the PF at one site—and thus its inability to protect multiple targets—has caused a shutdown of all test projects. That site's management greatly reduced the PF without considering the impact on other projects that needed safeguarding. At other sites, the PF staffing levels increased when an independent assessment by the Office of Independent Oversight and Performance Assurance (OA) and other audits showed serious flaws, and then decreased in years following successful audits and inspections. One site's PF staffing increased to meet contingency planning for one target, and then the site redirected the PF to address issues at other target locations, essentially leaving the first target as vulnerable as before.

No specific policy establishes methods sites can use to determine PF staffing levels through appropriate analysis or performance testing. Some determine staffing levels on the basis of JCATS analyses and others elect to use limited-scope performance tests. Very few sites conduct full-scale force-on-force exercises to capture an aggregate of pass and fail ratios with varying numbers of PF responders. All but one site declares that PF staffing levels are adequate for implementation of their protection strategies. This declaration may be true from the sites' perspective and demonstrated through their philosophy of analyses and testing, but determining its validity from the outside is difficult without clear policy for testing and validation.

Each site differs in how it uses response force times (RFTs) and pictures in time, and some don't use them at all. Some sites don't roll completed RFTs back into the VA analysis to determine their effectiveness in relation to adversary task time or incorporate them into force-on-force exercises or JCATS analyses. Without accurate RFT data, determining whether a site PF can respond in time with the appropriate numbers to interrupt or neutralize an adversary force is nearly impossible. No formal protocol describes how to test PF response time or how to roll test results back into the VA, which makes it difficult to determine whether appropriate analyses were completed to determine PF staffing levels.

[2] National Nuclear Security Administration, NNSA Safeguards and Security Strategic Plan, June 2003, p.1.
[3] See Note 2, p.2.

8.3.2 Clearance Process

The backlog in pending security clearances, because of the lengthy clearance approval process, has excessively increased NNSA overtime, affecting budgets and detracting from PF performance. NNSA has recognized this problem, and the strategic plan says it will "expand authorities and options for reducing time required to obtain security clearance and reinvestigation results."[4]

Excessive overtime budgets are still required for filling Q-cleared Personnel Security Assurance Program (PSAP) PF positions required by new DBT implementation plans and increased security condition levels.[5] New hires cannot fill positions until their clearances are granted, creating inordinate overtime demands for the already-cleared PF. As a result, sites must pay for the new hires who can't work the position and pay overtime to the cleared personnel who can. Excessive over-time leads to fatigue, burnout, and high turnover rates and can affect the PF's ability to conduct training and exercises because the officers are scheduled to work on days when training and exercises are often scheduled.

Facilities have a tremendous backlog of obtaining clearances for new hire PF personnel. Sites said that the Accelerated Access Authorization Program (AAAP) didn't work to expedite this effort because participants have to be too "squeaky-clean" to get through it.[6] Q clearances routinely require an average of more than a year, with another three months for PSAP approval.

8.3.3 Training and Qualifications

ADVERSARY PATHWAYS AND RESPONSE PLANS

Some site PFs do not receive adequate training in identified adversary pathways and their applicable response plans. DOE Manual 473.2-2 requires plans to address response to security incidents and adversary intrusion as described in the DBT policy.[7] In general, the existing response plans describe PF response activities, but usually contain little detail on the adversary attack methods and pathways identified and analyzed in the VA process. An effective PF should clearly understand adversary worst-case pathways and capabilities in addition to security incident response plans. Only two sites have trained PF personnel in VA probabilities and adversary worst-case pathways.

[4] See Note 2, p.6.
[5] In January 2004, DOE established the Human Reliability Program (HRP), which incorporates the important elements of the PSAP and Personnel Assurance Program (PAP) into one comprehensive program. Source: Federal Register, Volume 69, Number 129, July 2004. Available from http://edocket.access.gpo.gov/2004/04-15331.htm.
[6] NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis,* Henry G. Chiles, Jr. et. Al., March 2004, p.2-9.
[7] U.S. Department of Energy, *Protective Forces Program Manual,* DOE Manual 473.2-2, June 2000.

Some sites do not require the PF to be familiar with or study and analyze response plans; these sites claim that response plan training takes place during force-on-force and tabletop exercises. This training approach is ineffective; at some sites, force-on-force exercise participation is voluntary, exercises are infrequent, and their relation to response plan review is questionable. No systems are in place to verify that appropriate PF personnel have participated in response plan training. Tracking individual participation in written response plan training is difficult at best. Officers on duty at any given time may not have read or been trained on these plans.

FIREARMS AND PHYSICAL FITNESS

Firearm and physical fitness qualifications are mandatory, but ongoing proficiency training between qualifications is optional at most sites. Not all sites re-quire SPOs to have firearm proficiency or physical fitness training between qualifications. Most allow officers to conduct voluntary training while on duty or make overtime hours available for them to schedule and conduct their own fire-arms proficiency and physical fitness training. At most sites, SPO IIIs take more advantage of this training than SPO IIs.

Physical fitness qualifications typically occur within a month of the officer's birthday, and firearm qualifications are semiannual, so many elect to only work out or practice several weeks before the test. This situation raises the question of whether the testing reflects the actual capability of the response force year-round or just individual capabilities at known test times—a question that becomes more critical as the PF ages.

RECAPTURE, RECOVERY, AND PURSUIT

Training and qualification are inadequate for recapture, recovery, and pursuit. In general, PF protection strategies focus on meeting only a portion of the worst-case DBT, denial of access. Although this strategy should be primary, sites need to have plans in place for denial of task, recapture, recovery, and pursuit contingencies to meet the full intent of the new DBT policy. Sites do not routinely test or validate preparation for these contingencies to demonstrate that they can perform missions should denial of access fail. Without these elements, sites are left with the potential for a single-point failure in their protection strategies.

FORCE-ON-FORCE EXERCISES

Force-on-force training at some NNSA sites lacks realism. It is difficult to con-duct realistic training exclusively at NNSA sites because the use of explosives, live fire weapons and, at some sites, even simulation type weapons are not al-lowed in the vicinity of storage facilities for safety reasons.

Site PFs are not conducting enough force-on-force exercises to maintain perish-able tactical skills. OA leadership has expressed a similar concern that the PF is stretched too thin across the complex and therefore not conducting enough force-on-force

testing, which leads to the loss of or reduction in perishable tactical skills and reduces overall efficiency. Force-on-force exercises are the closest replication of actual combat that can safely be used for training and evaluation of PFs. Sites should not use this valuable tool just to pass inspections or audits. If PFs do not frequently conduct these exercises and use the lessons learned to train their personnel, or if PFs substitute computer simulations or other training methods for exercises, their officers may not be tactically prepared to perform their missions.

8.3.4 VA and PF Coordination

At some sites, VA and PF personnel do not collaborate closely to ensure the accuracy and consistency of the VA and PF response plans. To ensure that response plans are effective and security systems are adequate for delay and detection, the VA and PF representatives must share information such as task times of adversaries, most likely pathways, and PF response times for interruption and neutralization of the adversaries. In the VA process, PF actual capabilities and accurate response times have to be captured in VA reports.

Some sites do not involve the PF adequately in the VA process. One facility does not include PF management in the initial review of VAs, and the VA planning group actually writes the PF response plans without PF participation—leaving the subject matter experts in tactics (the PF) without input to its response strategy. On the basis of lessons learned, one site now uses PF supervisors to write response plans, with the VA planning group, to avoid discrepancies.

8.3.5 Response Plan Effectiveness

Site response plans lack sufficient detail in several key areas. All sites except for one have active response plans in place, but most plans don't have detailed procedures for recapture, recovery, pursuit, communications, loss of communications, and chain of command. Some have conflicting information as to whether their target objectives are containment, denial of access, or denial of task. Sites that address these topics in response plans have either ineffective or contradictory planning information. For example, at one site, the VA group has a target objective listed as denial in its analysis, and the PF has the same target objective listed as containment in its response plans.

Local law enforcement and FBI cooperation with NNSA sites is severely deficient. Sites do not have memorandums of understanding/memorandums of agreement (MOUs/MOAs) with outside agencies to respond to potential contingencies. DOE Manual 473.2-2 states that sites that identify the need for outside agency support will establish formal MOUs/MOAs, annually update them with the off-site agency, and conduct annual force-on-force exercises.[8] Most sites have met with off-site federal and local law enforcement agencies (LLEAs) but coordination has generally been limited to discourses and table-top exercises. Other unresolved issues involving coordination with LLEAs include the following:

- Overall tactical command responsibility
- Different use-of-force policies
- Appropriate maximum speed during a pursuit
- Conflicts among internal documents concerning pursuit tactics and coordination with LLEAs.

In general, sites that deputized selected PF staff into the LLEA or established a federal officer program within their PF had more success in bringing the LLEA and site PF personnel together on these issues.

8.3.6 Target Folders

Only half of the sites visited have some form of target folders in place; none of the sites completely follow the approved, enhanced guidance of the 1998 McCallum memorandum.[9] This memorandum—developed and agreed upon by DOE and FBI headquarters—gives specific guidance as to what the DOE target folders encompass. The remaining sites do not have target folders in place, or they are not sufficient for planning purposes. Only two sites have target folders sufficient for tactical planning for basic response and, more important, recapture and recovery (R&R).

Sites develop target folders to assist the PF and outside law enforcement agencies in conducting interagency-compatible tactical operations. However, sites are un-sure of what the target folder includes and the approved format. DOE Order 473.2-2 directs sites to follow OSS director guidance, which outlines the required information and approved format. In addition, during semiannual SRT quality panel meetings, the DOE Office of Security (SO) encouraged site representatives on the panel to use the director guidance.

[8] See Note 7.

[9] U.S. Department of Energy, memorandum from Edward McCallum, Director, Office of Safeguards and Security, to DOE director distribution, subject: *Enhanced Target Folder Development and Use,* June 4, 1998. DOE Manual 473.2-2 (see Note12) directs that site target folders use the format and content approved by the Office of Safeguards and Security (OSS) Director. The memorandum from Director McCallum describes the current approved format and content.

8.3.7 Chemical and Biological Weapon Defense

The NNSA-wide response to the chemical and biological weapons (CBW) threat lacks uniformity. All sites have respirators and limited personal protective equipment (PPE) clothing. [REDACTED]

8.3.8 Central Alarm Station Alarm Rates

Some sites' central alarm station (CAS) false and nuisance alarm rates are excessive or not tracked. One site's false or nuisance alarm rates are in the thousands per month. In effect, portions of the protective system are not operational because the CAS operator has to access (turn off) or ignore the alarms as a nuisance be-cause there are too many to assess and respond to. This increases the risk to the protected area, and this risk is not accurately reflected in the site's VA. For example, if the site's VA takes a large amount of credit for certain properly working protection elements, then it should also accurately reflect degraded operations. Another site's alarm administrator, who had no false or nuisance alarm data, said the site system is antiquated.

In general, the PF is not properly trained in recording alarms; for example, the difference between nuisance (environmental or animal caused) and false (un-known and needing assessment) alarms is frequently not made. Understanding the difference is critical to documentation and evaluation of the system's effective-ness.

8.3.9 Recapture, Recovery, and Pursuit

RECAPTURE AND RECOVERY (R&R)

Site R&R contingency plans are nonexistent or inadequate.[10] The sites explain that they focus on a denial-of-access strategy. Denial of access is the primary mission of NNSA sites, and resources and efforts should be dedicated to developing robust denial strategies. However, some sites' reliance on the viability of their denial strategies has precluded them from adequate planning, training, and procurement of appropriate tools for R&R should denial fail. Some sites' R&R plans incorporate a

[10] This does not include plans of the Nuclear Emergency Search Team, which we did not review.

denial-of-access strategy that inappropriately assumes they will never lose control of the facility. If adversaries gain access to a facility or leave with material, R&R programs are critical. Furthermore, the new DBT policy established site responsibility for instituting an R&R program.[11]

Site safeguards and security plans (SSSPs) and some facility response plans ad-dress R&R programs and plans, but they vary widely, and some do not fulfill the need for a timely, effective, and viable R&R capability or meet the intent of DOE Manual 473.2-2.[12] Some approaches include R&R response activities and requirements (spread throughout different response documents) but do not identify one specific response plan for R&R of an SNM storage facility or material in un-authorized control.

Other R&R approaches include tactical options that are rudimentary, very high risk, and not tactically viable. For example, the mechanical and electronic entry techniques used at some sites have not been performance tested or fully evaluated for their effectiveness, and, during iterative site analysis (ISA) processes or OA inspections, some of these techniques have failed testing. DOE Manual 473.2-2 states that when mechanical entry alone will not meet required response times, the site or facility must develop an explosive tactical entry capability.[13] [REDACTED]

[REDACTED]

Although the elements of response plan training and testing are critical to effective R&R programs, very few sites have conducted actual training or testing, and those that have use tabletop activities or walk-through drills.

Adversary capabilities continue to increase, but NNSA threat planning lacks dedicated offensive response teams for each site to meet these threats. The manpower-intensive denial-of-access strategy requires numerous PF personnel dedicated to a material access area (MAA) in a repel-type posture. Sites say that the resources committed to this effort prevent them from assigning an offensive force as a dedicated, ready, and equipped element for R&R response activities.

[11] U.S. Department of Energy, memorandum from Robert Card, Under Secretary, to Field Operation Office Directors, subject: *Design Basis Threat,* May 20, 2003.
[12] See Note 7.
[13] See Note 7.

The DOE system has an offensive PF program (SPO IIIs),[14] but most sites utilize SPO IIIs in a defensive position, often separating them to operate individually or with SPO IIs not trained in team tactics. This use defeats the purpose of a highly trained offensive team that can rapidly and aggressively respond to R&R options and other adversary attacks and constitutes nothing more than using SPO IIIs as highly trained SPO IIs.

PURSUIT

Sites do not have sufficient planning, equipment, and training to conduct pursuit operations. Pursuit capability is a critical component of effective R&R. Most sites have not conducted recovery or pursuit training or exercises beyond the protected area of a facility, even on-site. [REDACTED]

Pursuit guidelines allow PF personnel to use vehicle immobilization techniques and tire deflation systems, and fire at and from moving vehicles (all of which fall under deadly force). To maintain pursuit capability, sites need to provide emergency vehicle operation course (EVOC) training, a perishable skill that requires refreshing and practice. However, most sites do not provide this training due to resource limitations.

8.4 RECOMMENDATIONS

1. Establish policy to ensure that protective force staffing is based on an ac-curate VA. Include specific guidance to help sites prepare plans for PF staffing, equipment, and training in a defendable and consistent manner to eliminate the wide variation in site to site interpretation.

2. Increase clearance investigation personnel staffing to help reduce the security clearance backlog.

3. Adopt the recommendations of the Security Affairs Support Association (SASA) "to improve and streamline the current processes for granting new security clearances and reinstating existing accesses."[15]

4. Direct sites to train or brief the PF on VAs, including worst-case adversary pathways, task times, and adversary attributes.

[14] In addition to SPO II training, SPO IIIs take a 3-week course in room-clearing tactics, receive limited tactical operation training, and have slightly higher physical fitness and firearms standards. However, these qualifications alone do not completely fulfill R&R mission needs.

[15] Letter, from Kenneth A. Minihan, President and Chairman of the Board, SASA, to directors of various agencies, February 13, 2004. Available from www.greaterla.isac.com/docs/sasaltrtodci.doc.

5. Have sites establish formal training to ensure that all PF personnel have current knowledge of response plans and strategies.

6. Consider establishing requirements for more frequent weapons and fitness training, rather than making it optional between qualifications.

7. Consider conducting random testing of the PF throughout the year in both firearms and physical fitness. This testing will encourage officers to maintain weapons skills and physical fitness levels year-round and will give management a more realistic picture of the overall PF's capabilities.

8. As recommended by the ETE Review, NNSA, in partnership with DoD, should establish a national training center for protective forces. The center should provide for realistic, force-on-force training against a well-trained, well-equipped adversary that simulates the DBT. The facility should be flexible enough to allow simulation of representative storage and transportation configurations. Training should be scheduled to allow all protective forces to participate at least once every two years.[16]

9. Ensure that sites are required to routinely and frequently conduct force-on-force exercises to evaluate and train in the tactical skills needed for com-bat operations.

10. Direct the standardized use of PF subject matter experts in the development of VAs and PF response plans to ensure the cooperation and integration of personnel responsible for effective protection strategies. Promote greater collaboration between site VA teams and PFs to develop VAs and response plans.

11. Direct site offices to ensure that target folders meeting DOE guidance are in place to tactically plan an R&R operation and support other strategies identified in site incident response plans. Consider giving the site office, PF, and local law enforcement or FBI (the entities with a vested interest, should the need for target folders arise) final approval of target folders.

12. Consider consolidating the various memos, guides, and policies concerning target folders into a single policy document.

13. Establish, with appropriate urgency, a CBW defense policy. It should identify specific criteria for implementation of specific levels of CBW equipment, including a minimal level of PPE, training, and detection. Develop a baseline threat for CBW, detailed enough to assist sites in identifying their program

[16] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Indpenedent Assessment of the U.S. Nuclear Command and Control Systems (U),* Final Report, April 2002 (Top Secret)

needs and providing a good rationale for SSSP documentation as required by DOE order. The identified criteria and threat will provide sites and headquarters a tool to plan for appropriate funding and implementation, including development of an exercise and testing pro-gram for effective evaluation.

14. Direct site offices to regularly check the false or nuisance alarm rates from the CAS and compare them with the credit taken in the VAs to ensure the analysis accurately reflects field conditions. Establish a method to properly record and document the false or nuisance alarm rate and ensure proper training for CAS PF personnel. Install modern computer alarm equipment that has an automated alarm tracking system to replace antiquated systems.

15. Ensure sites establish viable, effective R&R plans, which include exploring the need to retake a facility and the most current tactical methods (mechanical and explosive breaching) available. Sites should analyze and document the practicability of an explosive breaching strategy for their specific storage facility. [REDACTED]

16. Direct sites to establish testing and evaluation of R&R contingency plans, including evaluation criteria, to determine the effectiveness of the pro-gram. Require each site to maintain a dedicated offensive force—trained, equipped, and responsible for R&R missions. Consider creating a training program that includes offensive team tactics and tactical entry techniques for hardened targets in line with current R&R needs. Ensure sites have the ability to train and equip their PFs with the most current methods of R&R and pursuit, including hands-on training with equipment, coordination, and exercises with outside agencies.

17. Urgently establish and periodically revalidate MOAs with the FBI and local law enforcement agencies (LLEAs) for each applicable NNSA site. Improve FBI and local law enforcement cooperation with NNSA sites to include development of recapture/recovery plans for appropriate sites and actual exercises (i.e. not just table-top) of plans in recapture/recovery scenarios. Consider encouraging sites to deputize some site PF personnel into surrounding LLEAs or establishing a federal officer program.

18. Establish policy detailed enough to enable sites to prepare response plans covering R&R, pursuit, communications, loss of communications, and chain of command. Direct sites to prepare realistic pursuit plans that detail chase parameters.

19. Establish policy that directs sites to have a dedicated offensive element—separate from the denial-of-access contingent—that can implement R&R and other offensive missions like pursuit, ambush, and counter-sniper actions.

Section 9
Security Incidents and Inquiries

9.1 BACKGROUND

The reporting, investigation, monitoring, and analysis of security incidents within NNSA are vital to the overall protection of NNSA assets. A successful, robust program includes timely identification and recognition of incidents, proper categorization by consequence and seriousness, timely notification of appropriate management, full investigation, adequate corrective action, and dissemination of lessons learned to prevent recurrence. DOE recently replaced DOE Notice 471.3 and issued DOE Order 471.4, *Incidents of Security Concern*, to set forth program requirements.[1]

9.2 SUMMARY

The reporting, investigation, monitoring, and analysis of security incidents within NNSA are hindered by inconsistent practices, redundant reporting, and inadequate reviews. More formal and disciplined processes are needed to ensure the underlying causes of incidents are identified and addressed, appropriate corrective action is effectively implemented, and lessons learned are disseminated within NNSA to mitigate against recurrence.

9.3 OBSERVATIONS

9.3.1 Inconsistent Incident Categorization

DOE Order 471.4 describes the categorization of incidents of security concern as follows:

> Incidents of security concern are categorized in accordance with their potential to cause serious damage or place safeguards and security interests and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an impact measurement index (IMI) number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of

[1] U.S. Department of Energy, *Incidents of Security Concern*, DOE Order 471.4, March 2004.

physical security, protective forces, information security, personnel security, and nuclear material control and accountability[2].

Sites inconsistently categorize incidents using the IMI tables in DOE Order 471.4 because interpretations vary widely from site to site. For example, some incidents that should have been categorized and reported as IMI-3 or -4 were categorized as not reportable. Other incidents that should have been categorized as IMI-2 or -3 were categorized as IMI-4, which allows monthly compilation reporting instead of reporting to headquarters within 8 hours of categorization.

The following are examples of inconsistent site categorization of incidents of security concern using the DOE Order 471.4 IMI tables:

- At some sites, instances of personal cell phones found inside limited areas were categorized as IMI-3, and at another site, as IMI-4.

- At one site, an incident where a camera and cell phones were found inside a sensitive compartmentalized information facility (SCIF) was categorized as IMI-4; at other sites, this incident would have been categorized as IMI-2.

- At one site, some instances involving classified information on unclassified computers were categorized as non-incidents or IMI-4; at other sites, they were categorized as IMI-1, -2, or -3, as appropriate for the level of classified information and duration exposed.

- At another site, an unsecured alarm point was categorized as a non-incident. At the other sites visited, this incident would be categorized as IMI-4.

- At one site, an incident involving a Category IB of U^{235} left outside a vault overnight was categorized as the lowest IMI-4. This incident should have been categorized as IMI-2 and reported to the Office of Security (SO) within 8 hours of categorization. Because it was categorized IMI-4, the only notification SO received was an end-of-month compilation report of IMI-4 incidents at the site. Personnel did not inform contractor security management, site office security management, SO, or NNSA of the incident as required.

- Some sites are incorrectly interpreting "more than 8 hours" (under IMI-4 type 13) to mean that if an unclassified PC or network on which the classified information resides can be pulled offline, secured, or sanitized within 8 hours of discovery, the incident can be categorized as IMI-4 or a non-incident—no matter how long the classified information resided (and was vulnerable) on the unclassified PC or network.

[2] See Note 1, p. I-2.

The current incident reporting process allows (and somewhat encourages) the recategorization of incidents to a lower consequence when sites determine that no compromise of classified information occurred. Some sites downgrade the incident category after determining that no compromise or potential compromise of classified information occurred, and others do not. This inconsistency hinders efforts to obtain and track meaningful metrics that reflect the type and seriousness of incidents that have occurred. The recategorization and submittal of a new DOE Form 471.1 to change the incident from the initial, more serious category to a lesser one obscures the potential seriousness of the initial incident.[3] This practice gives DOE/NNSA senior managers a false sense of security; when incidents are recategorized, DOE/NNSA management is precluded from evaluating the potential gravity of the initial incidents or number of near misses, which could be pre-cursors of a more serious security problem.

9.3.2 Redundant Reporting Systems

Incident reporting systems are redundant. DOE requires the reporting of incidents under the DOE Office of Security (SO) purview through the Incidents of Security Concern (IOSC) reporting process to headquarters. Additionally, security-related safety incidents are required to be reported through the Occurrence Reporting Processing System (ORPS). These different reporting systems are not integrated, so one incident is sometimes reported through more than one channel or system to headquarters. This redundant reporting can lead to confusion. Finally, DOE Notice 205.4 requires the reporting of cyber incidents—such as unauthorized access, malicious code, denial of service, and scans and probes—through cyber channels to the Computer Incident Advisory Capability (CIAC).[4]

9.3.3 Inadequate Incident Inquiries and Report Review

Some site offices, NNSA headquarters, and the DOE Office of Security (SO) do not sufficiently review final inquiry reports for adequacy, completeness, and thoroughness of inquiry. The panel noted a number of inadequate IMI-1 and -2 reports at one particular site and a lack of thoroughness in investigating certain cyber incidents at another.

At one site, the cyber organization does not give incidents of security concern the same priority as the inquiry team does, so its support is not as forthcoming or complete as it should be. The cyber organization reportedly does not want to generate any classified information, so it does not provide adequate reports to the inquiry officials. Review of a number of inquiry reports found a failure to fully investigate cyber incidents, for example, determining whether further dissemination of the classified information went beyond the initial distribution or whether uncleared or non–U.S. citizens were in proximity to computers containing classified information.

[3] U.S. Department of Energy, *Security Incident Notification Report*, Form 471.1.
[4] U.S. Department of Energy, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents,* DOE Notice 205.4, March 2002.

The adequacy of transient electromagnetic pulse surveillance technology (TEMPEST) experience and knowledge for those involved in conducting official inquiries is lacking. At most sites visited, the distance from unauthorized cellular telephones to classified processing equipment is not considered in the investigation and evaluation of an incident.

One site generates brief, inadequate IMI-1 and -2 final inquiry reports and uses Form 5639.3, "Report of Security Incident/Infraction," almost exclusively for all incidents (IMI-1 through -4). DOE Order 471.4,[5] DOE Notice 471.3,[6] and Secretary Memorandum, June 14, 2002, require full, [7]final reports for IMI-1 and -2 incidents. Form 5639.3 is only to be used for IMI-3 and -4 incidents.[8] The continuation of this practice for some time reinforces the observation that the site office, NNSA, and DOE headquarters do not appropriately review final inquiry reports. An SO representative stated that his office has not reviewed final inquiry reports since about 2001 when his office was taken out of the oversight role; how-ever, NNSA has not, until recently, exercised their responsibility for final incident report review. NNSA recently assigned an employee as its point of contact for incidents of security concern. This employee is awaiting classified workspace but stated that part of her new responsibilities will be to review all final NNSA inquiry reports and return inadequate reports to the originator.

The process for incident closure does not sufficiently involve final report review for adequacy and promulgation of lessons learned. Sites submit initial incident reports to the DOE Operations Center for appropriate distribution, and final incident reports are sent to the Office of Security (SO). Although copies of the initial and final reports are provided to NNSA, closeout is conducted by SO—which does not have direct, day-to-day oversight responsibilities for NNSA sites. Incidents are inappropriately closed out upon receipt of a final report at SO, rather than upon NNSA review of the final report for adequacy of corrective action and dissemination of lessons learned.

9.3.4 Inadequate Tracking and Communication

At most sites, a formalized and disciplined site-level process for tracking security incident corrective actions is lacking. As a consequence, determination of whether appropriate corrective actions have been institutionalized is difficult. Most sites reported that line management is responsible for tracking and implementing corrective actions identified by an inquiry into an incident of security concern. However, most sites do not have a formalized, disciplined process for tracking and verifying that identified corrective actions were properly implemented. Site senior supervisory awareness and oversight of the status and completion of corrective actions is needed.

One site does have a good manual method of tracking the corrective actions at the

[5] See Note 1, p. 1-8
[6] U.S. Department of Energy, *Reporting Incidents of Security Concern,* DOE Notice 471.3, April 2001.
[7] U.S. Department of Energy, memorandum from Spencer Abraham, Secretary of Energy, to Lead Program Secretarial Officers, subject: *Reporting Incidents of Security Concern,* June 14, 2002.
[8] See Note 1. p. 1-9.

inquiry official and specific incident line management level. However, without a site-level tracking process, timely completion and sharing of incidents and actions—to preclude similar incidents at the same site—is difficult.

DOE/NNSA has no dedicated, formalized program for reviewing incidents, analyzing root causes, verifying adequacy of corrective actions, and disseminating lessons learned across DOE/NNSA to promote awareness and minimize recurrence. Although DOE/NNSA has a variety of means for disseminating information, the ad hoc process for disseminating security incident lessons learned is not timely, complete, or effective.

The Chiles report found the following:

> Incident reviews, root cause analyses, corrective action plans, and corrective action tracking are common elements of each site's security pro-gram. Specific issues and incidents vary among the sites, but a number of common areas have bearing throughout.
>
> The complexity of NNSA activities, level of staffing, and continuously evolving security challenges underscore the importance of both informal and formal mechanisms for the timely communication of issues and application of lessons-learned within and across the NNSA sites. This practice is similar to those for sharing lessons-learned from safety evaluations and incidents.
>
> The coordination and sharing of security lessons-learned is an important responsibility for NNSA. Dissemination of this information helps improve security performance within the NNSA complex, provides a highly beneficial training and development tool for the federal security staff, and helps strengthen professional relationships within the security work-force. An effective synthesis of lessons-learned from internal security re-views and recurring external inspections of NNSA and other DOE sites serves not only to improve security performance at the evaluated site, but also helps to identify site and complex-wide trends and leading indicators that can be communicated throughout the complex.
>
> NNSA has a variety of methods for disseminating current issues, best practices, and lessons-learned: participation in quality panels, periodic S&S directors conferences, monthly conference calls involving S&S directors, lessons-learned database systems, and an occasional newsletter or special e-mail. NNSI also conveys current issues. Nevertheless, the current processes have limitations. For example, lessons-learned are not published regularly. Only 9 percent of our survey respondents strongly

agree that the lessons-learned process is timely and effective, and fully 30 percent did not consider it so.[9]

9.3.5 Inadequate Security Incident Metrics

Security incident metrics provided quarterly to senior DOE and NNSA headquarters leadership are inadequate to monitor and assess security program performance. They do not reflect the true nature of the incidents and near misses occurring across the complex. Examples include the following:

- The metrics inordinately focus on comparing sites' incident closures as measures of success rather than on analysis of underlying causes (such as procedures, training, materiel, and personnel) and occurrence trends. One headquarter's metric compares open to closed incidents at each individual site. If a site has a number of incidents open compared with other sites, it reflects negatively in the metrics. In effect, sites are positively recognized for incident closure rather than for thoroughness of inquiry and adequacy of corrective action. Additionally, this measure does not accurately reflect whether sites close inquiries within 60 working days (as required by order for IMI-1 and–2 incidents).

- One metric, for information security incidents, weights them according to the classification level or type of the information involved, regardless of the IMI number of the incident and whether the information was compromised or not. In effect, incidents involving top secret, special access pro-gram (SAP), or sensitive compartmentalized information (SCI) material where no compromise occurred are routinely graded more negatively than a compromise of secret national security information (NSI) material.

- IMI-4 incidents are not included in the quarterly metrics because sites only report IMI-4 incidents monthly as a compilation and do not include information on the level or type classified information involved. When incidents are recategorized down to IMI-4 (after determination that no compromise occurred), they are not factored into the metric. As a result, senior leadership is unaware of the nature and frequency of potentially serious incidents determined to be near misses.

- Cyber security incidents are not fully integrated in the security incident metrics because of a lack of collaboration between SO and the DOE CIO and their separate incident reporting systems.

[9] NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: In Independent Analysis,* Henry G. Chiles Jr. et al., March 2004, pp.2-10 and 2-11

9.3.6 Inconsistent Infraction Administration

NNSA guidance on implementation and application of the infraction program is lacking. This omission results in widely varying local interpretations of criteria for charging individuals with security infractions. Some sites have different levels of security infractions and occurrences, warnings, or near misses. An employee at one site may receive an infraction for an action that would incur only an occurrence, warning, or near miss at another site.

There are no clear standards for what constitutes in an infraction, and thus there are consistencies across the complex. For example, many sites issue infractions to employees who introduce personal cell phones into security areas. In contrast, one site did not issue an infraction when an employee brought a personal cell phone into a sensitive compartmentalized information facility (SCIF). The same site sometimes issued infractions when the cell phones were introduced into limited areas. Another site office did not issue infractions to a number of employees who put classified information on unclassified PCs. Some sites that have more than one level of infractions, warnings, occurrences, or near misses do not provide re-ports of certain levels to the personnel security office as required for derogatory information. Because infractions are considered derogatory information in clearance reviews, administration of infractions needs to be more standardized.

9.3.7 Inadequate Inquiry Resources

NNSA has a shortage of experienced and qualified inquiry officials across the complex (at all sites), and some of the security incident organizations lack administrative support. The increase in incidents has outpaced staffing levels to report and conduct the inquiries. The shortage prevents timely investigation, reporting, and closure of incidents. It can also rush completion of an inquiry, impede a thorough investigation, and hinder the sites' ability to proactively reduce incidents. Some sites have difficulty completing the inquiry and reporting closure within 60 working days as required.

Organizations outside of the inquiry teams sometimes fail to provide timely and effective support to the team or official in incident resolution. For example, at one site, Human Resources does not review draft inquiry reports in a responsive manner to determine disciplinary action, and, at some other sites, line management does not conduct or support timely causal analysis or provide timely corrective action plans. One site had a cyber incident involving Sigma 15 weapon data on hold because no one had the access to forensically examine a hard drive at the site, and the site had not obtained resources from off-site to do so.

None of the contractor inquiry officials visited has been issued the DOE Basic Security Credential. Though infrequently needed, the Basic Security Credential allows inquiry officials to properly identify themselves on the few occasions when their authority is questioned. The DOE Basic Security Credential is avail-able for issuance and has been issued to contractor inquiry officials at some non-NNSA sites. One site office requested Basic Security Credentials for its contractor inquiry

officials from headquarters over a year ago and still had not received them at the time of our visit.

Each of the inquiry teams visited was at least four levels removed from the site director. The site director has responsibility for supporting and ensuring full investigation and reporting of incidents and complete, timely corrective actions. Excessive levels of management between the inquiry team and the site director can reduce the importance of the function in the eyes of site management and employees, and reduce site director awareness of incidents occurring at the site.

Many of the people assigned and available to conduct inquiries at the sites do not possess the access needed to perform inquiries into all of the potential incidents that could occur at the site. Each site director should have the capability to enlist people (external to the program that caused the incident) with appropriate accesses to quickly respond to and fully investigate any security incident that may occur at that site. Once an incident occurs, it may be too late to grant access, which delays the response to the incident, preventing an adequate inquiry.

Some sites allow the special security officer (SSO) for a SCIF or the SAP security manager to conduct inquiries into incidents in their own programs, which are among the most sensitive. This is not appropriate and many times is a clear conflict of interest. When this type of incident occurs, a cleared and appropriately trained individual—trusted by management and independent of the affected SCI or SAP—must be assigned to conduct a full inquiry. This person does not have to be an inquiry official from the IOSC team, but should be inquiry-trained and external to the affected program.

9.4 RECOMMENDATIONS

1. Provide timely interpretive guidance and training to ensure the IMI tables are consistently applied.[10] Ensure guidance on urgency of incident report submissions is clear.

2. Ensure individuals notify site offices of all incidents as they are categorized to provide timely oversight of incident categorization and eliminate or reduce the potential for incident miscategorization.

3. Eliminate the policy and practice of incident recategorization on the basis of a determination that no compromise occurred. The final inquiry report contains the information needed to indicate whether a compromise did or did not occur.

4. Consolidate reporting systems into a single system to eliminate redundant reporting, standardize reporting elements, and facilitate adoption of a common incident database. Use distribution controls at headquarters, rather than separate report formats, to ensure different categories of incidents are routed to the

[10] See Note 1, pp. 1-3 – 1-7.

appropriate people.

5. Establish a more rigorous process within DOE/NNSA headquarters to thoroughly review initial incident reports; monitor the inquiry progress; review final reports for adequacy of the inquiry, corrective actions, and analysis of underlying causes; and keep senior DOE/NNSA leadership appropriately advised.

6. Close incidents only after DOE/NNSA headquarters has reviewed and approved the final incident report, rather than upon receipt at headquarters.

7. Educate all organizations regarding the priority of incidents of security concern and importance of responsiveness and cooperation in the inquiry process. Encourage site managers and directors to educate their employees and management on the importance of timely support to inquiry teams.

8. Establish a more formal and disciplined process at sites to track security incident corrective actions to completion. Consider requiring site management to include findings and corrective action plans in a site-level corrective action tracking process involving senior line management to ensure corrective actions are adequate and complete. Ensure reviews are con-ducted to execute continuous improvement. Have all site offices randomly review corrective actions for completion during surveys, and have the Office of Independent Oversight and Performance Assurance (OA) review a sample during performance inspections.

9. As also recommended by the Chiles report, establish a dedicated and more effective formalized process within NNSA headquarters to disseminate incident lessons learned to the NNSA community.[11] Consider publishing a quarterly lessons-learned message for all DOE/NNSA sites, with procedures for ad hoc promulgation of urgent lessons learned.

10. Develop more meaningful security metrics that accurately measure the nature, frequency, and significance of incidents; the underlying root causes; and the timeliness of reporting, investigation, and corrective action development. Periodically provide these metrics to senior headquarters and site leadership, as well as appropriate security officials, to promote greater awareness of security performance and concerns.

11. Review the infraction programs and provide guidance for standardization to enable consistent application across DOE/NNSA sites. NNSA site offices should review the infraction programs at their facilities to ensure the infractions are administered consistently for federal employees and contractors.

12. Assess the adequacy of IOSC staff levels complex-wide to ensure they have sufficient people and expertise to conduct and report adequate, complete inquiries.

13. Issue the DOE Basic Security Credential to all DOE/NNSA-approved inquiry

[11] See Note 9.

officials.

14. Consider temporarily assigning the inquiry official as a direct report to site management during the course of an investigation to effectively reduce the number of management levels between the incident inquiry team and the contractor site director.

15. Ensure procedures are in place to avoid the perception that an individual conducting an inquiry has a conflict of interest or bias in the possible out-come of the inquiry. Discontinue the practice of having SSOs and SAP security managers conduct inquiries into incidents involving their own programs.

Section 10
Design Basis Threat Implementation

10.1 BACKGROUND

The events of September 11, 2001 dramatically illustrated that the accepted tenets of the then-existing postulated threat to nuclear weapons and material were no longer valid. As a consequence a new postulated threat was produced by the intelligence community in January 2003 and became the new foundation for the DOE's Design Basis Threat (DBT). The new DBT was promulgated by DOE in May 2003.

Countering a new, potentially larger, and more sophisticated threat to nuclear weapons and material has required senior leadership within NNSA to reevaluate existing security and protective forces and upgrade them to meet identified vulnerabilities. In fall 2003, NNSA took steps to begin implementing the new DBT: requesting initial cost inputs and draft implementation plans from the sites and hosting meetings at headquarters to get additional input and review the plans. Several interrelated issues needed to be resolved to get viable implementation plans and accurate associated costs; but, to meet budget-cycle requirements, NNSA and DOE pressed forward to obtain whatever time and cost estimates they could for DBT implementation. The stated goal is full implementation by the end of FY06.

In April 2004, the General Accounting Office (GAO) published a report which questioned whether this goal could be met for all sites.[1] Specifically, it questioned the time it took DOE to formulate the new DBT; its decision to use lesser threats than the Defense Intelligence Agency postulated threat; possible weaknesses in the criteria for protecting against new terrorist threats, such as chemical, biological, and radiological sabotage; and DOE's slowness in issuing guidance, preparing implementation plans, and developing adequate budgets.

[1] U.S. General Accounting Office, *DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat,* GAO-04-623, April 2004. Available from http://www.gao.gov/new/items/d04623.pdf.

10.2 SUMMARY

There has been insufficient collaboration between DOE and DoD and among NNSA sites in translating the intelligence community's postulated threat into security requirements. As a result, NNSA security standards differ:

- from those of DoD nuclear weapons facilities, because DOE/NNSA has taken a different approach to dealing with the postulated threat than that of DoD, and
- from site to site, because sites have interpreted terms such as insider threat, mission-critical facilities, escorting policies, and improvised nuclear devices (INDs) differently.

Determining whether NNSA will meet DBT implementation objectives by FY06 is difficult: the process for managing the program and funding requirements largely depends on the sites' interpretations of DBT requirements.

10.3 OBSERVATIONS

10.3.1 Insufficient Collaboration and Guidance

DOE/NNSA has taken a rational approach to converting the intelligence community's postulated threat into a risk-based DBT. The only substantive criticism is that the approach was taken in isolation, without any apparent collaboration with DoD, despite recommendations for greater coordination between the two departments.[2] On its own, DoD has belatedly adopted a dramatically different approach, not fully consistent with DOE's. The result of the profoundly different approaches is that the same nuclear weapons under nearly identical conditions are not protected under the same or equivalent security standards. From a national security perspective, the lack of security equivalency is inexplicable and unwarranted.

DOE/NNSA has not provided sufficient, clear guidance on DBT implementation to ensure consistent interpretation department-wide. DOE/NNSA headquarters and the sites have not sufficiently collaborated to develop a shared appreciation of the measures required to meet the new DBT. Examples of this lack of guidance and collaboration include the following:

- NNSA has not provided sufficient guidance to the sites for defining mission-critical facilities, which require a higher level of protection. Without this guidance, the sites are trying to determine whether they have mission-critical facilities with protection requirements as specified in the new DBT

although the sites can clearly identify the activities critical to their missions, NNSA headquarters should clearly identify the missions that are critical to national security. The inconsistent interpretation of mission-critical facilities is likely to greatly increase the cost of facility protection because the sites will err on the side of caution, unnecessarily requiring the deployment of more security resources than may be actually needed.

- As identified in a GAO report,[3] the criteria established for protection of facilities may not be sufficient. For example, the "industry standards" that sites are required to implement to protect against chemical sabotage have yet to be developed. Similarly, the criteria for protection against radiological sabotage may be inadequate to prevent radiological dispersal over wide areas (see Section 12).
- The guidance for sites with improvised nuclear device (IND) concerns is still evolving,[4] and it could eventually result in more costly than anticipated protection strategies. To date, sites have implemented inconsistent solutions for meeting this requirement.
- DOE policy does not clearly define the new DBT insider threats, particularly with respect to escorting policies; as a result various sites have interpreted the term differently. Policies regarding personnel allowed within protected areas, escorted or unescorted, differ from site to site. Some re-port certain acts as violations, and others do not; some apply a less rigorous policy than others. Some sites are interpreting the policy in their own interest, to require less work to be performed or to redefine the problem in a way that minimizes the need for protection strategies. For example, some sites have interpreted the DBT policy on escorting of non-Personnel Assurance Program (PAP)—now Human Reliability Program (HRP)—employees within the material access area (MAA) to mean escorted employees are exempt from being insider threats.

10.3.2 Inconsistent Site to Site DBT Implementation

The site to site implementation approach to DBT implementation has resulted in inconsistent interpretation of guidance across the complex:

- Some sites have conservatively interpreted the new DBT requirements and requested significant additional resources, while other sites (recognizing the existing tension between the new DBT requirements and available re-sources) have based their DBT implementation requirements on anticipated security budget levels.

[2] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, A Critical Independent Assessment of the U.S. Nuclear Command and Control System (U), Final Report, April 2002 (Top Secret).
[3] See Note 1.

- As discussed earlier, the weaknesses and uncertainties noted in the individual site vulnerability assessment (VA) and site safeguards and security plan (SSSP) processes create significant uncertainties in the validity of the assessments which underpin the new DBT implementation plans.

- One submitted SSSP acknowledges that a certain threat exists per the DBT, but then analytically excludes that threat and assumes the risk for that particular adversary capability. This practice—basing upgrades on an assessment that excludes specific DBT attributes—may prove costly if the site is ultimately required to implement all attributes of the DBT.

As discussed in Section 12, the lack of an enterprise-wide approach to special nuclear material (SNM) consolidation has significant implications for DBT implementation. The antiquated, dispersed facilities in which some SNM is stored require more security manpower and resources than more modern structures on a reduced footprint. Accordingly, the DBT implementation scope and costs are likely to be larger for NNSA's older facilities located within a larger protection footprint.

Finally, the site to site implementation approach complicates DOE/NNSA's ability to prioritize resource requirements to address the most critical vulnerabilities identified as part of the new DBT implementation. NNSA relies on individual site assessments and periodic independent OA performance assessments to validate DBT implementation, rather than directly performing its own assessments.

10.3.3 DBT Implementation Resources

It is difficult to assess whether there are adequate resources, programmed or planned, to meet the new DBT implementation deadline of FY06 because of many of the factors cited above—uncertainties associated with the sites' assessment methodologies, inconsistencies in the sites' interpretation of DBT policy requirements, potential funding impacts of SNM consolidation, and evolution of guidance on INDs, as well as the lack of a robust resource-requirements validation process as described in Section 13.

10.4 RECOMMENDATIONS

1. Collaborate with DoD to reconcile the differences between approaches to the postulated threat, and establish equivalent, if not identical, approaches to address it, such that protection standards for nuclear weapons and material are fully consistent for essentially equivalent conditions. The Nuclear Weapons Council [REDACTED] may be the appropriate forum for such collaboration.

2. Establish a collaborative process to achieve complex-wide consistency and standardization in DBT policy interpretation and implementation. DOE/NNSA must provide clear guidance on the definition of mission-critical facilities, protection requirements for INDs, criteria for protection against chemical and

[4] [REDACTED]An IND is a device designed or constructed outside an official government agency which has, appears to have, or is claimed to have the capability to produce a nuclear explosive.

radiological sabotage, and requirements associated with protection against the insider threat.

3. Adopt a comprehensive and integrated department-wide approach to DBT implementation by consolidating individual site DBT implementation plans into an NNSA master DBT implementation plan. As part of this consolidation, incorporate initiatives that have the potential to reduce re-source requirements, such as SNM consolidation and infrastructure recapitalization. This action will facilitate gap analysis, result in improved prioritization and utilization of scare resources, and assist in developing a realistic budget. The master DBT implementation plan should include the following:

   - Improved justification and validation of DBT implementation requirements based on more consistent and robust VAs, SSSPs, and performance-testing processes (see Section 7.)

   - Centralized responsibilities and accountability for plan validation and implementation within NNSA headquarters (see Section 13.)

4. As recommended in Section 13, in the near term, consider establishing an independent panel to validate the adequacy of funding to implement both the new.

Section 11
Security Research and Development Programs

11.1 BACKGROUND

During the Cold War, DOE had a vigorous research and development (R&D) program for improving nuclear weapon and material security systems. The end of the Cold War and the accompanying decline in support for the nuclear mission have eroded senior decision-makers' support of R&D for improving security systems and led to the deterioration of the once strong R&D management and coordination structures.

11.2 SUMMARY

DOE/NNSA lacks a strategic vision and plan for R&D, procurement, and installation of technologies to improve security across the enterprise. There is no centralized technology component within the department to oversee such a plan. As a consequence, security upgrade initiatives to employ new technologies are inconsistent. Sites are independently engineering upgrades without benefit of expert headquarters oversight and complex-wide collaboration. There is no robust technology R&D foundation for an advanced protection strategy.

11.3 OBSERVATIONS

DOE/NNSA lacks a strategic vision or plan for R&D, procurement, and installation of technologies to improve security across the enterprise. As reported by a federal advisory committee,[1] neither DoD nor DOE/NNSA have a robust R&D program that seeks innovative improvements to nuclear security. Over the years, both departments have changed security R&D programs from a "push" orientation, in which managers sought new and innovative ideas and approaches to nuclear security, to a "pull" orientation, in which they wait until a customer identifies a need and the willingness to "pay" for the development. As a result, both rely on older, dated protection technologies, mostly tied to expensive, man-power-intensive security programs.

[1] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System (U)*, Final Report, April 2002 (Secret).

The DOE *Strategic Security Plan* calls for the establishment of a

> Technology Development and Implementation Plan that will direct the identification, development, acquisition, and application of advanced technologies that will serve as the foundation for an advanced protection architecture.[2]

However, DOE/NNSA has not created a centralized technology component within the department to create such a plan and oversee technological policymaking, research, development, and procurement related to security.

In NNSA, individual laboratories and the Transportation Safeguards Division maintain very small R&D programs, most of which focus on improving existing designs and equipment instead of searching for new and innovative approaches. Some laboratories are engaged in technology R&D programs in their "work for others" programs (such as Department of Homeland Security work.) Self-directed, independent organizations at each site plan and maintain the various security systems. However, little effort has gone into standardizing and improving the systems complex-wide; as a result, each site employs its own unique systems, and the application of similar security resources is not standardized. Most of the limited attempts to standardize security-related items have focused on protective force equipment. Although DOE has quality panels and working groups devoted to this purpose, the sites have realized few technological or labor-saving benefits for security from these initiatives.

Security upgrade initiatives to employ new technologies are inconsistent. Sites are independently engineering upgrades without the benefit of knowledgeable over-sight or direction. Examples are as follows:

- Several sites are in various phases of perimeter upgrades. Rather than taking advantage of the possible synergy from combining upgrade design efforts, each is proceeding independently, possibly duplicating past efforts, wasting resources, and failing to adopt best-of-breed designs and practices.

- One site is planning to design and install a new perimeter intrusion detection system that will also provide denial at the perimeter. No accepted NNSA-wide strategic vision or policy drives this planning decision. Denial at the perimeter has not been demonstrated or been shown superior to denial systems located at the target itself.

On a positive note, some sites have adopted security upgrades that have clearly improved security. One has developed an innovative underground storage for infrequently-used special nuclear material (SNM.) Others have made simple procedural changes which have significantly improved security at little or no cost. One has closed a road to public access; another has permanently closed a site access gate.

[2] U.S. Department of Energy, *The Department of Energy's Strategic Security Plan,* March 2003.

Both initiatives have significantly reduced potential vulnerabilities and are good examples of how changes in policy, procedures, or operations can improve security and conserve resources. However, other sites are probably not aware of these initiatives and have not benefited from their example.

There is a prevalent attitude within NNSA that technology is not as flexible as manpower. As requirements change, redeploying security manpower is relatively easy and effective in the short term, but long-term considerations need to include technology. In addition, life safety issues have historically overshadowed the potential use of new security technologies. While safety is essential, a zero tolerance approach to safety deficiencies often precludes safety personnel from working with the operational communities to develop acceptable risk-based approaches to improve security through the use of new technologies.

11.4 RECOMMENDATIONS

1. Reinvigorate nuclear security R&D programs, with an immediate focus on developing improved access delay and denial technologies, including disrupting, disabling, or lethal systems. NNSA should seek to integrate advanced security technologies into facility construction and refurbishment planning processes to anticipate and mitigate emerging threats.

2. Establish a centralized technology component within DOE/NNSA to formulate a Technology Development and Implementation Plan, or equivalent, as authorized in the DOE *Strategic Security Plan*. Assign responsibility, accountability, and resources to this organization to oversee and coordinate policymaking, research, development, procurement, and application of advanced security technologies that can serve as the foundation of an enhanced protection architecture.

3. Collaborate closely with DoD and other government agencies, such as the Technical Security Working Group, to collectively pursue advance security technologies. Leverage R&D initiatives in the “work for others” programs.

4. Consider a reasonable standardization of site security system architecture, design, and implementation, including the security upgrades in progress. NNSA site oversight and headquarters should be involved in each critical decision stage of security upgrade projects. Project rationale and justification should be scrutinized and compared with complex-wide needs and overall direction. This would optimize the use of security up-grade funding and present a clear direction for security strategy.

5. Establish an NNSA R&D security panel to periodically review, evaluate, and critique R&D programs related to security.

Section 12
Nuclear Materials and Waste Storage

12.1 BACKGROUND

A large percentage of DOE/NNSA security resources are devoted to protecting nuclear weapons and special nuclear material (SNM). The wide spectrum of SNM storage facilities—in age, condition and location—drive many of these resource requirements. Because of the evolution of the nuclear weapon infrastructure during the Cold War, the storage facilities tend to be geographically dispersed. SNM is stored at these facilities because of the sites' past and present missions. Radiological waste is also stored at many NNSA sites; protection standards for radio-logical waste are less stringent than those for SNM.

12.2 SUMMARY

DOE/NNSA lack an enterprise-wide plan for SNM consolidation. A lack of collaboration between NNSA and other elements of DOE, such as Environmental Management (EM) and Nuclear Energy (NE), may preclude some secure and cost effective alternatives for consolidation from consideration. DOE/NNSA should seek to make greater use of underground storage. Some radiological waste storage areas may lack adequate protection against sabotage which could cause wide area radiological dispersal.

12.3 OBSERVATIONS

12.3.1 SNM Consolidation

DOE/NNSA has no comprehensive complex-wide SNM consolidation strategy, and NNSA has not coordinated effectively in the past with other program offices in DOE, such as EM and NE, Science and Technology (NE), with respect to underutilized or emptied SNM storage facilities, some of which are underground.

One site has old and deteriorating SNM storage locations, some of which were not designed or intended for long-term storage. Their nature, design, and geographical dispersal make it difficult to provide adequate security against a modern, sophisticated threat. As a consequence, the labor and security technology costs to adequately protect these locations are far greater than those for equivalent, more modern storage facilities. The geographic dispersal also creates multiple potential vulnerabilities. In effect, an aging infrastructure is a primary driver of security resources.

Although isolated efforts have been made to relocate some SNM or design new storage facilities, a detailed, department-wide, comprehensive SNM consolidation study that includes an overall cost-benefit analysis is lacking. Funding requests for SNM transfers and upgrade construction projects could benefit from this type of study.

Past studies have specifically recommended the need to review the existing SNM storage infrastructure and the consolidation of SNM.[1] They found newer, state-of-the-art storage infrastructures that are currently underutilized or empty.

It appears that some SNM is being stored at some DOE/NNSA sites more for convenience than necessity. Some sites perceive that SNM holdings are inextricably tied to their missions. Some quantities of nuclear materials are stored to allow scientists access to their work; however, moving this material to more secure and remote sites, and bringing the scientists and mission to the material would de-crease the number of storage locations and consolidate SNM in more secure, un-populated areas.

A number of underutilized facilities, far from populated areas, could potentially be used to consolidate storage of nuclear weapons and material. The Device Assembly Facility (DAF) at the Nevada Test Site (NTS) is a logical choice. NNSA has only recently begun to relocate SNM to the DAF.

EM's emphasis on closure and objectives related to cleanup and reducing the Department's footprint has hindered the coordination between NNSA and other DOE program offices for evaluating existing SNM infrastructures. Evaluating these facilities—some of which are underutilized, soon to be empty, or empty—may have cost and security benefits. For example, a relatively new 160,000-square-foot, three-level, underground, reinforced-concrete storage facility at the Idaho National Engineering and Environmental Laboratory (INEEL), has never been used.

As far as other underutilized or empty storage vaults, EM could still reach its footprint goals if a DOE EM building could be used to store NNSA SNM, which would entail a transfer of building ownership to NNSA. This effort could potentially also save DOE EM funds if the building(s) could be put to NNSA use thus eliminating the need for EM to commit and spend Deactivation and Decontamination (D&D) funds.

12.3.2 Underground Storage

Insufficient emphasis has been given to the inherent long-term advantages of underground storage. An underground storage vault may initially cost more to build; but, in the long term, the facility is likely to improve security and conserve resources. From a protective system viewpoint, above-ground storage presents additional protection challenges and costs associated with less complicated adversary

[1] *Review of the Special Security Study (for the DOE Security Council),* 1998, and *A Security Architecture for NNSA (A Special Security Study),* 2002.

barrier breaching and greater vulnerability to airborne threats. While some facilities (e.g. the Highly Enriched Uranium Material Facility at the Y-12 Plant) cannot be placed underground for geological reasons, NNSA should seek underground storage wherever possible.

12.3.3 Protection of Radiological Material

DOE/NNSA protection requirements for radiological waste and material storage are minimal or nonexistent. In comparison to other departmental assets such as SNM, classified and other departmental security interests, there is significantly less protection afforded to radiological waste. Protection for radiological waste currently amounts to a fenced boundary area with no consideration given to vehicle barriers, alarms or an armed guard presence, nor is there any requirement for the protective force to develop response plans or conduct performance testing for this type of material. In some cases, assets such as the protective force already exist at a site where radiological materials are stored, but no requirement exists to have them provide any level of protection to this potential adversary target. In some cases there is more access control, detection, and response dedicated to DOE and NNSA owned and operated administrative office buildings than what is applied to radiological waste and material storage areas.

This is not intended to imply that the degree of protection afforded to SNM should be used as a basis for radiological storage. Rather, there is a concern that the lack of protection afforded to radiological materials could make these materials an attractive target to an adversary threat. It is recognized that some of the radiological holdings within the department do not exceed the publicized off-site public dose rates, which precludes them from being identified as a radiological sabotage target. However, even if the material is under this threshold, based upon the type and significant quantities of radiological waste storage areas within the department, a terrorist sponsored wide-area radiological dispersal could cause evacuation of local populations, shut down of site operations for a considerable period of time and considerable cleanup costs.

12.4 RECOMMENDATIONS

1. DOE/NNSA should urgently develop a comprehensive plan for SNM consolidation based on the significant amount of funding that will continue to be spent at NNSA SNM storage facilities that may later become candidates for SNM removal once the consolidation plan is completed. Nuclear weapons and SNM should be consolidated at fewer, better protected sites and where practical, in underground storage sites (e.g. DAF). Where consolidation in underground storage sites is impractical, above-ground structures should be modified to earth-covered structures where feasible to reduce the potential vulnerability from ground or air attack. This effort should receive appropriate emphasis considering

the increased protection required to meet the new DBT. A thorough review of existing infrastructures within DOE to determine if existing structures could be used to consolidate SNM, minimize new construction cost, increase security and potentially save DOE D&D funds should be conducted as part of this plan.

2. In parallel with the nuclear weapons assessment recommended by the End to End Review,[2] direct a feasibility assessment of providing underground storage for all SNM. Evaluate the adequacy of current protection requirements for radiological materials and make cost effective determinations for those areas that can be improved upon.

3. Evaluate the adequacy of current protection requirements for radiological materials and make cost effective determinations for those areas that can be improved upon.

4. Reevaluate the criteria for radiological sabotage to provide sufficient protection strategies for radiological waste against wide-area radiological dispersal.

[2] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System (U)*, Final Report, April 2002 (Top Secret).

Section 13
Security Resources and Requirements

13.1 BACKGROUND

From the beginning, NNSA senior management committed to a planning, programming, budgeting, and evaluation (PPBE) process modeled on the DoD system. A PPBE process uses short- and long-term planning to define program requirements and matches requirements with budgetary resources. The Administrator established the overall objective that the PPBE process become the core management protocol for NNSA.[1]

The PPBE process allows site managers and contractors to define site resource needs and evolve them into unified budgets, including security requirements, be-fore they are evaluated against all program needs at headquarters. Decisions about resources can be made in an integrated manner, taking into account administration policy and the needs of the entire complex. The PPBE process links "long-range planning (*what* NNSA needs to do) with programming (*how* NNSA will accomplish it), with budgeting (obtaining *resources* and applying fiscal *constraints*), and with evaluation (*verifying* that the mission has been accomplished as planned)."[2] NNSA began using the PPBE system for the past three budget years, starting with FY02:

- For FY02, the plan for managing appropriations reflected an integrated NNSA PPBE processes for financial execution, closely tied to milestones and deliverables contained in work authorizations. NNSA began implementing an automated system to streamline budget execution record keeping.

- For FY03, the Office of Management and Budget (OMB) reviewed the NNSA-developed budget, with input from DoD regarding NNSA's weapons-related requirements and associated budgets.

- For FY04, each program component developed an integrated plan. The issuance of the *Five-Year Program and Fiscal Guidance* began the

[1] U.S. Department of Energy, Office of Inspector General, Office of Audit Services, *Audit Report: National Nuclear Security Administration's Planning, Programming, Budgeting, and Evaluation Process,* DOE/IG-0614, August 2003. Available from http://www.ig.doe.gov/text/ig-0614.rtg.
[2] Congress, House, Special Oversight Panel on Department of Energy Reorganization Committee on Armed Services, February 26, 2002. Statement of John A> Gordon, Undersecretary of Energy and Administrator for Nuclear Security National Nuclear Security Administration, U.S. Department of Energy. Available from http://www.nnsa.doe.gov.

"programming" step in the NNSA PPBE process. The FY04 budget submitted to Congress fully met the congressional intent of having a PPBE system driving the resource decision process.[3]

By design, NNSA headquarters is responsible for strategic and program planning, budgeting, and oversight of research, development, and nonproliferation activities. Headquarters manages the PPBE process, and the field offices execute it. The process recognizes that each of the five principal program or management elements within NNSA, including Infrastructure and Security, manages program execution and interface with contractors differently.

The *Safeguards and Security (S&S) Program Management Plan* uses formalized planning and measurement techniques that align with the four PPBE phases (Table 13-1).[4]

Table 13-1. Process Alignment with Program Management

PPBE phase	S&S Program Management Plan
Planning	S&S Strategic Plan, S&S Multiyear Program Plan
Programming	S&S Programming and Budget Integration
Budgeting	Work Implementation and Site Change Control
Evaluation	Contractor Performance Evaluation and NA-70 Implementation Phase

13.2 SUMMARY

NNSA has made good progress in implementing the PPBE process, but much remains to be done. The lack of an enterprise approach to security planning, inconsistent site-by-site interpretation and implementation of security resource requirements, lack of collaboration among the participants in the budget process, lack of a centralized budget validation process, and a cumbersome and unresponsive reprogramming process complicate rational resource planning, programming, budgeting, and evaluation to meet evolving security needs.

13.3 OBSERVATIONS

13.3.1 PPBE Implementation

NNSA has made significant progress in the implementation of the PPBE process. The migration to the 5-year PPBE system is forcing more disciplined and consistent

[3] See Note 2.
[4] National Nuclear Security Administration, *NNSA Safeguards and Security Program Management Plan: Work Implementation, Control, and Performance Evaluation at NNSA Sites*, February 2004.

planning in the resource allocation process for security. NNSA is perceived as the model for the rest of DOE, which has been slower to embrace the multi-year PPBE process. However, much remains to be done. The weakest elements in the process are planning and evaluation.

Inconsistent site-to-site interpretation and implementation of security requirements have complicated accurate prioritization of security needs and rational re-source allocation decisions across the NNSA complex. The decision makers, who establish security requirements, the sites, who establish resource requirements, and the resource allocators, who program resources, lack the collaboration needed to ensure that security risk is appropriately balanced across the complex. The lack of an enterprise approach to security and the variation in security policy interpretation and implementation deprive NNSA of the assurance that appropriate priority is accorded to assets needing protection and precludes potential budget savings through economies of scale.

NNSA headquarters has not established a budget validation process. Individual site contractor estimates, which form the basis for budget requests and resource allocation decisions, lacked validation for FY03 and FY04. As identified by the DOE Inspector General, NNSA lacks an independent analysis group to facilitate centralized resource allocation decisions.[5]

Because the NNSA and DOE budgeting processes differ, site contractors are burdened with providing budget and financial information to both organizations.

13.3.2 Security Funding

There is a general debate within DOE/NNSA on the relative merits of direct versus indirect security funding. (DOE has made a recent decision to retain direct line security budgeting.) Direct funding ensures appropriated funds for safeguards and security are not diverted for other purposes; however, direct funding lacks the flexibility to provide additional funds, beyond appropriated levels, to meet emerging needs. In contrast, indirect funding provides great flexibility but lacks congressional visibility in how funds are utilized and creates a potential that safeguards and security may be neglected. While there are pros and cons to each method, the real problem is not direct funding versus indirect funding but lack of sufficient flexibility in reprogramming authority to be sufficiently responsive to emerging security needs. The existing reprogramming process is characterized by the DOE/NNSA senior comptroller officials as a “nightmare.” One of the recognized problems is the poor quality of the reprogramming request justifications.

There is a widespread perception that there are insufficient security resources to implement both the new DBT security requirements by FY06 (see Section 10) and the evolving cyber security threat requirements (based on the cyber DBT initiative discussed in Section 5).

[5] See Note 1.

13.4 RECOMMENDATIONS

1. Accelerate the transition to a multiyear PPBE process, which:

   - promotes greater collaboration among the security requirement setters, security resource requesters, and resource allocators;
   - validates site contractor security cost estimates;
   - facilitates more meaningful site-to-site security comparisons;
   - promotes an enterprise view of security priorities and enables a more rational prioritization of security needs; and
   - promotes greater savings from complex-wide security initiatives (for example, from special nuclear material consolidation and migration to underground storage).

   Place particular emphasis on strengthening the planning and evaluation elements of the PPBE process. As part of this initiative, adopt an enterprise-wide, risk-based, security model, as recommended by the Commission on Science and Security, to enable NNSA to better "balance resources, which are limited, and risk, which can never be eliminated."[6] A better understanding of the resource and security tradeoffs would also facilitate creation of a comprehensive NNSA-wide S&S strategic plan, which NNSA envisions as part of the first phase of the PPBE process.

2. Encourage DOE to adopt a similar PPBE process to simplify site contractor budget submissions.

3. Establish an independent analysis group to facilitate centralized resource allocation decisions. This type of group will improve the PPBE process through program reviews, alternatives analysis, and cost estimate validation. In the near term, consider establishing an independent panel to validate the adequacy of funding to implement both the new DBT by FY06 and evolving cyber security threat requirements.

[6] Commission on Science and Security, *Science and Security in the 21st Century: A Report to the Secretary on the Department of Energy Laboratories*, John J. Hamre, commission chair, Anne Wikowsky, project director, April 2002, p.xv. Executive summary available from http://www.csis.org/css/ExecSummary.pdf.

4. Seek DOE, OMB, and congressional approval to grant the NNSA Administrator:

   - limited reprogramming authority for the S&S program and
   - authority to submit streamlined formal reprogramming requests directly to OMB and Congress when NNSA needs to transfer security funds beyond the limits of reprogramming authority.

Limited reprogramming authority and streamlined procedures for formal reprogramming requests will go a long way in providing the flexibilities of an indirect funding method but retain the transparency and accountability of the present direct funded budgeting of, and accounting for, security funds.

5. Improve the quality of reprogramming justifications.

Section 14
Security Contracting

14.1 BACKGROUND

In February 2002, NNSA reported to Congress an acquisition strategy to improve accountability. In that report, NNSA stated that it

> must maximize enterprise-wide procurement opportunities and integrate procurement considerations directly with program and project management organizations. To do this, NNSA will develop and implement a simpler, less adversarial contracting approach that capitalizes on the private-sector expertise and experience of its management and operating contractors while simultaneously increasing their accountability for performance on NNSA programs.
>
> The NNSA Office of Procurement and Assistance Management (PAM) is responsible for creating policies and establishing practices that will enable the organization to achieve its goals. … PAM will (1) maximize enterprise-wide procurement opportunities, (2) ensure the integrity of the acquisition process, (3) enhance performance based contracting and rely on commercial standards for judging contractor support functions, (4) streamline procurement processes, and (5) improve NNSA supply chain and logistics management. NNSA will also create an acquisition corps to develop staff with an enterprise wide perspective of acquisition management.[1]

NNSA has recently proposed a formal rulemaking as the first step in establishing a tailored NNSA acquisition regulation that is independent of the existing DOE acquisition regulation.

Additionally, the Secretary of Energy has recently proposed consideration of alternatives to the existing security contract arrangements.

14.2 SUMMARY

The contractual relationships for security, which NNSA has inherited, are varied and diverse. Current and past security contracts insufficiently delineate performance expectations. The NNSA move to emphasis on broad, performance-based contracting—with appropriate focus on security as a key element of mangement and operations (M&O) contractor performance—is a very positive, overdue step. NNSA has been operating under the Department of Energy Acquisition Regulation (DEAR);

[1] National Nuclear Security Administration, *Report to Congress on the Organization and Operations of the National Nuclear Security Administration*, February 2002.

however, NNSA requires a unique set of tailored acquisition regulations and a common, standardized policy and practices to enable greater consistency and discipline across its breadth of national security missions.

14.3 OBSERVATIONS

The contractual relationships for security, which NNSA inherited, are varied and diverse. The former DOE operations offices established the reporting relation-ships, and the models are still in place at NNSA today. Under the three basic con-tract types, security is the responsibility of one of the following:

- a management and operations (M&O) contractor,
- a contractor that reports directly to the government—separate from the M&O contractor—or
- a subcontractor to the M&O contractor.

The latter two are known as "non-M&O" contracts. In general, government managers and contractors prefer a contract vehicle that establishes a direct relationship between the government officials and contractors responsible for security over one where the security contractor is a subcontractor to the M&O contractor. Government managers particularly tout the benefits of direct security contract management over that of indirect management.

Dissatisfaction with security performance at some sites has led to proposals to consider alternatives to the present arrangement of site security contracts, including:

- a single security contract for the entire NNSA complex rather than separate contracts for each individual site, or
- federalization of site security forces, or at least selected elements of the site security forces, similar to the Transportation Safeguards Division.

Consideration has also been given to using the site security contracts as small business set asides.

Current and past security contracts insufficiently delineate performance expectations. The NNSA move to emphasis on broad, performance-based contracting—with appropriate focus on security as a key element of M&O contractor performance—is a very positive, overdue step.

Until recently, DOE/NNSA has not used the full range of options available for incentivizing security contract performance. It has unnecessarily limited itself to a few incentives (such as award fees and termination), when a wider range could be

used (as identified in the FAR, recommended by the Blue Ribbon Commission Report,[2] and contained in a proposed acquisition regulation under consideration within NNSA). Award fees—because they generally represent a small percentage of contract value, are structured to be regressive in nature, and are relatively predictable—provide limited motivation to contractor behavior. Security contracts that incentivize the contractors with potential time extensions (such as award-term extensions for superior performance) or terminations or recompetition of their contracts for poor performance are far more influential than those with award fee incentives.

Security contractors are tacitly disincentivized from promoting initiatives that would simultaneously improve security and reduce security staffing requirements, such as improved technology or special nuclear material (SNM) consolidation, because the security staffing requirements primarily drive the contract revenue value.

Many of the findings of the Blue Ribbon Panel, which focused solely on DOE laboratory M&O contracts, apply to the existing security contracts within NNSA. Ratings inflation, questionable objectivity of site office ratings, excessive numbers of performance reviews, weak linkage of reviews to compete-or-extend decisions, high cost of competitions, ineffectiveness of incentives, and weak delineation of performance expectations are all characteristic concerns of the pre-sent NNSA security contract arrangements.

Since its inception, NNSA has been operating under the DEAR; however, the DEAR is a one-size-fits-all regulation that legitimately seeks to accommodate the disparate needs of DOE's many diverse program elements—solar energy, fossil energy, energy regulation, site closures, etc. As a result, the DEAR monolithically deals with a host of complex, multifaceted acquisition policies, issues, and approaches. Additionally, the DEAR does not reflect the statutory prohibition against DOE exercising authority, direction, or control over NNSA and its con-tractors (50 U.S.C. 2403).

NNSA's organizational structure and operating philosophy as a corporate enterprise are unique within DOE and require a unique set of tailored acquisition regulations. In addition, NNSA has identified several contracting and contract management initiatives to better control and motivate its laboratories, plants, and test site, such as enterprise acquisitions, supply chain management, and a simplified fee policy and award term incentives. NNSA is also moving toward consolidating disparate systems and guidance into common, standardized policy and practices to enable greater consistency and discipline across its breadth of national security missions.

[2] U.S. Department of Energy, Blue Ribbon Commission on the Use of Competitive Procedures for the Department of Energy Labs, *Competing the Management and Operations Contracts for DOE's National Laboratories,* November 2003. Available from http://www.seab.energy.gov/publications/brcDraftRpt.pdf.

Nearly a year ago, NNSA proposed a formal rulemaking as the first step in establishing a tailored NNSA acquisition regulation independent of the DEAR. This NNSA-unique regulation remains in a process of review and comment within DOE.

Site managers are generally designated as the fee determination official for non-M&O security contracts. Such desegregation leads to perceptions of favoritism and bias because of the close working relationship between site managers and security contractors. Additionally, such designation leads to a wide variation in performance evaluation from site to site.

14.4 RECOMMENDATIONS

1. Continue, with urgency, the development of standardized contracts (both M&O and security where separate) that identify and define desired performance in clear and measurable terms, and utilize the full range of incentives to reward successful performance, including longer-duration security contracts with periodic evaluations to determine an extension or competition. Promote better linkage between performance and the compete-or-extend decision.

2. Evaluate with extreme thoroughness, any proposed alternatives to the pre-sent arrangement of individual site security contracts, commensurate with the gravity of the security mission. Potential risks and benefits need to be carefully assessed. Reject experimental and unvalidated alternatives.

3. Incentivize contractors by rewarding them for initiatives that lead to improved security through improved technology and processes that will en-able lower security staffing costs (such as SNM consolidation).

4. Have DOE formally support NNSA in the creation of an acquisition regulation, independent of the DEAR, tailored to support NNSA's unique mission.

5. Elevate the designation of fee determination official (FDO) for security contracts from site managers to either the NNSA Administrator or the new Associate Administrator for Defense Nuclear Security (NA-70). Such action would:

   - elevate the site contractor's security performance to headquarters level,
   - enhance an enterprise approach to performance evaluations, and
   - mitigate against perceptions of lack of site manager objectivity be-cause site managers work so closely with security contractors.

Section 15
Past Studies

15.1 BACKGROUND

Over the years, dozens of reports from various committees, panels, and DOE organizations have identified and addressed issues the same as or similar to those in this report. Many reports addressed DOE before the formation of NNSA, but several examine the issues since NNSA's creation.

As one report stated,

> Management and security problems have recurred so frequently that they have resulted in nonstop reform initiatives, external reviews, and changes in policy direction. As one observer noted in Science magazine in 1994: "Every administration sets up a panel to review the national labs. The problem is that nothing is done."[1]

15.2 SUMMARY

Past studies and reviews of DOE/NNSA security have reached similar findings regarding the cultural, personnel, organizational, policy and procedural challenges which exist within DOE and NNSA. Many of these issues are not new; many continue to exist because of a lack of clear accountability, excessive bureaucracy, organizational stovepipes, lack of collaboration, and unwieldy, cumbersome processes. There are also many other contributing reasons for the failure to implement corrective action. Classified or sensitive information cannot always be shared. Organizational changes and staff reductions impede corporate memory and achievable workload. Lack of prioritization confuses the important with the trivial and the urgent with the non-urgent.

15.3 OBSERVATIONS

Robust, formal mechanisms to evaluate findings, assess underlying root causes, analyze alternative courses of action, formulate appropriate corrective action, gain approval, and effectively implement change are weak to non-existent within DOE/NNSA. Of particular concern, DOE/NNSA has failed to take decisive action to the findings and recommendations of the End-to-End Review and has been slow to

[1] President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

respond to the requirements of [REDACTED]current guidance (which had its origins in the End-to-End Review)[2] despite the gravity of these documents.

Appendix B contains a partial list of past studies and reports addressing similar security subjects to this review.

15.4 RECOMMENDATION

Develop, with urgency, a more robust, integrated DOE/NNSA-wide process to provide accountability and follow-up on security findings and recommendations.

[2] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System* (U), Final Report, April 2002 (Secret).

Bibliography

The panel specifically cites the following documentation in the text of this report. This bibliography represents only a small portion of the documentation the panel reviewed in the course of this assessment.

Commission on Science and Security, *Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories*, John J. Hamre, Commission Chair, Anne Witkowsky, Project Director, April 2002. Executive summary available from http://www.csis.org/css/ExecSummary.pdf.

Congress, House, Special Oversight Panel on Department of Energy Reorganization Committee on Armed Services, February 26, 2002. Statement of John A. Gordon, Under Secretary of Energy and Administrator for Nuclear Security National Nuclear Security Administration, U. S. Department of Energy. Available from http://www.nnsa.doe.gov/.

Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347, Title III, December 2002.

Federal Register, Volume 69, Number 129, July 2004. Available from http://edocket.access.gpo.gov/2004/04-15331.htm.

Letter, from Kenneth A. Minihan, President and Chairman of the Board, SASA, to directors of various agencies, February 13, 2004. Available from www.greaterla-isac.com/docs/sasaltrtodci.doc.

Letter, from G. Peter Nanos et al., Laboratory Directors, to Kyle McSlarrow, Deputy Secretary, October 10, 2003.

National Defense Authorization Act for Fiscal Year 2000, Public Law 106-65, Section 3212(b)(2).

National Nuclear Security Administration, "NNSA Announces Security Initiatives for Weapons Laboratories," Press Release, July 8, 2003.

National Nuclear Security Administration, *Functions, Responsibilities and Authorities Manual*, May 2003.

National Nuclear Security Administration, NNSA Policy Letter 14.1, *Cyber Security Program*, September 2003.

National Nuclear Security Administration, *NNSA Safeguards and Security Pro-gram Management Plan: Work Implementation, Control, and Performance Evaluation at NNSA Sites*, February 2004.

National Nuclear Security Administration, *NNSA Safeguards and Security Strategic Plan*, June 2003.

National Nuclear Security Administration, *Report to Congress on the Organization and Operations of the NNSA*, February 2002.

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

U.S. Department of Energy and Department of Defense, *Joint DOE/DoD Nuclear Weapon Classification Policy Guide*, CG-W-5, January 1984.

U.S. Department of Energy, *The Department of Energy's Strategic Security Plan*, March 2003.

U.S. Department of Energy, DOE Directives System Working Group, Office of Management, Budget and Evaluation, *Report on Streamlining Directives System, presented to the DOE Management Council*, July 23, 2002.

U.S. Department of Energy, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents*, DOE Notice 205.4, March 2002.

U.S. Department of Energy, *Identifying and Protecting Official Use Only Information*, DOE Order 471.3, April 2003.

U.S. Department of Energy, *Incidents of Security Concern*, DOE Order 471.4, March 2004.

U.S. Department of Energy, memorandum from Bill Richardson, Secretary of Energy, to John T. Conway, subject: *Providing Revision 1 of the 2000-1 Implementation Plan*, January 19, 2001.

U.S. Department of Energy, memorandum from Edward McCallum, Director, Office of Safeguards and Security, to DOE director distribution, subject: *Enhanced Target Folders Development and Use*, June 4, 1998.

U.S. Department of Energy, memorandum from Robert Card, Under Secretary, to Field Operation Office Directors, subject: *Design Basis Threat*, May 20, 2003

U.S. Department of Energy, memorandum from Spencer Abraham, Secretary of Energy, to Lead Program Secretarial Officers, subject: *Reporting Incidents of Security Concern*, June 14, 2002.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Audit Report: National Nuclear Security Administration's Planning, Programming, Budgeting, and Evaluation Process*, DOE/IG-0614, August 2003. Available from http://www.ig.doe.gov/text/ig-0614.rtf.

U.S. Department of Energy, Office of Management Communications, "Department of Energy Directives Checklist," Directives, Regulations, and Standards, August 2004. Available from http://www.directives.doe.gov/cgi-bin/currentchecklist#POLICY

U.S. Department of Energy, Office of Management, Budget and Evaluation, *RevCom Review and Comment System*, August 2004. Available from http://www.revcom.doe.gov/.

U.S. Department of Energy, *Protective Force Program Manual*, DOE Manual 473.2-2, June 2000.

U.S. Department of Energy, *Reporting Incidents of Security Concern*, DOE Notice 471.3, April 2001.

U.S. Department of Energy, *Safeguards and Security Program*, DOE Order 470.1, September 1995.

U.S. Department of Energy, *Security Incident Notification Report*, Form 471.1.

U.S. Government Accountability Office, *DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat*, GAO-04-623, April 2004. Available from http://www.gao.gov/new.items/d04623.pdf.

United States Nuclear Command and Control System Federal Advisory Commit-tee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System* (U), Final Report, April 2002 (Top Secret).

Appendix A
Security Plan Status

Table A-1 shows the status of security plans for the various sites.

Table A-1. DOE NNSA Security Plan Status Summary

Facility	Type	Date
Kansas City Plant	FSP	April 2004
Lawrence Livermore National Laboratory	SSSP	January 2001
Los Alamos National Laboratory	SSSP	September 30, 1999
• Bio Level 3 (LANL)	FSP	June 18, 2002
Nevada Test Site	SSSP	August 1, 1998
• Remote Sensing Laboratory	FSP	January 28, 2004
Office of Secure Transportation NA-15	SSSP	October 2001
Pantex Plant	SSSP	January 2001
Sandia National Laboratories		
• California	FSP	January 2003
• New Mexico	SSSP	November 2000
• Tonopah Test Range	SSSP	September 7, 2001
Savannah River Site Office (Defense Programs Tritium Facilities)	FSP	February 18, 2004
Y-12 Plant	SSSP	May 20, 2004

Appendix B
Past Studies

This appendix lists past studies that pertain to DOE and NNSA security. They are listed under the sections to which they pertain.

SECTION 2. CULTURE

Chairman, House Armed Services Committee, *Reforming the Department of Energy*, National Security Report Vol. 3, Issue 3, September 1999.

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

U.S. Department of Energy, memorandum from Deputy Secretary of Energy for All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

U.S. Government Accountability Office, *Improvements Needed In DOE's Safeguards and Security Oversight*, GAO RCED-00-62, Report to the Chairman, Committee on Commerce, House of Representatives—Nuclear Security, February 2000.

U.S. Government Accountability Office, *Major Management Challenges and Program Risks*, GAO-01-246, Performance and Accountability Series, January 2001.

U.S. Government Accountability Office, *Nuclear Security—DOE Faces Security Challenges in the Post September 11, 2001 Environment*, GAO-03-896, Re-port to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, June 2003.

U.S. Government Accountability Office, *Nuclear Security—Improving Correction of Deficiencies at DOE's Weapons Facilities*, GAO RCED 93-10, Report to the Chairman, Subcommittee on Environment, Energy, and Natural Re-sources, Committee on Oversight and Investigations, House of Representatives, November 1992.

U.S. Government Accountability Office, *Nuclear Security—Lessons to Be Learned From Implementing NNSA's Security Enhancements*, GAO-02-358, Report to the Chairman, Committee on Armed Services, Special Oversight Panel on DOE Reorganization, House of Representatives, March 2002.

U.S. Government Accountability Office, *Nuclear Security—NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives May 2003.

U.S. Government Accountability Office, *Safeguards and Security Planning at DOE Facilities Incomplete*, GAO RCED-93-14, Report to the Chairman, Subcommittee on Oversight and Investigations, Nuclear Security, December 1992.

U.S. Government Accountability Office, *Safeguards and Security Weaknesses at DOE Weapons Facilities*, GAO RCED-92-39, Report to the Chairman, Subcommittee on Oversight and Investigations, December 1991.

U.S. Government Accountability Office, *Security Issues at DOE and Its Newly Created National Nuclear Security Administration*, GAO RCED-00-123, Testimony before the Subcommittee on Energy and Power and the Subcommittee on Oversight and Investigations Committee on Commerce, Nuclear Security, March 2000.

SECTION 4. SECURITY POLICY

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

A Security Architecture for NNSA—A Special Security Study (Hagengruber study), March 2002.

U.S. Department of Energy, Office of Inspector General, Office of Inspections, *Summary Report on Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process*, DOE-IG-0482, September 2000.

U.S. Government Accountability Office, *Improvements Needed In DOE's Safeguards and Security Oversight*, GAO RCED-00-62, Report to the Chairman, Committee on Commerce, House of Representatives—Nuclear Security, February 2000.

U.S. Government Accountability Office, *Nuclear Safety, Potential Security Weaknesses at* [site name] *and Other DOE Facilities*, GAO RCED-91-12, Report to the Congressional Requesters, October 1990.

U.S. Government Accountability Office, *Nuclear Security—Lessons to Be Learned From Implementing NNSA's Security Enhancements*, GAO-02-358, Report to the Chairman, Committee on Armed Services, Special Oversight Panel on DOE Reorganization, House of Representatives, March 2002.

U.S. Government Accountability Office, *Nuclear Security—NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives May 2003.

U.S. Government Accountability Office, *Safeguards and Security Weaknesses at DOE Weapons Facilities*, GAO RCED-92-39, Report to the Chairman, Subcommittee on Oversight and Investigations, December 1991.

SECTION 5. CYBER SYSTEM SECURITY

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

U.S. Government Accountability Office, *Major Management Challenges and Program Risks*, GAO-01-246, Performance and Accountability Series, January 2001.

U.S. Government Accountability Office, *Safeguards and Security Weaknesses at DOE Weapons Facilities*, GAO RCED-92-39, Report to the Chairman, Subcommittee on Oversight and Investigations, December 1991.

SECTION 6. COUNTERINTELLIGENCE

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

SECTION 7. SITE SAFEGUARDS AND SECURITY PLAN, VULNERABILITY ASSESSMENTS, AND PERFORMANCE TESTING

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

U.S. Department of Energy, memorandum from Deputy Secretary of Energy, to All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Protective Force Performance Test Improprieties*, DOE-IG-0602, Audit Report, January 2004.

U.S. Department of Energy, Office of Inspector General, Office of Inspections, *Summary Report on Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process*, DOE-IG-0482, September 2000.

U.S. Government Accountability Office, *Nuclear Security—DOE Faces Security Challenges in the Post September 11, 2001 Environment*, GAO-03-896, Re-port to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, June 2003.

U.S. Government Accountability Office, *Nuclear Security—Improving Correction of Deficiencies at DOE's Weapons Facilities*, GAO RCED 93-10, Report to the Chairman, Subcommittee on Environment, Energy, and Natural Re-sources, Committee on Oversight and Investigations, House of Representatives, November 1992.

U.S. Government Accountability Office, *Nuclear Security—Lessons to Be Learned From Implementing NNSA's Security Enhancements*, GAO-02-358, Report to the Chairman, Committee on Armed Services, Special Oversight Panel on DOE Reorganization, House of Representatives, March 2002.

U.S. Government Accountability Office, *Nuclear Security—NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives May 2003.

U.S. Government Accountability Office, *Safeguards and Security Planning at DOE Facilities Incomplete*, GAO RCED-93-14, Report to the Chairman, Sub-committee on Oversight and Investigations, Nuclear Security, December 1992.

U.S. Government Accountability Office, *Safeguards and Security Weaknesses at DOE Weapons Facilities*, GAO RCED-92-39, Report to the Chairman, Sub-committee on Oversight and Investigations, December 1991.

SECTION 8. PROTECTIVE FORCE

Booz Allen Hamilton, [site name] *National Laboratory Safeguards and Security Department Review*, November 2003.

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *The Department's Basic Protective Force Training Program*, DOE-IG-0641, Audit Report, March 2004.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Protective Force Performance Test Improprieties*, DOE-IG-0602, Audit Report, January 2004.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Management of the Departments Protective Forces*, DOE-IG-062, Au-dit Report, March 2004.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Security Overtime at the* [site name] *Operations Office*, ER-B-00-02, Audit Report, June 2000.

U.S. Government Accountability Office, *Key Factors Underlying Security Problems at DOE Facilities*, GAO RCED-99-159, Report to the Chairman, Sub-committee on Oversight and Investigations, Department of Energy, April 1999.

U.S. Government Accountability Office, *Nuclear Security—DOE Actions to Improve the Personnel Clearance Program*, GAO RCED 89-34, Report to the Chairman, Subcommittee on Environment, Energy, and Natural Resources, Committee on Government Operations, House of Representatives, December 1987.

U.S. Government Accountability Office, *Nuclear Security—DOE Needs a More Accurate and Efficient Security Clearance Program*, GAO RCED 88-28, Re-port to the Chairman, Subcommittee on Environment, Energy, and Natural Resources, Committee on Govern Operations, House of Representatives, December 1987.

U.S. Government Accountability Office, *Nuclear Security—NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives May 2003.

U.S. Government Accountability Office, *Personnel Security—Efforts by DOD and DOE to Eliminate Duplicative Background Investigations*, GAO RCED 92-93, Report to the Chairman, Committee on Armed Services, House of Representatives, 1993.

U.S. Government Accountability Office, *Safeguards and Security Weaknesses at DOE Weapons Facilities*, GAO RCED-92-39, Report to the Chairman, Subcommittee on Oversight and Investigations, December 1991.

United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System* (U), Final Report, April 2002 (Top Secret).

SECTION 9. SECURITY INCIDENTS AND INQUIRIES

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

A Security Architecture for NNSA—A Special Security Study (Hagengruber study), March 2002.

U.S. Department of Energy, memorandum from Deputy Secretary of Energy for All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

U.S. Department of Energy, Office of Inspector General, Office of Inspections, *Summary Report on Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self Assessments at [site] National Laboratory*, DOE/IG-0471, Audit Report, May 2000.

U.S. Government Accountability Office, *Key Factors Underlying Security Problems at DOE Facilities*, GAO RCED-99-159, Report to the Chairman, Sub-committee on Oversight and Investigations, Department of Energy, April 1999.

SECTION 10. DESIGN BASIS THREAT IMPLEMENTATION

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

A Security Architecture for NNSA—A Special Security Study (Hagengruber study), March 2002.

U.S. Government Accountability Office, *Nuclear Security—DOE Needs to Re-solve Significant Issues Before It Fully Meets the New Design Basis Threat*, GAO-04-623, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, April 2004.

U.S. Government Accountability Office, *Nuclear Security—DOE Needs to Re-solve Significant Issues Before It Fully Meets the New Design Basis Threat*, GAO-04-701T, Testimony to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, April 2004.

SECTION 11. SECURITY RESEARCH AND DEVELOPMENT PROGRAMS

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

A Security Architecture for NNSA—A Special Security Study (Hagengruber study), March 2002.

U.S. Department of Energy, memorandum from Deputy Secretary of Energy for All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

SECTION 12. NUCLEAR MATERIALS AND WASTE STORAGE

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

A Security Architecture for NNSA—A Special Security Study (Hagengruber study), March 2002.

U.S. Department of Energy, memorandum from Deputy Secretary of Energy for All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Design of the Uranium Storage Facility at the* [site name] *National Security Complex*, IG-0643, Audit Report, March 2004.

United States Nuclear Command and Control System Federal Advisory Commit-tee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System* (U), Final Report, April 2002 (Top Secret).

SECTION 13. RESOURCES AND REQUIREMENTS

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

SECTION 14. SECURITY CONTRACTING

U.S. Department of Energy, memorandum from Deputy Secretary of Energy for All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.