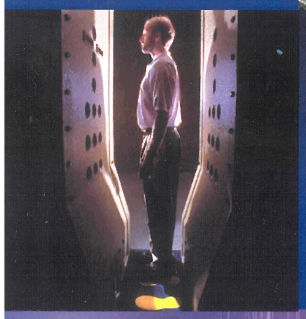

LMI®

# Strengthening NNSA Security Expertise

## An Independent Analysis

Contract Number:
DE-AD26-02NT41465


# Strengthening NNSA Security Expertise

## An Independent Analysis

March 2004

Contract Number:
DE-AD26-02NT41465

Henry G. Chiles Jr.
Charles B. Curtis
John Foster Jr.
David R. Graham
Richard L. Haver
Frank K. Martin
Michael S. Nicholson
Michael O. Wheeler
Edward H. Wright

# Strengthening NNSA Security Expertise: An Independent Analysis

MARCH 2004

The National Nuclear Security Administration security expertise study team was formed at the direction of the NNSA Administrator. He stated, "We need to take a fresh look at safeguards and security operations in NNSA in light of the post-9/11 threat environment, and we need to find a way to deal with a shortage of qualified, experienced security managers in NNSA." The study team was directed to develop recommendations for recruiting and retaining sufficient security experts to effectively oversee safeguards and security (S&S) in the NNSA complex now and in the long term. Although security at NNSA facilities includes a mix of federal and contractor security workforces, our primary focus was on the federal workforce. We coordinated our efforts with a team chaired by Admiral Richard Mies, USN (Retired), who was tasked with recommending improvements in physical security and material control and accountability in the NNSA complex.

We have formulated eight recommendations, which we believe will help ensure that competent, well-qualified personnel are available to oversee security of the nuclear weapons complex in future years.

1. *Develop and execute a comprehensive human capital management program.*

   NNSA not only should regard security personnel as a collective community, but should manage it as such, consistent with the intent to invest managers in the field with the authority and responsibility for coordinating federal interaction with site contractors. This will require the development of a human resource plan and corresponding programs to ensure timely hiring and an experience distribution that avoids the current seniority dilemma by permitting an orderly progression from junior responsibilities to supervisory roles. The plan must address weaknesses due to "one-deep staff" capabilities and provide time for training, professional development, rotations, and retirements.

2. *Improve the training, qualifications, and stature of the NNSA security workforce.*

   Federal security professional employees require specific training appropriate for their technical expertise, and their oversight roles and responsibilities in contract administration. NNSA should require participation in challenging, widely respected, and tailored professional development programs with demanding certifications designed to improve the proficiency of federal security professionals.

3. *Reengage in national markets to hire security professionals.*

   NNSA must institute an aggressive hiring plan for security professionals. The schedule for hiring should address near-term needs and provide for entry of new personnel on board well in advance of loss of incumbents. Recruitment of the next generation of security specialists should include substantial numbers of technically competent personnel to deal with increasingly technical security issues.

4. *Institute a long-term practice of security staff rotation.*

   NNSA should provide its engineering and technical staff, and selected managers, appropriate developmental S&S positions. This would include rotational assignments and opportunities within and across NNSA field sites and NNSA and DOE headquarters and, for some employees, temporary assignments with NNSA contractors and security positions in other government agencies.

5. *Identify options for accelerating the security clearance process.*

   NNSA should immediately review the process and develop an action plan to significantly reduce unnecessary delays or constraints. It should institute a processing system for clearance management that will permit improved tracking of individual cases to show status and dispel misunderstandings. It should periodically publish statistics to facilitate administration of the clearance process.

6. *Improve security information flow.*

   NNSA should institute a security information system that allows for frequent and timely written and interactive communication of both classified and unclassified information, among NNSA headquarters and the sites. It should determine the best methods for dissemination of lessons-learned and adopt practices to strengthen response and execution.

7. *Revise the NNSA Safeguards and Security Strategic Plan.*

   NNSA should revise its *Safeguards and Security Strategic Plan* to identify priorities in the near, mid, and long term. Particular attention should be given to the implementation of a comprehensive S&S professional development and proficiency enhancement program with specific timelines. Given the changing character of the threat or threats, the strategic planning process must itself be dynamic. It should incorporate a proactive risk management approach that provides for periodic reviews that pay particular attention to the mid- and long-term components and to the contribution of emerging technologies.

8. *Provide specific budget support and track recommendation progress.*

   NNSA should create a specific budget in its annual planning, programming, and budget and evaluation process to support the implementation, performance tracking, and progress of the aforementioned recommendations. It should provide specific additional budgetary support for the human capital management plan and the corresponding programs outlined in these recommendations.

# Contents

# Acknowledgments

The LMI project team—Linda T. Gilday, Shea W. Bader, Tanya D. Corrie, Dr. Robert L. Crosslin, Anna M. Wallace, and Gerald W. Westerbeck—thank the authors of this report, the NNSA security expertise study team, for their perspicacity, dedication, and hard work. The study team members are as follows:

- Admiral Henry G. Chiles, Jr. (USN Ret.), Study Team Director
- Mr. Charles B. Curtis, Nuclear Threat Initiative
- Dr. John Foster, Jr., Technology Strategies & Alliances
- Dr. David R. Graham, Institute for Defense Analyses
- Mr. Richard L. Haver, Northrop Grumman Corporate
- Brigadier General Frank K. Martin (USAF Ret.), Wackenhut Services, Inc.
- Mr. Michael S. Nicholson
- Dr. Michael O. Wheeler, Science Applications International Corporation
- Mr. Edward H. Wright, Systems Planning and Analysis, Inc.

The study team, in turn, is grateful for the active support of Mr. Jim Spracklen and his colleagues. At the kickoff meeting, they briefed the team on their census of the NNSA security workforce and their analyses of its functions and responsibilities. Subsequently, they provided their databases and graciously responded to numerous questions.

The study team also appreciates the contributions of Mr. Greg Rudy of Haselwood Enterprises, Inc., during the development of this report.

Finally, the study team also wishes to commend Mrs. Linda Gilday for her astute professionalism and strong support, enabling timely completion of this project.

# Chapter 1
# Introduction

## 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 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 semi-autonomous 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. 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 approximately 150 federal security professionals in NNSA.[1] 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.[2] 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.

Against this background, NNSA Administrator Linton Brooks announced in July 2003 that he was establishing two review groups to assess long-range issues affecting security management and protection, one to recommend improvements in physical security and materials control and accountability (MC&A) programs at the NNSA sites, another to develop recommendations for recruiting and retaining sufficient security experts to effectively oversee S&S in the NNSA complex over the long term.[3]

This situation, then, led to the creation of the NNSA security expertise study team, and this is our report. (Appendix A discusses the terms of reference for this team.)

# APPROACH

For the past 7 months, we studied the factors that shape and influence the workplace for the nuclear security program. Our members reviewed documents relating to the nuclear security program and received briefings on topics germane to this study from responsible officials in DOE and NNSA, the national laboratories and other nuclear facilities in the NNSA complex, the contractors managing those facilities and activities, and security professionals in the federal and contractor workforces. We attempted to understand the subtle distinction between overseeing NNSA contracts as opposed to managing contractors and reviewed DOE's overall organizational and management practices as they relate to NNSA nuclear security.

We also evaluated the operations of other high-priority national security programs, reviewed federal and private security training programs, and examined the expertise and skills (especially technical skills) needed to administer a world-class security program across the primary categories of S&S responsibilities: physical

[1] 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., chairs the current study on nuclear security personnel expertise, recruitment, training, and retention. Several others associated with that earlier study are involved in the new security study.

[2] 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. A member of the Hamre commission is involved in this security study.

[3] NNSA Press Release, "NNSA Announces Security Initiatives for Weapons Laboratories," July 8, 2003.

security, information security, cyber security, MC&A, personnel security, classification, and technical security. Because this study is focused on the long term, we also held open the possibility that new primary categories of responsibility may emerge and mature for the next generation of security professionals, as cyber security has for this generation. We surveyed over 150 men and women in the NNSA federal security workforce. The survey solicited their views, attitudes, concerns, and recommendations regarding their jobs and organizations and sought their current levels of satisfaction. We also held over 15 focus group discussions with a large number and variety of nuclear security personnel at seven locations. We held teleconferences with the remaining three sites: Kansas City Plant, Nevada Test Site, and Savannah River Site. In the survey, focus groups, and individual discussions we promised non-attribution to encourage candid and frank exchanges. (Appendix B describes our information-gathering activities; Appendix C describes our survey results.)

Chapter 2 contains our findings, and Chapter 3 contains our recommendations. At the end of each section in these two chapters, we cross-reference the findings and recommendations by number.

# Chapter 2
# Findings

In establishing this study, the NNSA Administrator has again recognized the importance of the nuclear security mission and is seeking our candid recommendations on how to improve NNSA's security posture. Our study has identified personnel planning, management, and resource deficiencies that could significantly impact NNSA's ongoing capacity to recruit, train, and retain sufficient security expertise to effectively oversee the S&S of its weapons materials, information, and infrastructure.

We also find that the federal security workforce is dedicated to the task at hand and has a genuine concern for security at all levels. Our recommendations are structured to augment the efforts NNSA has already made to improve the near- and long-term effectiveness of its S&S oversight.

NNSA faces a series of challenges in recruiting, training, and retaining enough skilled federal staff members to fill current and projected future security positions. The primary challenges include

- the number and skills mix of the security staff,
- the near-term retirement eligibility of a significant percentage of the workforce,
- professional development and training programs, and
- resources.

NNSA recognizes these challenges but has not yet developed a comprehensive plan for meeting them.

## 1. HUMAN CAPITAL MANAGEMENT

Federal security personnel at sites, the Service Center, and headquarters are managed by plans specific to each location. We find no integrated master plan or management process that treats security human capital as a community or draws these specific plans together.

The *Functions, Responsibilities, and Authorities Manual* (FRAM) includes seven skill areas that are specifically tracked as qualifications for NNSA security personnel.[1] Expertise in threat and vulnerability assessments is not included.

The individual managed staffing plans do not appear to provide adequate manpower ceilings for professional development and training or transfer of expertise associated with personnel rotation or retirement.

NNSA headquarters personnel identified the need for resources to support a professional development program, but such resources have not been consistently provided.

(See recommendations 1, 2, and 8.)

# 2. DEMOGRAPHICS AND NEAR-TERM STATUS

To provide a basis for our assessment of recruitment, retention, and training requirements, we documented the demographics of the NNSA federal workforce as of January 2004 and examined likely trends.[2] (Appendix D details this work.)

NNSA has authorized 149 billets for the NNSA federal security workforce based on an inventory of current responsibilities and workload performed in 2002. The NNSA federal workforce now numbers 145, four below the authorization.

NNSA's ongoing reorganization of the federal workforce entails the transfer of 15 billets from the former Nevada and Oakland Operations Offices to the Service Center during 2004. The people currently filling these billets reside in Nevada and California, and the majority, perhaps as many as 10, are expected to leave NNSA service rather than relocate. Consequently, without hiring in the coming year, the federal staff could fall 14 people—about 10 percent—short of the authorized ceiling.

(See recommendations 1, 3, and 8.)

# 3. REQUIRED SKILLS MIX

Managing the skills mix of the NNSA federal workforce entails identifying the areas of expertise needed in the workforce, setting the required number of personnel in each area, and maintaining the appropriate balance of seniority, experience, and training in each area.

---

[1] The skill areas in the FRAM are Physical Security, Information Security, Cyber Security, MC&A, Personnel Security, Classification, and Technical Security.

[2] We used data from a comprehensive census of the NNSA security workforce—known as the "Spracklen Survey"—performed in summer 2002 to provide a basis for reorganizing NNSA. We asked each site within NNSA to update the data in this census in January 2004.

Security supervisors across the complex said that NNSA needs to recruit more technically competent personnel to accomplish the security mission. From this supervisor input and other evidence, we find that NNSA's federal staff needs a broad range of technical, procedural, and managerial expertise to effectively carry out its oversight roles. The respondents to our survey support this finding; at least half rated the following six areas of knowledge "highly important":

- Knowledge of security threats
- NNSA's security strategy
- Understanding of the facility and ongoing programs
- Vulnerability assessment methods
- Technical background in the work area
- Resource and program management skills.

Key federal personnel must adequately understand security threats and have sufficient technical knowledge and familiarity with site operations, to perform oversight functions—assessing site safeguards and security plans (SSSPs), surveying site operations, and reviewing site self-assessments—and to give the Site Manager and NNSA leadership informed judgments on risks and vulnerabilities.

Regarding future skill requirements, four of the expertise areas (technical security, cyber security, MC&A, and classification) have a very high level (about 90 percent) of technical content. Presently, of the 37 people filling these positions, 29 of hold college degrees.[3]

In addition, over half the physical security specialist positions require extensive technical knowledge in areas such as civil engineering, blast assessment, and threat and vulnerability assessment. In most cases, the incumbent needs a technical degree, other training, or substantive experience commensurate with a technical degree. Currently, 9 of the 16 physical security specialists have degrees.

NNSA has no overall targets for complex-wide staffing in these critical skill areas (physical security, technical security, cyber security, MC&A, and classification). Under current management practices, the Site Managers determine the appropriate mix of skills within their assigned personnel ceilings, so security headquarters managers do not regularly track or assess the mix of skills in the workforce. This ceiling-driven approach can result in mismatches between the number of personnel onboard and the workload.

[3] People listed in the management and "general engineering, security specialist, and multiple areas" categories provide additional expertise, but they are not dedicated to these highly technical areas and no doubt have other duties.

NNSA has tried to adjust its workload requirements by reengineering tasks, and by obtaining expert contractor support to augment federal technical staffs, but the current technical workforce is some 20 percent below desired levels.[4] We conclude that the complex is very thin in all five areas, especially where small numbers of experts reside (technical security and MC&A) and where significant numbers are eligible to retire in the next 5 years (classification).

In the following sections, we discuss NNSA's hiring needs in the coming years. This hiring opportunity gives NNSA the means to implement a systematic program for hiring and training personnel to meet its future requirements in these highly technical areas. A complex-wide focus on hiring and training the workforce in these technical areas, supplemented by staff rotational assignments, would provide NNSA the ability to manage the one-deep challenge facing certain sites and an opportunity to develop effective succession strategies.

(See recommendations 1 through 4 and 8.)

# 4. RETIREMENT TRENDS

Data show that 106 of the federal staff of 145 will be eligible to retire in the next 5 years (2009 or earlier). The number of actual retirees will depend, of course, on many factors; the most significant is that many workers plan to work beyond their retirement eligibility age. Our assessment (Appendix D) indicates that slightly over one-quarter of the workforce can be expected to retire by 2009.[5] Replacing these retirees will require hiring 8 to 10 security personnel per year. These projections could change for better or worse over time, depending on workplace and general economic factors.

Although the *NNSA Safeguards and Security Strategic Plan* recognizes the retirement challenge,[6] we find no indication of a corporate master plan for hiring several years in advance of retirement of senior personnel.

(See recommendations 1, 3, and 8.)

# 5. RECRUITMENT

NNSA sites have not recruited or hired security personnel from the national labor pool in the last 3 years due to hiring freezes and budget limitations. The most

[4] Safeguards and Security Workforce Analysis and Report, January 2003.

[5] From the Spracklen Survey, 63 of those eligible to retire in 2009 or earlier said they would not retire when they become eligible. So, if 10 leave this year as the result of the transfer of billets, and all 63 of the remaining 96 stay, then 33 individuals can still be expected to retire after the coming year and before 2009. So, the total projected departures are 43 (10+33), which is 28 percent of the current workforce.

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

recent hiring freeze, which is associated with the ongoing NNSA restructuring, has been in effect since October 1, 2001, was modified several times, and was partially lifted in December 2003. During this freeze, Site Offices could only recruit from within NNSA, competing against each other from a fixed pool of security expertise.

In addition, each Site Office has unique recruitment challenges. For example, the cost of living is very high at Los Alamos and Livermore. For other sites, remoteness and the complexity of security can be issues. On the other hand, sites like Pantex have succeeded in maintaining the needed federal staff.

Intern programs, which bring people onboard directly out of college or later in their career, are a time-tested means for transitioning people into an area with requisite skills. NNSA has an intern program, but it is not centrally managed. This year, individual Site Offices took the initiative to hire the first three security interns, one at Los Alamos and two at Sandia.

In the post-9/11 world, demand and competition for security professionals in government service and the private sector have greatly increased. Accordingly, NNSA faces competition as private firms and other federal agencies seek to hire experienced and entry-level security staff. NNSA contractors and other government organizations with which we met have been able to compete in this marketplace and have greatly expanded their workforces since the terrorist attacks, giving them extensive recent experience with and knowledge of the national marketplace for security professionals.

In our survey, 33 percent of respondents have moved for job-related reasons in the last 10 years, and 61 percent said that they are unwilling or slightly unwilling to relocate to another site. As stated previously, the majority of those asked to relocate as a result of NNSA's ongoing reorganization of the federal workforce would rather leave NNSA service than relocate.

Appendix E compares the pay permitted under DOE's federal salary-grade structure with the competitive pay found in national labor markets for entry-level personnel, senior technical personnel, and executives. These comparisons show the following:

- The prevailing standard government policy of offering GS-5 or GS-7 grades for entry-level positions does not appear sufficiently competitive to attract high quality, entry-level technical talent into the NNSA S&S program. To compete in national job markets, NNSA likely needs to use Excepted Service hiring authority or offer GS-9 positions to recent engineering graduates.

- For the most part, government pay at GS-13, GS-14, and Excepted Service grade 4 is competitive with the prevailing pay for technical security specialists and technical security managers. Likewise, government pay at the GS-15 level, Senior, Executive Service (level I), and Excepted Service grade 5 is competitive with the prevailing pay for all but the most senior security executives.

Building and sustaining a cadre of highly qualified professionals will require a complex-wide management approach that targets the use of Excepted Service authority and allocates senior billets across the complex.

(See recommendations 1, 3, 4, and 8.)

# 6. PROFESSIONAL TRAINING, QUALIFICATIONS, AND STATURE

Our research indicates that people at all levels in the NNSA security community recognize the need for increased attention to professional development and training (see Appendix F.) This shortfall is also recognized in NNSA and the contractor community. In many instances, the workforce is foregoing needed training due to the press of urgent business or the shortage of resources. Over 50 percent of NNSA personnel survey respondents disagree or strongly disagree that the existing training and education of the federal workforce is adequate. Twenty-nine percent "strongly disagree." This situation will not necessarily get better anytime soon. Current managed staffing plans do not have the built-in flexibility to allow for professional development and training.

We also find that the federal security workforce is interested in increasing its professional standing. Federal field employees work alongside and oversee highly qualified contractor employees. To be effective, these federal employees must consistently earn respect by mastering and demonstrating an understanding of the technical and oversight aspects of their positions. Expertise in areas such as program oversight, contract administration, security policies, vulnerability assessments, root cause analysis, and performance testing are necessary for success.

The federal security staffs are interested in formal qualification standards or professional certification to demonstrate sufficient skills and experience. NNSA security managers recognize the lack of an effective professional development program: fully 60 percent of those surveyed have received no formal career counseling.

Technical certification is considered "highly important" by one-third of the workforce and all of those with cyber expertise. Yet less than one-quarter report extensive use or completion of Nonproliferation and National Security Institute (NNSI)

certification, and only 15 percent of those specializing in cyber security report extensive use or completion of The SANS Institute[7] certifications.

At the beginning of its work, the team was briefed on NNSI capabilities and the plans for its expansion into a "security college." Its training venues ranged from traditional classroom to distance- and e-learning formats, but budgetary reductions appear to have limited the distance- and e-learning capability. Nonetheless, the facility infrastructure remains, and NNSI's Professional Enhancement Program is available to the NNSA security workforce. It clearly has the capability to provide training in support of a security professional development program.

NNSA is reorienting its operational practices to return to a model, which, in theory, clearly delineates between the *oversight* responsibilities of the federal staff and the *management* responsibilities of the contractors that hold contracts to manage NNSA facilities. (See the following section.) This is a dramatic change in culture, especially at the newly restructured Site Offices. We find no formal training program that provides NNSA federal officials (security or otherwise) with the subtle but important skills that distinguish oversight from management. We also find no evidence of intent to systematically develop and catalog case studies of effective oversight within the NNSA security complex to facilitate training.

(See recommendations 1, 2, 4, 7, and 8.)

# 7. FEDERAL OVERSIGHT OF CONTRACTOR PERFORMANCE

To address the dynamic environment of security in the post cold war and September 11 era and to ensure consistently improved and responsive security within available funding, NNSA is making a strategic management shift in the execution of security oversight at its facilities.[8] The federal security staff role is more clearly defined as establishing the "what" while enabling the contractor to determine the "how." Contractors are then held accountable for performance through assessments and oversight by federal security staff. This transition necessitates a greater focus on integrated performance results. Notwithstanding the major shift in oversight and management approach, we found no integrated,

[7] Reference http://www.sans.org.

[8] Since its beginning, America's nuclear weapons research, development, and production complex has consisted of government-owned, contractor-operated (GOCO) facilities. Previous studies have recognized and documented that the management culture at DOE evolved such that the federal staff activities often resulted in micromanagement rather than oversight. These studies strongly recommended change. The *Report to Congress on the Organization and Operations of the National Nuclear Security Administration* (February 2002) registered NNSA intent to eliminate this damaging trend and to ensure and enhance the oversight focus of NNSA federal officials. This shift, underway since 2002, marks an important change in culture for the NNSA federal officials in the newly restructured Site Offices, including NNSA security specialists.

sustained training program to prepare the federal security personnel for their new responsibilities[9].

NNSA uses an iterative site analysis (ISA) process as a security performance assessment and planning tool across its facilities. It provides the federal and contractor staffs the additional benefits of exposure to independent security professional perspectives and experience. It also provides an opportunity for the federal security staff to strengthen professional collaboration with the site contractor security staff. This approach reinforces the focus on assessment of integrated security program performance as opposed to a checklist approach to compliance with DOE orders.

Compliance and performance testing both have a place in the security world. Compliance testing by itself, however, is not sufficient, and the distinction between these approaches is thus important. Compliance might be satisfied, for example, if protective force training includes individual firearms proficiency testing and, separately, a test to see whether the security officers can locate and quickly don their chemical and biological agent protective ensemble. Performance testing, in contrast, seeks to understand whether the protective force can effectively fight using their full equipment—as a unit.

Compliance testing is easy to design and score, yet reliance on compliance testing only can lead to complacency and a focus on yesterday's threat. Performance testing focuses on the integrated story. It is harder to design, but can provide additional, important information to assess system effectiveness.

Evidence indicated that the federal security workforce is mainly focused on compliance testing rather than performance testing.

We find that sites and contractors are concerned about the frequency of inspections, assessments, and audits. Contractors are required to do extensive self-assessments—the results of which are part of the federal security personnel oversight—for their annual contract evaluations. DOE (Office of Security and Safety Performance Assurance and Inspector General) and General Accounting Office (GAO) assessors also visit sites. Data from the field sites indicate that 10 to 20 percent of their time is devoted to supporting these external assessments. The extent of this oversight involvement is not unreasonable, especially if coordination of schedules can be improved.

[9] *Managing* security and *overseeing* the management of security subtly differ. The Site Office Manager determines whether the contractor's security program is operating within acceptable levels of risk. If the risk is deemed excessive, the Site Office Manager has the power to direct activities (such as the suspension of certain security practices) until remedial actions have been taken to eliminate the perceived excessive risk. This judgment of "excessive risk"—how quickly it is made, what it entails—in fact gives the Site Office Manager the ability to substitute his or her judgment for what otherwise would be the security contractor's decision on *how* to do security. Thus, in practice, the distinction between management and oversight of security depends on the expertise and administrative skills of the federal NNSA officials.

(See recommendations 2 and 8.)

# 8. CLEARANCE BACKLOG AND DELAYS

The personnel security specialist constitutes the single largest category in the NNSA federal security workforce. Some 43 of the 145 federal employees in NNSA have a personnel security specialty. The personnel security area also has a long-standing, well recognized impact on nuclear security: the protracted time it takes to grant a Q clearance hinders recruitment and productivity. (See Appendix G for additional information.)

Advances in information technology (IT) should help resolve the problem, and extensive effort outside DOE is incorporating new technologies in clearance and reliability programs. Examples include electronic processing of clearance applications by the Office of Personnel Management (OPM), the Automatic Continuing Evaluation Study (ACES) tool within the Department of Defense (DoD), and advanced computing capability modeled after OPM and the Defense Security Service. The Service Center is investigating more efficient processes based on IT, but NNSA has no long-term plan for using advanced computing capability tailored to this area.

Virtually every location we visited is concerned about contractor recruiting problems caused by the backlog of personnel clearance cases and extended delays in obtaining access authorizations (clearances) or approvals for personnel reliability programs. As the employment freeze is lifted and NNSA offices begin to hire, they will likewise face delays in clearance processing.

Personnel clearance investigations influence staff management because the tendency is to try to hire a person with an existing clearance. Costs also affect the hiring process: the estimated cost of each individual awaiting a clearance is $50,000 per employee.[10]

NNSA processes about 12,000 cases annually through OPM: initial cases number about 3,000 and reinvestigations, 9,000. As of January 2004, a backlog of 10,800 cases was pending, up from about 2,500 on September 11, 2001. Virtually the entire backlog is at the investigative agencies, not the Service Center. Data at the Site Offices and the Service Center make it difficult to correlate processing delays with responsible agents. The current statistics do not permit accurate monthly measurement of the backlog of clearances being processed.

The Accelerated Access Authorization Program (AAAP) is used, yet about 70 percent of the AAAP cases are rejected. Service Center data show that AAAP clearances take an average of 106 days, whereas some sites report it takes up to a year. One-quarter of the Service Center's average AAAP processing time could

[10] Service Center presentation "Rapid Interim Clearance Program" February 04, 2004, page 22.

be eliminated by moving the risk acceptance official from DOE headquarters to the Service Center.

On October 1, 2003, DoD moved approximately 425,000 civilian personnel security clearance cases and over 300 trained investigators to OPM, which already has difficulty processing its current workload.[11] This transfer will exacerbate the problem of slow clearances for NNSA.

The current clearance process is extremely ineffective in obtaining timely clearances. While the statutory and regulatory responsibility for certain requirements rests outside NNSA, the seriousness of the situation dictates that NNSA take action, in coordination with DOE, to identify and implement all viable approaches to expedite clearances throughout its facilities.

(See recommendations 5 and 8.)

# 9. PERFORMANCE, INCIDENTS, AND LESSONS-LEARNED

Incident reviews, root cause analyses, corrective action plans, and corrective action tracking are common elements of each site's security program. 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 workforce. An effective synthesis of lessons-learned from internal security reviews 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

[11] Information Security Oversight Office, *The 2002 National Industrial Security Program Report, Industry's Perspective: Making Progress, But Falling Short of Potential*, National Archives and Records Administration, p. 10.

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.

(See recommendations 6 and 8.)

# 10. STRATEGIC PLANNING

The safeguarding and security of NNSA's assets (weapons, materials, information, infrastructure and people) are an integral part of mission accomplishment. This dynamic, resource-intensive process presents management with challenges for which strategic planning is essential.

The *NNSA Safeguards and Security Strategic Plan* does not prioritize or clearly differentiate time horizons for goal accomplishment. It also does not perform a truly strategic function in priority setting or budget planning within NNSA. Planning at the Service Center, Site Office, or contractor level shows little evidence of incorporating its goals or strategies.

Areas of the plan imply that the S&S responsibility is a "subordinate" support role or, alternatively, a top-down regulatory function imposed on NNSA's primary mission. Either concept implies a function separate from NNSA's core mission accomplishment; S&S management should be seen as an essential, integral part of the mission.

(See recommendations 7 and 8.)

# 11. RESOURCES FOR SECURITY

During the course of our visits and discussions, we were repeatedly informed that workload and the sparse manning of the federal security field activities necessitated the full attention of personnel assigned, leaving little opportunity for education, training, and mentoring of personnel. Our survey information reinforces this finding.

We also find that budget planning does not allow for smooth, face-to-face transfers of authority and expertise during personnel rotations or retirements. We were advised that there was no budget for overlap of personnel in these instances.

We did not find a lack of financial support for training and education, but, at times, the financial resources for training were diverted for other purposes. As discussed in earlier sections, adjusting personnel ceilings upward to provide flexibility for training and professional development programs obviously has resource implications.

Historically, in DOE the S&S function was funded indirectly. For the past several years, S&S has been funded directly, in that NNSA headquarters transferred funds to sites for coverage of specific security expenditures, which the federal managers in the field then allocated. In FY06, this form of underwriting reportedly may change to some degree of indirect funding. (See Appendix H.)

Opinions differ as to the relative merits of direct and indirect funding. Under either approach, human resources management can be effective as long as budgets include sufficient funding and comprehensive information.

(See recommendations 3 and 8.)

# 12. SUPPORTING INFORMATION

Appendix I lists the documents the team reviewed and generated in the course of this study.

Appendix J lists the abbreviations used in this report.

# Chapter 3
# Recommendations

## 1. *Develop and execute a comprehensive human capital management program.*

NNSA not only should regard security personnel as a collective community, but should manage it as such, consistent with the intent to invest managers in the field with the authority and responsibility for coordinating federal interaction with site contractors. This will require the development of a human resource plan and corresponding programs to ensure timely hiring and an experience distribution that avoids the current seniority dilemma by permitting an orderly progression from junior responsibilities to supervisory roles. Such an approach will require an integrated focus on interns or new hires just entering the workforce, experienced security professionals with needed skills, and personnel from other fields within the DOE/DoD complex.

NNSA should immediately review and adjust the current FRAM to ensure that it includes all critical skills, such as threat and vulnerability assessment.

Managed staffing plans should be adjusted in accordance with the human resource plan, specifically addressing weaknesses due to "one-deep staff" capabilities, time for training and professional development, and productivity losses due to rotation, temporary assignments, and retirements.

A formal, centrally managed intern program should be instituted to attract select personnel to NNSA Security.

(See findings 1 through 6 and 8.)

## 2. *Improve the training, qualifications, and stature of the NNSA security workforce.*

Federal security professional employees require specific training appropriate for their technical expertise and their oversight roles and responsibilities in contract administration. NNSA should require participation in challenging, widely respected, and tailored professional development programs with demanding certifications designed to improve the proficiency of federal security professionals.

NNSA should develop and provide specific training to embed and sustain its policy of focusing on management of the contract, not the contractor, to strengthen the management authority and responsibility of its security contractors.

The training of the federal workforce should prepare them to oversee contractor performance as well as compliance testing. The threat will not remain stagnant, and an audit process focused mainly on compliance testing will not suffice to ensure the protection of NNSA's assets.

NNSA should study distance-learning approaches, which can reduce time away from sites and travel costs. In cooperation with the Office of Security and Safety Performance Assurance and NNSI, NNSA should explore creation of an e-Learning community of practice for security professionals, including knowledge management, sharing of best practices, just-in-time web-based instruction, and online performance support tools, much along the lines of the Defense Acquisition University and other DoD organizations. NNSA should align these materials with those of professional organizations, such as ASIS International[1], and academic institutions to increase the attractiveness and quality of the offerings.

(See findings 1, 3, 6, and 7.)

## *3. Reengage in national markets to hire security professionals.*

NNSA must reengage in national markets for security professionals with an aggressive hiring plan. The schedule for hiring should address near-term needs and provide for entry of new personnel onboard well in advance of the loss of incumbents.

Our sense is that adjusting the FRAM and managed staffing plans (discussed above) will increase ceiling levels by 10 to 15 percent. But, even if only the current staffing levels are maintained, NNSA will need to hire 8 to10 people per year for the next 5 years to replace expected retirees.

Recruitment of the next generation of security specialists should include substantial numbers of technically competent personnel to deal with cyber security and other increasingly technical security issues. To attract highly qualified technical personnel (entry level and higher), NNSA needs to maximize use of pay and appointment authorities. It must also increase the use of relocation bonuses, retention allowances, and other incentives for critical S&S positions.

(See findings 2 through 5 and 11.)

## *4. Institute a long-term practice of security staff rotation.*

As mentioned in its *Safeguards and Security Strategic Plan*, NNSA should institute a long-term practice of rotating NNSA engineering and technical staff and selected managers, through appropriate developmental S&S positions. This would include rotational assignments and opportunities within and across NNSA field sites and NNSA and DOE headquarters and, for some employees, temporary

[1] Reference http://www.asisonline.org

assignments with NNSA contractors and security positions in other government agencies. This practice will give these personnel a new perspective, expand the pool of those who may seek an S&S career, and provide those who rotate back into federal line engineering and technical functions with a better understanding of S&S considerations and the ability to factor them into their daily work.

(See findings 3, 5, and 6.)

## *5. Identify options for accelerating the security clearance process.*

The Chief of Defense Nuclear Security should be directed to immediately secure the cooperation of the Director, Safeguards and Security Performance Assurance, DOE, in reviewing the clearance process and submitting an action plan in 60 days to significantly reduce unnecessary delays or constraints in security clearance and reliability programs (including those in AAAP). The action plan should incorporate technologies and techniques from inside and outside DOE. The review should address needs and, if necessary, requisition advanced computing equipment for the Service Center to accelerate clearance and investigative processes.

NNSA should institute an ongoing processing system for clearance management that will permit improved tracking of individual cases to show status and dispel misunderstandings. To facilitate the administration of the system, NNSA should periodically publish statistics (such as the number of cases received, cleared, and in adjudication and the time frames associated with each step).

The team considers this issue serious enough that the review should include not only analysis of methods to improve processes and procedures set by DOE policy, but also statutory and regulatory requirements upon which that policy is based. To the extent those requirements, or the manner in which they have been addressed, have fostered a condition that results in an untimely clearance process, DOE should seek to amend them. In the process, DOE should consider innovative alternatives to the current system.

(See finding 8.)

## *6. Improve security information flow.*

NNSA should institute a security information system that allows for frequent, timely, written and interactive communication of both classified and unclassified information among NNSA headquarters and the sites.

It should seek information from outside the nuclear weapons community to determine the best methods for dissemination of lessons-learned and adopt practices to strengthen response and execution.

It should also use analysis of incidents as a basis for identifying leading indicators of security problems and areas needing increased attention.

(See finding 9.)

## 7. *Revise the NNSA Safeguards and Security Strategic Plan.*

NNSA should revise its *Safeguards and Security Strategic Plan* to identify priorities in the near, mid, and long term. In recasting this Plan, the authors should emphasize that the S&S function is an integral part of NNSA's mission accomplishment. Particular attention should be given to the implementation of a comprehensive S&S professional development and proficiency enhancement program.

Given the changing character of the threat or threats, the strategic planning process must itself be dynamic. It should incorporate a proactive risk management approach that provides for periodic reviews that pay particular attention to the mid- and long-term components and the contribution of emerging technologies.

The Administrator should sign the restated plan and promulgate it throughout NNSA. (This will give the plan authoritative status, increase the importance of the S&S function, and help ensure the complex takes up the plan's objectives, priorities, and strategies.)

The Service Center, Site Offices, and contractors should align their plans with the restated NNSA *Safeguards and Security Strategic Plan* and, as appropriate, incorporate its relevant priorities and strategies as well as appropriate elements of the DOE *Security Strategic Plan*.

(See findings 6 and 10.)

## 8. *Provide specific budget support for and track progress of the preceding recommendations.*

NNSA should create a specific budget in its annual planning, programming, budget, and evaluation process to support the implementation, performance tracking, and progress of the aforementioned recommendations. It should provide specific additional budgetary support for the human capital management plan and the corresponding programs outlined in these recommendations.

(This recommendation applies to all findings.)

# Appendix A
# NNSA Security Expertise Study Team
# Terms of Reference

## BACKGROUND

The NNSA Administrator has established two groups to assess long-range issues affecting security management and protection:

a. A team, chaired by Admiral Rich Mies, to recommend improvements in physical security and materials control and accountability at the weapons laboratories.

b. Separately, this team (the NNSA Security Expertise Study Team) to develop recommendations for recruiting and retaining sufficient security experts to effectively oversee safeguards and security in the NNSA complex in the long term. Primary focus is on the federal workforce. We are encouraged to coordinate our efforts with the Mies team.

These teams address two concerns, as expressed by Ambassador Brooks. "While we need to make use of past recommendations, I think we need to take a fresh look at safeguards and security operations in NNSA in light of the post-9/11 threat environment, and we need to find a way to deal with a shortage of qualified, experienced security managers in NNSA."

## SCOPE

A key theme for our team is the thorough assessment of the NNSA security skills required to provide security oversight for a safe and reliable nuclear weapons stockpile, well into the future, in an environment in which a robust stockpile stewardship and management program is being instituted with sufficient production capability for critical components (over time it is envisioned that all components could be considered critical).

The assessment of security personnel skills should include study of DOE and NNSA policies for personnel recruitment, hiring, and training; employee background, education, academic qualifications, and age distribution; retention; advancement; future recruitment plans, efforts, goals, and measures of success.

The team should visit a range of NNSA facilities (laboratories, test sites, production sites, field support activities, and headquarters). These visits should be conducted with the view to understand the activities in progress, core competencies,

facilities, missions, and personnel management practices being executed relative to the aspects of the preceding paragraph. In addition to discussion with senior personnel at these facilities, the team should ensure that adequate time is set aside for discussion with junior and middle grade personnel to assess their attitudes, understanding of the security mission at the facility, enthusiasm for their work, and sense of value associated with their function.

The team should consider examining the security personnel management plans of other organizations for comparison and to assess corporate ideas. Appropriate organizations may include DoD (with considerable responsibility for security as well as safety and reliability of the weapons systems), highly technical companies and corporations, and other laboratories managing classified programs. We should provide insights on what is needed to ensure that NNSA (and perhaps DOE) can compete with industry in attracting high quality security personnel.

LMI should provide a report of the findings and recommendations of the team to the Administrator, NNSA, in March 2004.

## GENERAL

Tasks of the LMI staff currently envisioned are listed in the enclosure.

Pay, allowances, travel, and other funding issues will be handled in accordance with LMI procedures.

Visits to NNSA facilities will be necessary. Ideally, all team members will participate. Schedule conflicts will likely preclude the full complement on all trips; accordingly, trips will be arranged to accommodate the schedules of at least three team members. If three team members cannot participate, the trip will be rescheduled.

Reports of prior studies, policies, other assessments, and planning documents will be forwarded to members of the team as they become available to facilitate early familiarization with the issues before the team.

During the course of this review, the team will not attribute the comments and responses obtained in any interviews or surveys of personnel within the nuclear weapons complex.

ENCLOSURE

STAFF TASKS FOR THE NNSA SECURITY EXPERTISE STUDY TEAM

1) Support site visits to NNSA weapons complex and other facilities:

- Work with the staff at the sites to secure required data for review before the site visit.
- Arrange for meeting rooms and develop an agenda with the chair, deputy chair, and site management.
- Collect data during site visits using recordings, etc., and provide documentation of meeting notes and summaries of data.
- Assemble data and ensure that data summaries are provided to team members in a timely manner.
- Conduct follow-up activities to site visits as directed by the deputy chair.

2) Support team members:

- Arrange for travel, reimbursement, and pay.
- Ensure that telephones, faxes, etc., are available for panel members during site visits.
- Provide additional support for team members as directed

3) Provide headquarters support for data analysis and briefings:

- On the basis of site visits or other input, conduct research into areas of interest to the team and prepare point papers.
- Arrange meetings with team members and review findings.
- Assemble, maintain, and archive a repository of reports, presentations, and other material used by the team members during its deliberations and in preparation of the report.
- Arrange data to easily identify issues and reflect trends for presentations to NNSA, and others if directed by NNSA.
- Assist team members in preparing an interim (if desired) and a final report to NNSA, including technical editing.
- Provide other support as directed after consultation with the team deputy chair.

# Appendix B
# Information-Gathering Activities

The study team used a variety of methods to gather information about the NNSA federal workforce and to develop a thorough understanding of DOE and NNSA policies and practices for recruitment, hiring, training, retention, and advancement (Table B-1). The team visited DOE facilities, held meetings, and participated in teleconferences. Documents collected from the sites, as well as others the team reviewed, are listed in Appendix J. The team also distributed a survey, provided in Appendix C, to the federal staff at each DOE facility to collect their perspectives on personnel practices. In addition, the team met with other organizations that perform security functions similar to those performed by NNSA.

*Table B-1. Information-Gathering Activities*

| Date | Activity | Principal contacts |
|---|---|---|
| October 19–22, 2003 | Site Visit to Los Alamos | |
| | Los Alamos Site Office | Ralph Erickson, Manager, LASO |
| | | Scott Gibbs, Interim Division Director<br>Safeguards & Security |
| | Los Alamos National Lab (LANL) | Pete Nanos |
| | | Mike Wilson, Acting General Manager<br>Protection Technologies |
| October 22, 2003 | Site Visit to NNSA Service Center | Jim Hirahara, Director<br>NNSA Service Center |
| | | Mike Spence, Supervisory General Engineer<br>Security Support |
| | | Rick Phillips, Director, Security Support |
| | | Wayne Rancher, Supervisory Security Specialist, Security Support |
| | | Larry Kirkman, Director<br>Office of Federal Services |
| October 22, 2003 | Site Visit to NNSI | Art Flynn, Supervisory Security Specialist<br>Office of Training & Education |
| | | Jack Killeen, SVP/Gen Manager<br>Wackenhut Services, Inc. |
| November 6, 2003 | Site Visit to Pantex | |
| | Pantex Site Office | Daniel Glenn, Director<br>Pantex Site Office |
| | | Gary Wisdom, Assistant Manager<br>Safeguards & Security |
| | Pantex Plant | Paul Sowa, Manager<br>BWXT |

*Table B-1. Information-Gathering Activities (Continued)*

| Date | Activity | Principal contacts |
|---|---|---|
| November 12–13, 2003 | Site Visit to Sandia | |
| | Sandia Site Office | Jo Loftis, Assistant Manager<br>Safeguards & Security |
| | Sandia National Laboratory | Dennis Miyoshi, Director<br>Safeguards & Security |
| | | Mary Lynn Garcia<br>Intrusion Detection Technology |
| November 13–14, 2003 | Site Visit to Livermore | |
| | Livermore Site Office | Camille Yuan-Soo Hoo, Director<br>Livermore Site Office |
| | | Michael Connolly, Assistant Manager<br>Safeguards & Security |
| | Lawrence Livermore National Lab (LLNL) | Dave Leary, Director<br>Safeguards & Security |
| | | Paul Sowa, BWXT Management |
| November 16–17, 2003 | Site Visit to Y-12 | |
| | Y-12 Site Office | Bill Brumley, Site Manager |
| | | Sharon Daly, Security Officer<br>Assistant Manager for Safeguards & Security |
| | | Dennis Ruddy, BWXT Management |
| | | John Burleson, Wackenhut |
| December 8, 2003 | Meeting with HQ | Toby Johnson, Acting Chief<br>Defense Nuclear Security |
| December 10, 2003 | NRC Benchmarking Visit | Dan Dorman, Deputy Director<br>Office of Nuclear Security & Incident Response |
| December 10, 2003 | Naval Reactors Benchmarking Visit | Stephen J. Trautman, Director<br>External Affairs, Naval Reactors |
| December 11, 2003 | Meeting | Dr. John Nuckolls, Director Emeritus of LLNL |
| December 12, 2003 | NSA Benchmarking Briefing | POC requested identity be withheld |
| January 13, 2004 | Teleconference with Kansas City Site Office | Steve Taylor, Acting Site Manager |
| | | Patrick Hoopes, Assistant Manager<br>Office of Safety & Security |
| | | Sherry Kinsey-Cannon, Administrative Officer<br>Office of Business Management |
| | | John Cowan, IT Specialist<br>Office of Safety & Security |
| | | John Vaughn, Security Manager<br>Honeywell |

*Table B-1. Information-Gathering Activities (Continued)*

| Date | Activity | Principal contacts |
|---|---|---|
| January 15, 2004 | Teleconference with Nevada Site Office | Jay Norman, Deputy Manager for Operations<br>Terry Wallace, Assistant Manager Safeguards & Security<br>Wayne Adams, Director Safeguards & Security<br>Mike Kiley, Security Program Manager<br>Cyle Iverson, Physical & Technical Security Team Leader<br>Ricky Honaker, Electronics Engineer, Security<br>Mike Ebert, SVP/General Manager Wackenhut Services, Inc.<br>Jeff Herhold, Assistant General Manager Technical Services, Wackenhut Services, Inc.<br>Dave Bradley, Deputy General Manager Wackenhut Services, Inc.<br>Steve Warner, Training Director Wackenhut Services, Inc.<br>Bob Gasperino, Security Director Wackenhut Services, Inc. |
| January 16, 2004 | Teleconference with Savannah River (SR) | Ed Wilmot, Director, SR Site Office<br>Ron Bartholomew, Director, Safeguards and Security<br>Tom Williams, Deputy Director, Safeguards & SecurityLarry Brede, SVP/General Manager Wackenhut Services<br>Chris Baker, Westinghouse Savannah River Co<br>Greg Myer, Westinghouse Savannah River Co |
| January 21, 2004 | Meeting | John Browne, former Director of LANL |
| January 21, 2004 | Meeting with HQ | Winnie Lehman, Security Specialist Office of Nuclear Safeguards & Security<br>Cathy Tullis, Information Security Specialist Office of Nuclear Safeguards & Security |
| January 23, 2004 | Meeting with DOE Office of Homeland Security Programs | James Spracklen, Security Officer |
| January 30, 2004 | Meeting with HQ/OA | Mike Kilpatrick, Director Office of Independent Oversight & Performance<br>Glenn Podonsky, Director Office of Safeguards & Security Performance |
| January 30, 2004 | Air Force Benchmarking Visit | Dan Bishop, Chief Information Security Division, Directorate of Security Forces |

*Table B-1. Information-Gathering Activities (Continued)*

| Date | Activity | Principal contacts |
|---|---|---|
| February 13, 2004 | Site Visit to NNSA Service Center | Patricia Armijo, Executive Officer<br>Office of Federal Services<br>Tracylynn Loughead, Public Affairs Specialist,<br>Office of the Director, NNSA Service Center |
| February 23, 2004 | Meeting | John C. Todd, former Chief Defense Nuclear Security, NNSA |
| February 26, 2004 | Meeting | Joseph S. Mahaley, former Director of DOE Office of Security |
| February 26, 2004 | Meeting | Dr. Siegfried S. Hecker, former Director of LANL |
| February 26, 2004 | Meeting | Bruce Darling, Acting University of California Vice President for Laboratory Management |

# Appendix C
# NNSA Federal Workforce Survey Responses

The NNSA Security Workforce Survey comprised 51 questions covering job satisfaction, views on the security enterprise and possible improvements, and workforce knowledge requirements, education, and training. This appendix discusses the survey responses in the following eight categories:

- Job satisfaction factors: importance and degree they are provided
- Key organizational success factors
- Threshold question: would you recommend NNSA federal employment, and why?
- Recommendations for NNSA improvement
- Future workforce capabilities and knowledge
- Education and training: availability, use, and importance
- Workforce mobility and willingness to move
- Sample population statistics.

(Attachment 1 to this appendix lists the survey questions.)

We sent the survey via a personal e-mail to S&S employees, inviting them to go to an LMI-hosted website. We received 103 responses or roughly 71 percent—a cross-section of NNSA Site Offices expertise and experience levels.

## JOB SATISFACTION FACTORS

### Summary

Seventy percent or more of the workforce rated 7 of the 17 job factors as "highly important." These key factors are benefits, employment security, interesting and challenging work, management support for the security mission, being treated with respect, compensation, and clear expectations for job performance:

- Benefits, interesting and challenging work, and compensation are relative strengths: they are important and considered to be relatively well provided.

- Employment security, being treated with respect, and clear expectations are important and also relatively well provided; however, this view is not uniform: 10 percent or more of the workforce say their provision is "inadequate."

- Management support for the mission is important; but not considered well provided. It has the largest gap between importance and provision, and the highest percentage of "inadequate" responses for provision (29 percent).

Twenty percent or more of the respondents consider six job satisfaction factors that relate to NNSA's management of the security function "inadequately provided." They are critical factors for developing workforce expertise, yet they are reported to be relative weaknesses in the NNSA federal workplace:

- Management and staff support for the security mission

- Proper equipment and support to do your job

- Opportunity for career advancement and promotion

- Quality of internal communication in your organization

- Recognition and rewards for outstanding job performance

- Opportunity for career education and training.

The combined low ratings for importance of career, education, and training factors and the low ratings for the provision of these factors suggests a workplace culture that is not conducive to fostering high levels of security workforce expertise.

## Discussion

This section of the survey asked the respondent: "How important are each of the following job-related factors and how well are they provided by your current organization?" The survey covered 17 job-related factors. Table C-1 shows the survey responses.

*Table C-1. Survey Responses on Job Satisfaction*

| Job satisfaction (first row is category; second row is the degree of satisfaction with the employer's provision) | Responses | 1 = Unimportant/ inadequately provided | | 2 = Somewhat unimportant/slightly inadequately provided | | 3 = Neutral | | 4 = Important/ adequately provided | | 5 = Highly important/well provided | | Mean value | Gap: provision versus importance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % | No. | % |
| Compensation | 101 | 0 | 0 | 0 | 0 | 2 | 2 | 26 | 25 | 73 | 71 | 4.7 | — |
| Satisfaction with provision | 99 | 8 | 8 | 14 | 14 | 32 | 31 | 25 | 24 | 20 | 19 | 3.4 | -1.3 |
| Benefits | 100 | 0 | 0 | 0 | 0 | 3 | 3 | 17 | 17 | 80 | 78 | 4.8 | — |
| Satisfaction with provision | 99 | 2 | 2 | 9 | 9 | 33 | 32 | 25 | 24 | 30 | 29 | 3.7 | -1.0 |
| Employment security | 100 | 0 | 0 | 0 | 0 | 4 | 4 | 17 | 17 | 79 | 77 | 4.8 | — |
| Satisfaction with provision | 99 | 12 | 12 | 11 | 11 | 36 | 35 | 17 | 17 | 23 | 22 | 3.3 | -1.5 |
| Physical working environment | 100 | 1 | 1 | 0 | 0 | 20 | 19 | 43 | 42 | 36 | 35 | 4.1 | — |
| Satisfaction with provision | 99 | 12 | 12 | 13 | 13 | 38 | 37 | 22 | 21 | 14 | 14 | 3.1 | -1.0 |
| Professional reputation of your employer | 101 | 2 | 2 | 0 | 0 | 7 | 7 | 31 | 30 | 61 | 59 | 4.5 | — |
| satisfaction with provision | 98 | 7 | 7 | 23 | 22 | 43 | 42 | 17 | 17 | 8 | 8 | 3.0 | -1.5 |
| Interesting and challenging work | 100 | 0 | 0 | 0 | 0 | 1 | 1 | 21 | 20 | 78 | 76 | 4.8 | — |
| Satisfaction with provision | 99 | 5 | 5 | 8 | 8 | 28 | 27 | 29 | 28 | 29 | 28 | 3.7 | -1.1 |
| Clear expectations for your job performance | 100 | 0 | 0 | 0 | 0 | 3 | 3 | 25 | 24 | 72 | 70 | 4.7 | — |
| Satisfaction with provision | 98 | 13 | 13 | 22 | 21 | 21 | 20 | 21 | 20 | 21 | 20 | 3.2 | -1.5 |
| Proper equipment and support to do your job | 100 | 0 | 0 | 0 | 0 | 2 | 2 | 33 | 32 | 65 | 63 | 4.6 | — |
| Satisfaction with provision | 99 | 25 | 24 | 20 | 19 | 24 | 23 | 16 | 16 | 14 | 14 | 2.7 | -1.9 |
| Management and staff support for the security mission | 100 | 0 | 0 | 0 | 0 | 3 | 3 | 19 | 18 | 78 | 76 | 4.8 | — |
| Satisfaction with provision | 99 | 29 | 28 | 19 | 18 | 23 | 22 | 19 | 18 | 9 | 9 | 2.6 | -2.2 |
| Opportunities to demonstrate and improve your skills | 99 | 0 | 0 | 1 | 1 | 8 | 8 | 23 | 22 | 67 | 65 | 4.6 | — |
| Satisfaction with provision | 100 | 15 | 15 | 19 | 18 | 34 | 33 | 22 | 21 | 10 | 10 | 2.9 | -1.6 |

*Table C-1. Survey Responses on Job Satisfaction (Continued)*

| Job satisfaction (first row is category; second row is the degree of satisfaction with the employer's provision) | Responses | 1 = Unimportant/ inadequately provided | | 2 = Somewhat unimportant/slightly inadequately provided | | 3 = Neutral | | 4 = Important/ adequately provided | | 5 = Highly important/well provided | | Mean value | Gap: provision versus importance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % | No. | % |
| Recognition and rewards for outstanding performance | 100 | 1 | 1 | 0 | 0 | 11 | 11 | 28 | 27 | 60 | 58 | 4.5 | — |
| Satisfaction with provision | 99 | 22 | 21 | 18 | 17 | 26 | 25 | 17 | 17 | 16 | 16 | 2.9 | -1.6 |
| Opportunity for career education and training | 100 | 0 | 0 | 1 | 1 | 14 | 14 | 28 | 27 | 57 | 55 | 4.4 | — |
| Satisfaction with provision | 99 | 23 | 22 | 23 | 22 | 30 | 29 | 20 | 19 | 3 | 3 | 2.6 | -1.8 |
| Opportunity for career advancement & promotion | 100 | 0 | 0 | 1 | 1 | 7 | 7 | 29 | 28 | 63 | 61 | 4.5 | — |
| satisfaction with provision | 99 | 26 | 25 | 29 | 28 | 22 | 21 | 18 | 17 | 4 | 4 | 2.4 | -2.1 |
| being treated with respect | 100 | 0 | 0 | 0 | 0 | 0 | 0 | 25 | 24 | 75 | 73 | 4.8 | — |
| satisfaction with provision | 99 | 13 | 13 | 10 | 10 | 28 | 27 | 28 | 27 | 20 | 19 | 3.3 | -1.4 |
| Opportunity to work with others you respect | 100 | 0 | 0 | 0 | 0 | 6 | 6 | 37 | 36 | 57 | 55 | 4.5 | — |
| Satisfaction with provision | 99 | 8 | 8 | 10 | 10 | 33 | 32 | 34 | 33 | 14 | 14 | 3.4 | -1.1 |
| Quality of internal communication in your organization | 100 | 0 | 0 | 0 | 0 | 6 | 6 | 41 | 40 | 53 | 51 | 4.5 | — |
| Satisfaction with provision | 99 | 21 | 20 | 21 | 20 | 26 | 25 | 25 | 24 | 6 | 6 | 2.7 | -1.7 |
| Opportunity to make a nationally important contribution | 100 | 3 | 3 | 2 | 2 | 13 | 13 | 39 | 38 | 43 | 42 | 4.2 | — |
| Satisfaction with provision | 99 | 11 | 11 | 8 | 8 | 45 | 44 | 21 | 20 | 14 | 14 | 3.2 | -1.0 |
| Overall satisfaction | 101 | 12 | 12 | 24 | 23 | 31 | 30 | 25 | 24 | 9 | 9 | 3.0 | — |

To judge importance, respondents had a range of 1 to 5 for job-related factors, where

- 1 = not important;
- 2 = somewhat unimportant;
- 3 = neutral;
- 4 = somewhat important; and
- 5 = highly important.

For each job-related factor, we calculated the mean response to gauge the importance of the factor. Table C-2 ranks the provision adequacy of job-related factors from most important to least important. In every case, the average score exceeds four (column 2), indicating that each of the listed factors is considered important or very important by a large majority of the federal workforce.

*Table C-2. Job Satisfaction Factors Ranked by Importance*

| Job satisfaction factor | Mean importance | Mean provision | "Gap" | Note: pct "inadequate" |
|---|---|---|---|---|
| Benefits | 4.8[a] | 3.7 | –1.0 | 2 |
| Employment security | 4.8[a] | 3.3 | –1.5 | 12 |
| Interesting and challenging work | 4.8[a] | 3.7 | –1.1 | 5 |
| Management and staff support for the security mission | 4.8[a] | 2.6 | –2.2 | 29 |
| Being treated with respect | 4.8[a] | 3.3 | –1.5 | 13 |
| Compensation | 4.7[a] | 3.4 | –1.3 | 8 |
| Clear expectations for your job performance | 4.7[a] | 3.2 | –1.5 | 13 |
| Proper equipment and support to do your job | 4.6 | 2.7 | –1.9 | 24 |
| Opportunities to demonstrate and improve your skills | 4.5 | 2.9 | –1.6 | 15 |
| Professional reputation of your employer | 4.5 | 3.0 | –1.5 | 7 |
| Opportunity to work with others you respect | 4.5 | 3.4 | –1.1 | 8 |
| Opportunity for career advancement and promotion | 4.5 | 2.4 | –2.1 | 25 |
| Quality of internal communication in your organization | 4.5 | 2.7 | –1.7 | 20 |
| Recognition and rewards for outstanding job performance | 4.5 | 2.9 | –1.6 | 22 |
| Opportunity for career education and training | 4.4 | 2.6 | –1.8 | 22 |
| Opportunity to make a nationally important contribution | 4.2 | 3.2 | –1.0 | 11 |
| Physical working environment | 4.1 | 3.1 | –1.0 | 12 |

[a] Seventy percent or more of the workforce considers this factor "highly important."

The top seven factors in column 2 appear particularly important to the federal workforce: seventy percent or more responded that they are "highly important." They include the bread and butter issues of benefits, security, and compensation. They also include four key workplace environmental factors: interesting and challenging work, management support, respect, and clear expectations.

Although none of the other workplace factors can be said to be unimportant to the federal workforce, some factors most relevant to workforce expertise fall toward the bottom in the federal workforce's ranking. These include opportunities to demonstrate and improve skills, opportunities for career advancement and promotion, and opportunity for career education and training.

## Provision in Relation to Importance

We asked respondents to rank the level to which a factor was provided on a scale of 1 to 5, where

- 1 = inadequate;
- 2 = somewhat inadequate;
- 3 = neutral;
- 4 = provided; and
- 5 = well provided.

Column 3 of Table C-2 shows the means of these responses. Ten of the 17 factors had an average provision rating of 3 or higher, with a highest average rating of 3.7. These better-than-neutral ratings thus fall somewhere between "neutral" and "provided." Six of the top seven are rated at 3.0 or better. Indeed, three of the top seven factors—benefits, compensation, and interesting and challenging work—are rated the best provided of all the factors.

The remaining factors have a mean provision rating below 3, falling between "neutral" and "somewhat inadequate." These include such key factors as management support for the mission, opportunity for career education and training, opportunity for career advancement and promotion, opportunities to demonstrate and improve skills, recognition and rewards, internal communication, and proper equipment to do the job. These management and career development factors are key to the development of workforce expertise, so the evidence of weakness in these areas is a significant concern.

For each factor, the difference between the importance and provision scores indicates the "gap" between importance to the workforce and the adequacy of its provision. The calculated gaps provide an index that confirms the general relationships discussed above. Since the average score for importance exceeds the average assessment of provision in every case, the reported gaps are all negative,

ranging from −1 to −2.2. The top four largest gaps are for management support of the mission, opportunity for career advancement, education and training, and proper equipment to do the job (all of these are 1.8 or greater, indicating that provision is especially weak compared with importance).

To highlight cases where there might be strong dissatisfaction with the provision of a factor, the column 5 reports the percentage of responses of "inadequate" provision. The frequency of "inadequate" is quite low (less than 10 percent) for three of the top seven factors: benefits, compensation, and interesting and challenging work, suggesting that these factors are relative strengths in the NNSA workplace. Management support stands out among the top seven: nearly 30 percent of the respondents report its provision as "inadequate." Of the seven key management and career development factors noted above, 15 percent or more of the respondents rated the provision of these factors "inadequate," and all but one exceeded 20 percent.

# KEY ENTERPRISE SUCCESS FACTORS

## Summary

Fewer than 20 percent of the federal workforce say that the NNSA security enterprise is excelling in key organizational success factors, such as defining the clarity of government and contractor roles, employing world-class systems and processes, educating and training the workforce, and hiring top personnel.

The majority disagree or strongly disagree that the existing training and education of the federal workforce is adequate.

## Discussion

This group of questions focused on characteristics of successful enterprise environments. We asked respondents to rate nine statements using a scale of 1 (strongly disagree) to 5 (strongly agree).

Table C-3 shows the statements, along with a summary of the responses. (Table C-4 presents the survey responses.) Column 2 shows the percentage of responses that disagree or strongly disagree with each statement. Column 3 shows the percentage that agree or strongly agree. These two percentages are juxtaposed to illustrate the balance of opinion within the workforce. In addition, column 4 shows the percentage who strongly agreed with each statement, to demonstrate the workforce's opinion on whether the enterprise is excelling in the areas covered.

There is not much support for the belief that the security enterprise is excelling across the board in any of these areas. The "strongly agree" responses are between 9 and 17 percent for the questions on roles, systems, and processes. They range

from 1 to 5 percent for the federal workforce expertise and recruitment statements and from 8 to 14 percent for the comparable contractor workforce statements.

For the three statements regarding roles, systems, and processes, the favorable responses roughly equal or exceed the disagreements. For the three statements regarding federal workforce expertise and recruitment variables, disagreement strongly dominates agreement with the statements. This implies a high degree of dissatisfaction with the current situation. The results are somewhat more positive for the contractor workforce.

*Table C-3. Workforce Views on Key Enterprise Success Factors*

| Organizational success factor | Disagree or disagree strongly (%) | Agree or agree strongly (%) | Note: Percent who agree strongly |
|---|---|---|---|
| Roles, System Capabilities, and Processes | | | |
| The respective roles and responsibilities of the federal and contractor workforce are appropriate and well understood | 28 | 46 | 17 |
| My site employs world-class security systems and methods in my assigned area | 37 | 34 | 13 |
| Lessons learned processes are timely in identifying and resolving security challenges. | 28 | 37 | 9 |
| Federal Workforce Expertise and the Hiring of Expertise | | | |
| Existing federal workforce training, education, and experience is adequate to meet security challenges. | 51 | 23 | 5 |
| The federal security organization is able to attract new hires with appropriate credentials in education, training, and experience. | 62 | 10 | 1 |
| The federal security organization is successful in recruiting from among the nation's best security professionals. | 63 | 7 | 2 |
| Contractor Workforce Expertise and the Hiring of Expertise | | | |
| My site's contractor's training, education, and experience is appropriate. | 29 | 39 | 8 |
| My site's contractor is able to attract new hires with appropriate credentials in education, training, and experience. | 32 | 38 | 14 |
| My site's contractor is successful in recruiting from among the nation's best security professionals. | 32 | 30 | 11 |

*Table C-4. Survey Responses on Key Organizational Success Factors*

| | Responses | 1 = Strongly disagree | | 2 = Disagree | | 3 = Neutral | | 4 = Agree | | 5 = Strongly agree | | No direct knowledge or no opinion | | Mean |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % | No. | % | No. |
| Respective roles and responsibilities of fed & contractor workforce appropriate & well understood | 99 | 6 | 6 | 23 | 22 | 12 | 12 | 40 | 39 | 17 | 17 | 1 | 1.0 | 3.4 |
| My site employees world-class security systems & methods in my assigned area | 99 | 13 | 13 | 25 | 24 | 20 | 19 | 22 | 21 | 13 | 13 | 6 | 5.8 | 2.8 |
| Lessons learned processes are timely in identifying & resolving security challenges | 99 | 11 | 11 | 18 | 17 | 29 | 28 | 29 | 28 | 9 | 9 | 3 | 2.9 | 3.0 |
| Existing federal workforce training, education, and experience are adequate to meet security challenges | 99 | 21 | 20 | 32 | 31 | 21 | 20 | 19 | 18 | 5 | 5 | 1 | 1.0 | 2.5 |
| Federal security organization is able to attract new hires with appropriate credentials | 99 | 32 | 31 | 32 | 31 | 20 | 19 | 9 | 9 | 1 | 1 | 5 | 4.9 | 2.0 |
| Federal security organization is successful in recruiting from among the nation's best security professionals | 99 | 32 | 31 | 33 | 32 | 21 | 20 | 5 | 5 | 2 | 2 | 6 | 5.8 | 1.9 |
| My site's contractor's training, education, and experience is appropriate | 99 | 10 | 10 | 20 | 19 | 19 | 18 | 32 | 31 | 8 | 8 | 10 | 9.7 | 2.8 |
| My site's contractor is able to attract new hires with appropriate credentials | 99 | 12 | 12 | 21 | 20 | 16 | 16 | 25 | 24 | 14 | 14 | 11 | 10.7 | 2.7 |
| My site's contractor is successful in recruiting from among the nation's best security professionals | 99 | 18 | 17 | 15 | 15 | 24 | 23 | 20 | 19 | 11 | 11 | 11 | 10.7 | 2.6 |

# WOULD YOU RECOMMEND NNSA FEDERAL EMPLOYMENT, AND WHY?

## Summary

Forty-four percent of respondents would recommend their organization as a good place to work. At the same time, about one-quarter of the workforce "strongly disagree" that their organization is a good place to work.

The majority of respondents would not recommend their organization as a good place to work. The leading reasons for not recommending their organization fall into two categories: understaffed and lack resources (32 percent of respondents) and poor management (18 percent of respondents.)

Only 2 percent of respondents to this question cited lack of benefits and salary.

## Discussion

In the survey, we included a question asked in the team's focus groups. We asked respondents to assess the statement: "I would recommend this organization as a good place to work" on a scale from strongly disagree (1) to strongly agree (5). Table C-5 shows the results.

*Table C-5. Would You Recommend NNSA Federal Employment to a Friend or Relative?*

| | Responses | 1= Strongly disagree | | 2 = Disagree | | 3 = Neutral | | 4 = Agree | | 5 = Strongly agree | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % |
| I would recommend organization as a good place to work. | 100 | 24 | 23% | 16 | 16% | 16 | 16% | 24 | 23% | 20 | 19% |

The responses indicate 23 percent strongly disagree and 16 percent disagree that they would recommend NNSA as a place of employment to a friend or relative. Forty-four percent strongly agree or agree that they would recommend NNSA to their family and friends.

We also asked respondents to explain, in text, why they gave this answer. We divided the results into six categories (Table C-6).

*Table C-6. Reasons Why*

| | Responses | Yes, would recommend (all reasons) | | No, under-staffed and lack resources to do the job | | No, poor management | | No, lack of benefits and salary | | No, lack of promotion potential | | No, other reasons | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % | No. | % |
| Why would or would not recommend organization as a good place to work. | 75 | 32 | 43 | 24 | 32 | 12 | 16 | 2 | 3 | 2 | 3 | 3 | 4 |

Respondents who would recommend NNSA indicated that they appreciated the challenge of the work and liked their working environment. Most respondents who would not recommend NNSA indicated that it was due to lack of staff and resources to do the job. Respondents who commented cited a rise in overtime and a significant backlog in fulfilling daily duties as evidence of lack of staff or resources. Sixteen percent cited poor management as a reason not to recommend NNSA. Respondents who commented noted a management failure to keep personnel informed of organizational changes and a general lack of respect or knowledge of the respondent's duties. Lack of promotion potential and lack of benefits and salary are not major factors why a respondent would not recommend NNSA.

# SURVEY RESPONSES ON AREAS FOR NNSA IMPROVEMENT

## Summary

Respondents made 82 recommendations for changes to better meet NNSA's security challenges. These fell into four main categories:

- Strengthen the professional development of the NNSA security workforce (36 percent).
- Resolve NNSA-wide organizational and management issues (28 percent).
- Eliminate poor performers—whether NNSA managers or staff (18 percent).
- Increase NNSA security staff and resources to the appropriate levels (18 percent).

Respondents made 80 recommendations for the *one thing* they would change or purchase to better do their jobs. These fell into the following categories:

- Improve the management in my area (33 percent).
- Provide additional personnel to accomplish the work in my area (26 percent).
- Provide better equipment (15 percent).
- Increase promotion opportunities (10 percent).
- Strengthen training (8 percent).
- Other (8 percent).

## Discussion

We invited respondents to write in recommendations for needed changes in two areas. The first broadly addressed NNSA's mission accomplishment. The second addressed the respondent's job performance.

The first write-in question asked respondents what recommendations they have for helping NNSA meet its security challenges. While conducting a content analysis of the 103 written comments, we identified recurring themes in the responses. We grouped these themes into four general categories: better professional development, resolve organizational issues, eliminate poor managers/employees, and increase resources.

Of all respondents to this question, 29 percent desired better professional development, including more training opportunities, the time to take training, and trips to professional conferences. Twenty-two percent identified the need to resolve ongoing organizational changes, and 15 percent wrote that unproductive managers and employees should be terminated or reassigned, stating that the lack of production causes them to work overtime. Finally, 29 percent of respondents identified needed improvements in the management of personnel. Of these, 14 percent cited insufficient staffing and excessive workloads as the problem, and 15 percent cited the need to remove poor-performing staff or managers as the problem.

Table C-7 summarizes these results.

*Table C-7. Recommendations for Better Meeting NNSA's Security Challenges*

| | Responses | Better professional development | | Resolve organizational/ management issues | | Eliminate poor managers and employees | | Increase staff and resources to the appropriate level | |
|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % |
| What recommended changes would you make to better meet NNSA's security challenges? | 82 | 30 | 29 | 23 | 22 | 15 | 15 | 14 | 14 |

The second write-in question asked respondents what one change or purchase would make their job better. Again, we conducted a content analysis and identified several general themes that we subsequently grouped into six categories. The most common single recommended change (27 responses) to improve the respondent's ability to do his or her job is to improve NNSA's management of the security function. Personnel management issues were also prominent: 20 percent identified the need for additional personnel to ease their workload, and 14 percent mentioned other personnel management issues, such as training and promotional opportunities. Twelve percent identified needs for specific pieces of equipment that would make them more efficient in their tasks.

Table C-8 summarizes these results.

*Table C-8. One Change or Purchase Relating to the Respondent's Job*

| | Responses | Better equipment | | Training | | Promotion opportunities | | Additional personnel | | Improved management | | Other | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % | No. | % |
| One thing about job to change, purchase, or acquire that would make job better | 80 | 12 | 12 | 6 | 6 | 8 | 8 | 21 | 20 | 27 | 26 | 6 | 6 |

# FUTURE WORKFORCE CAPABILITIES AND KNOWLEDGE

## Summary

The federal security workforce sees the need for a broad range of capabilities and knowledge, including knowledge of threats and facilities' operations, technical skills, and process and management skills:

- At least one-half the respondents rate six areas of knowledge "highly important": security threats, NNSA's security strategy, understanding of the facility and ongoing programs, vulnerability assessment methods, technical background in the work area, and resource and program management skills.

- Essentially the same capability and knowledge needs are identified for the contractor workforce as for the federal workforce.
- There was virtually no disagreement that any area will be important.

## Discussion

We asked respondents to assess the relative importance of the following credentials needed by the future federal and contractor workforces:

- Knowledge of security threats
- Knowledge of NNSA's security strategy
- Knowledge of vulnerability assessment methods
- Knowledge of the facility and ongoing programs
- Technical background in the work area
- Knowledge of root cause procedures
- Knowledge of audit and assessment procedures
- Resource and program management skills
- Personnel management skills
- Skills in external communications with the community and media.

Respondents ranked these future workforce capabilities from 1 (not important) to 5 (highly important). Every area was rated either important or highly important for both future federal and contractor workforces (Table C-9). The mean rating of the importance in each area of knowledge roughly equals or exceeds 4 ("important") for every category. The top three areas, all with means above 4.5, are knowledge of security threats, NNSA's security strategy, and the facility and ongoing programs. Fewer than 5 percent thought any of the areas of knowledge were "unimportant" or "somewhat unimportant." We conclude that the federal security workforce sees the need for a broad range of capabilities and knowledge.

The federal workforce's assessment of the knowledge requirements for the contractor workforce strongly parallels that for the federal workforce.

*Table C-9. Survey Responses on Importance of Future Workforce Capabilities*

| | Responses | 1 = Unimportant | | 2 = Somewhat important | | 3 = Neutral | | 4 = Important | | 5 = Highly important | | Mean |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % | |
| Importance that the Federal Workforce has knowledge of | | | | | | | | | | | | |
| Security threats | 99 | 0 | 0 | 1 | 1 | 1 | 1 | 22 | 21 | 75 | 73 | 4.7 |
| NNSA's security strategy | 99 | 0 | 0 | 2 | 2 | 6 | 6 | 27 | 26 | 64 | 62 | 4.5 |
| Vulnerability assessment methods 1 | 99 | 0 | 0 | 0 | 0 | 14 | 14 | 31 | 30 | 54 | 52 | 4.4 |
| The facility and ongoing programs | 99 | 0 | 0 | 0 | 0 | 8 | 8 | 26 | 25 | 65 | 63 | 4.6 |
| Technical background in the work area | 99 | 1 | 1 | 0 | 0 | 9 | 9 | 35 | 34 | 54 | 52 | 4.4 |
| Root cause procedures | 99 | 0 | 0 | 4 | 4 | 18 | 17 | 40 | 39 | 37 | 36 | 4.1 |
| Audit and assessment procedures 1 | 99 | 0 | 0 | 2 | 2 | 17 | 17 | 30 | 29 | 50 | 49 | 4.3 |
| Resource and program management skills | 99 | 0 | 0 | 1 | 1 | 10 | 10 | 33 | 32 | 55 | 53 | 4.4 |
| Personnel management skills | 99 | 0 | 0 | 1 | 1 | 16 | 16 | 34 | 33 | 48 | 47 | 4.3 |
| Skills in external communication with community and media | 99 | 2 | 2 | 6 | 6 | 28 | 27 | 25 | 24 | 38 | 37 | 3.9 |
| Importance that the contractor has knowledge of | | | | | | | | | | | | |
| Security threats | 98 | 0 | 0 | 1 | 1 | 3 | 3 | 20 | 19 | 74 | 72 | 4.7 |
| Vulnerability assessment methods 1 | 99 | 0 | 0 | 1 | 1 | 9 | 9 | 27 | 26 | 61 | 59 | 4.5 |
| The facility and ongoing programs | 98 | 0 | 0 | 0 | 0 | 8 | 8 | 26 | 25 | 64 | 62 | 4.6 |
| Root cause procedures | 98 | 0 | 0 | 2 | 2 | 17 | 17 | 29 | 28 | 50 | 49 | 4.3 |
| Audit and assessment procedures 1 | 98 | 0 | 0 | 2 | 2 | 12 | 12 | 35 | 34 | 49 | 48 | 4.3 |
| Resource and program management skills | 98 | 0 | 0 | 2 | 2 | 13 | 13 | 30 | 29 | 53 | 51 | 4.4 |
| Personnel management skills | 98 | 0 | 0 | 4 | 4 | 14 | 14 | 35 | 34 | 45 | 44 | 4.2 |
| Skills in external communication with community and media | 98 | 2 | 2 | 7 | 7 | 25 | 24 | 22 | 21 | 42 | 41 | 4.0 |

# IMPORTANCE AND AVAILABILITY/USE OF TRAINING

## Summary

Fifty-five percent of the respondents disagree that education and training opportunities are adequate to meet future security challenges.

Technical training and training in security procedures are the two areas deemed "highly important" by more than half the workforce; in these areas, between 20 and 30 percent have received no training.

In other areas, there is spotty availability and use of training. In particular,

- 60 percent have received no career counseling, and
- 40 percent have received no formal on-the-job training.

Regarding technical certification,

- One-third of the workforce consider NNSI certification "highly important"; nearly 60 percent report some use, and 23 percent report "extensive use or completion" of NNSA certification;
- All of those with cyber expertise consider SANS important, 61 percent report "some use," and 15 percent report "extensive use or completion"; and
- Only 14 percent consider ASIS certification highly important, and only about 1 percent have made extensive use.

## Discussion

We asked respondents to assess the importance of education and training, as well as the availability and use of this training. (Table C-10 shows the survey results.) The first group of questions focused on areas of training: technical, procedural, leadership and management, career development. The second group of questions focused on alternative modes for providing the training. The third group of questions addressed the importance and employment of professional certification.

We reviewed the responses to these questions in two ways. First, we noted all questions where 30 percent or more of the respondents rated the provision of a job-related factor as less than adequate (that is, a training/availability rate of less than 70 percent on these factors). Second, we noted all questions where the average response values for importance and availability/use differed by greater than 1.5—large differences indicate that importance of a factor to the employees is not matched by its availability/use.

*Table C-10. Survey Responses on Education, Training, and Professional Certification—Availability, Use, and Importance*

| | Responses | 1 = Not available/ not important | | 2 = Available but not used/ somewhat unimportant | | 3 = Some use/ neutral on importance | | 4 = Extensive use/ important | | 5 = Highly important | | Percent with some use or extensive use | Mean valuation of importance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % | | |
| **Areas of Training** | | | | | | | | | | | | | |
| Technical training | 99 | 16 | 16 | 11 | 11 | 53 | 51 | 19 | 18 | — | — | 70 | — |
| Availability and use importance | 98 | 2 | 2 | 0 | 0 | 13 | 13 | 27 | 26 | 56 | 54 | — | 4.4 |
| Training in security procedures | 100 | 11 | 11 | 8 | 8 | 50 | 49 | 31 | 30 | — | — | 79 | — |
| Availability and use importance | 99 | 2 | 2 | 0 | 0 | 8 | 8 | 31 | 30 | 58 | 56 | — | 4.4 |
| Leadership and management courses | 101 | 12 | 12 | 26 | 25 | 54 | 52 | 9 | 9 | — | — | 61 | — |
| Availability and use importance | 98 | 2 | 2 | 2 | 2 | 27 | 26 | 29 | 28 | 38 | 37 | — | 4.0 |
| Career planning and development | 99 | 25 | 24 | 33 | 32 | 35 | 34 | 6 | 6 | — | — | 40 | — |
| Availability and use importance | 99 | 1 | 1 | 3 | 3 | 30 | 29 | 26 | 25 | 39 | 38 | — | 4.0 |
| **Alternative Modes of Training** | | | | | | | | | | | | | |
| Tuition reimbursement or assistance programs | 98 | 32 | 31 | 42 | 41 | 17 | 17 | 7 | 7 | — | — | 23 | — |
| Availability and use importance | 97 | 3 | 3 | 3 | 3 | 40 | 39 | 21 | 20 | 30 | 29 | — | 3.7 |
| Distance learning courses | 99 | 16 | 16 | 32 | 31 | 46 | 45 | 5 | 5 | — | — | 50 | — |
| Availability and use importance | 97 | 1 | 1 | 3 | 3 | 48 | 47 | 26 | 25 | 19 | 18 | — | 3.6 |
| Formal training and apprenticeships | 99 | 27 | 26 | 8 | 8 | 47 | 46 | 17 | 17 | — | — | 62 | — |
| Availability and use importance | 98 | 2 | 2 | 2 | 2 | 22 | 21 | 3 | 29 | 42 | 41 | — | 4.1 |
| Seminars, professional conferences, and symposia | 99 | 12 | 12 | 20 | 19 | 54 | 52 | 13 | 13 | — | — | 65 | — |
| Availability and use importance | 99 | 1 | 1 | 0 | 0 | 19 | 18 | 38 | 37 | 41 | 40 | — | 4.2 |
| **Technical or Professional Certification** | | | | | | | | | | | | | |
| Technical or professional certification | 96 | 26 | 25 | 23 | 22 | 36 | 35 | 11 | 11 | — | — | 46 | — |
| Availability and use importance | 97 | 1 | 1 | 1 | 1 | 31 | 30 | 32 | 31 | 32 | 31 | — | 4.0 |

*Table C-10. Survey Responses on Education, Training, and Professional Certification—Availability, Use, and Importance (Continued)*

| | Responses | 1 = Not available/ not important | | 2 = Available but not used/ somewhat unimportant | | 3 = Some use/ neutral on importance | | 4 = Extensive use/ important | | 5 = Highly important | | Percent with some use or extensive use | Mean valuation of importance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % | | |
| Technical or professional certification (NNSI) | 94 | 14 | 14 | 19 | 18 | 37 | 36 | 24 | 23 | — | — | 59 | — |
| Availability and use importance | 91 | 3 | 3 | 1 | 1 | 27 | 26 | 26 | 25 | 34 | 33 | — | 4.0 |
| Technical or professional certification (SANS) | 94 | 48 | 47 | 31 | 30 | 11 | 11 | 4 | 4 | — | — | 15 | — |
| Availability and use importance | 91 | 10 | 10 | 6 | 6 | 44 | 43 | 16 | 16 | 15 | 15 | — | 3.2 |
| Technical or professional certification (ASIS) | 91 | 46 | 45 | 29 | 28 | 15 | 15 | 1 | 1 | — | — | 16 | — |
| Availability and use importance | 90 | 6 | 6 | 7 | 7 | 48 | 47 | 15 | 15 | 14 | 14 | — | 3.3 |

We also asked whether education and training are adequate to meet today's security challenges. Table C-11 shows the results. Only about one-third of the federal workforce "agree" or "strongly agree" that the education and training of the federal workforce is adequate to build and sustain a workforce that can meet security challenges; indeed, between one-quarter and one-third of the workforce strongly disagrees that education and training is adequate.

*Table C-11. Survey Responses, Education and Training—Adequacy to Meet Security Challenges*

| | Responses | 1 = Strongly disagree | | 2 = Disagree | | 3 = Neutral | | 4 = Agree | | 5 = Strongly agree | | Mean |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % | |
| Education and training operations sufficient to create a security workforce capable of meeting emerging security challenges | 101 | 29 | 28 | 26 | 25 | 13 | 13 | 24 | 23 | 9 | 9 | 2.6 |
| Access to professional education and training is sufficient to build and sustain a competent workforce | 101 | 33 | 32 | 24 | 23 | 12 | 12 | 23 | 22 | 9 | 9 | 2.5 |

# WORKFORCE MOBILITY AND WILLINGNESS TO MOVE

## Summary

Thirty-three percent of respondents have moved for job-related reasons in the last 10 years.

Sixty-one percent of security personnel across the complex respond that they are unwilling or slightly unwilling to relocate.

Thirteen survey respondents had been asked to move as part of DOE's ongoing reorganization. Of these, nine said they are unwilling or somewhat unwilling to move, and three expressed a high degree of willingness to move.

## Discussion

Tables C-12 and C-13 show survey responses on the workers experience with job-related moves and their expressed willingness to move**.** Less than one-quarter indicate they are "willing" or "somewhat willing" to move for job-related reasons. More than 60 percent indicate that they are "unwilling" or "somewhat unwilling to move." These responses indicate a workforce that is not highly mobile.

*Table C-12. Experience with Moves; and Requirement to Move*

| | Responses | Yes | | No | |
|---|---|---|---|---|---|
| | | No. | % | No. | % |
| Moved within last 10 years for job-related reasons | 101 | 33 | 33 | 68 | 66 |
| Have been asked to move as part of the reorganization | 101 | 13 | 13 | 88 | 85 |

*Table C-13. Willingness to Move*

| | Responses | 1 = Unwilling | | 2 = Somewhat unwilling | | 3 = Indifferent | | 4 = Somewhat willing | | 5 = Willing | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % | No. | % | No. | % |
| For all respondents | | | | | | | | | | | |
| Willingness to relocate | 101[a] | 36 | 35 | 27 | 26 | 15 | 15 | 11 | 11 | 12 | 12 |
| For respondents who have been asked to move | | | | | | | | | | | |
| Willingness to relocate | 13[b] | 5 | 39 | 4 | 31 | 1 | 8 | 0 | 0 | 3 | 23 |

[a] Total sample.

[b] Sub-sample of those asked to move in the ongoing reorganization.

# SURVEY POPULATION STATISTICS

## Discussion

Tables C-14 and C-15 report the responses to questions relating to retirement and work experience**.** The demographics of the survey respondents appear to represent the overall demographics of the NNSA security workforce. Three-quarters of the respondents have been with NNSA for 7 or more years, and the respondents indicate a workforce that predominantly sees nuclear security as a career.

*Table C-14. Retirement*

| | Responses | Yes | | No | |
|---|---|---|---|---|---|
| | | No. | % | No. | % |
| Intend to remain in nuclear weapons security work until retirement | 100 | 82 | 80 | 18 | 17 |

| | Responses | 0-1 years | | 2-4 years | | 5 or more years | |
|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % |
| Years to retirement eligibility | 103 | 20 | 19 | 14 | 14 | 69 | 67 |

*Table C-15. Survey Responses on Work Experience*

| | Responses | 0-2 years | | 3-7 years | | 7 or more years | |
|---|---|---|---|---|---|---|---|
| | | No. | % | No. | % | No. | % |
| Years involved with nuclear weapons security | 98 | 8 | 8 | 15 | 15 | 75 | 73 |
| Years worked outside nuclear security field | 97 | 14 | 14 | 15 | 15 | 68 | 66 |

*RESPONSES ARE NOT FOR ATTRIBUTION*

# CONFIDENTIAL SURVEY OF FEDERAL SECURITY PERSONNEL

A. How important to you are each of the following job related factors and how well are they provided by your current organization? (1 to 5; not important to highly important; 1 to 5 inadequate to well provided)

| | | Not Important / Highly Important | Inadequate / Well Provided |
|---|---|---|---|
| 1. | Compensation (salary) | O O O O O | O O O O O |
| 2. | Benefits (e.g. insurance, vacation, sick leave, pension) | O O O O O | O O O O O |
| 3. | Employment security | O O O O O | O O O O O |
| 4. | Physical working environment | O O O O O | O O O O O |
| 5. | Professional reputation of your employer | O O O O O | O O O O O |
| 6. | Interesting and challenging work | O O O O O | O O O O O |
| 7. | Clear expectations for your job performance | O O O O O | O O O O O |
| 8. | Proper equipment and support to do your job | O O O O O | O O O O O |
| 9. | Management and staff support for the security mission | O O O O O | O O O O O |
| 10. | Opportunities to demonstrate and improve your skills | O O O O O | O O O O O |
| 11. | Recognition and rewards for outstanding job performance | O O O O O | O O O O O |
| 12. | Opportunity for career education and training | O O O O O | O O O O O |
| 13. | Opportunity for career advancement and promotion | O O O O O | O O O O O |
| 14. | Being treated with respect | O O O O O | O O O O O |
| 15. | The opportunity to work with others you respect | O O O O O | O O O O O |
| 16. | Quality of internal communication in your organization | O O O O O | O O O O O |
| 17. | Opportunity to make a nationally important contribution | O O O O O | O O O O O |
| 18. | Overall, how do you rate your organization in providing the above listed compensation, challenges, opportunities, and environment? | | O O O O O |

19. a. Have you moved within the last 10 years for job-related reasons? O yes O no
    b. Have you been asked to move as part of the reorganization? O yes O no

| | Unwilling / Indifferent / Willing |
|---|---|
| c. How willing are you to relocate? | O O O O O |

20. If you could change one aspect of your job, or purchase or acquire one thing to make your work easier, what would it be?

*RESPONSES ARE NOT FOR ATTRIBUTION*

## B. What future workforce capabilities will be needed to meet future security challenges in your area of expertise?

21. Please indicate your area(s) of work:

O Threat and Vulnerability Assessments
O MC&A,
O Personnel Security
O Cyber
O Physical and Facilities
O Management or Administration
O Other (write in) _____

22. In your assigned area of work, assess the relative importance of the credentials needed for the future federal workforce: (1 to 5; not important to highly important)

| | Not Important | | | | Highly Important |
|---|---|---|---|---|---|
| knowledge of security threats | O | O | O | O | O |
| knowledge of NNSA's security strategy | O | O | O | O | O |
| knowledge of vulnerability assessment methods | O | O | O | O | O |
| knowledge of the facility and ongoing programs | O | O | O | O | O |
| technical background in the work area | O | O | O | O | O |
| knowledge of root cause procedures | O | O | O | O | O |
| knowledge of audit and assessment procedures | O | O | O | O | O |
| resource and program management skills | O | O | O | O | O |
| personnel management skills | O | O | O | O | O |
| skills in external communications with the community & media | O | O | O | O | O |

23. In your assigned area of work, assess the relative importance of the credentials needed for the future contractor workforce:

| | | | | | |
|---|---|---|---|---|---|
| knowledge of security threats | O | O | O | O | O |
| knowledge of vulnerability assessment methods | O | O | O | O | O |
| knowledge of the facility and ongoing programs | O | O | O | O | O |
| knowledge of root cause procedures | O | O | O | O | O |
| knowledge of audit and assessment procedures | O | O | O | O | O |
| resource and program management skills | O | O | O | O | O |
| personnel management skills | O | O | O | O | O |
| skills in external communications with the community & media | O | O | O | O | O |

*RESPONSES ARE NOT FOR ATTRIBUTION*

For your site and assigned area of work, please assess the following statements (1 to 5; strongly disagree to strongly agree):

| | Strongly Disagree | | Neutral | | Strongly Agree | No direct knowledge, or no opinion |
|---|---|---|---|---|---|---|
| 24. The respective roles and responsibilities of the federal and contractor workforce are appropriate and well understood | O | O | O | O | O | O |
| 25. My site employs world-class security systems and methods in my assigned area | O | O | O | O | O | O |
| 26. Lessons learned processes are timely in identifying and resolving security challenges | O | O | O | O | O | O |
| 27. Existing federal workforce training, education, and experience is adequate to meet security challenges | O | O | O | O | O | O |
| 28. The federal security organization is able to attract new hires with appropriate credentials in education, training, and experience | O | O | O | O | O | O |
| 29. The federal security organization is successful in recruiting from among the nation's best security professionals | O | O | O | O | O | O |
| 30. My site's contractor's training, education, and experience is appropriate | O | O | O | O | O | O |
| 31. My site's contractor is able to attract new hires with appropriate credentials in education, training, and experience | O | O | O | O | O | O |
| 32. My site's contractor is successful in recruiting from among the nation's best security professionals | O | O | O | O | O | O |

*RESPONSES ARE NOT FOR ATTRIBUTION*

C. What professional training and education opportunities have you personally been provided by your current organization, and how important and effective are these for meeting future security challenges? (1 to 5 not important to highly important)

| | Not Important / Highly Important | Not available | Available but not used | Some use | Extensive use/ completed | |
|---|---|---|---|---|---|---|
| Areas of training: | | | | | | |
| 33. Technical training | | O | O | O | O | O O O O O |
| 34. Training in security procedures | | O | O | O | O | O O O O O |
| 35. Leadership and management courses | | O | O | O | O | O O O O O |
| Forms of training: | | | | | | |
| 36. Distance learning courses | | O | O | O | O | O O O O O |
| 37. Tuition reimbursement or assistance programs | | O | O | O | O | O O O O O |
| 38. Career planning and development | | O | O | O | O | O O O O O |
| 39. Formal on-the-job training and apprenticeships | | O | O | O | O | O O O O O |
| 40. Seminars, professional conferences, and symposia | | O | O | O | O | O O O O O |
| 41. Technical or professional certification | | | | | | |
| -- NNSI | | O | O | O | O | O O O O O |
| -- SANS Institute | | O | O | O | O | O O O O O |
| -- American Society for Industrial Security | | O | O | O | O | O O O O O |

Assess the following statements regarding professional education and training in your organization:

| | Strongly Disagree / Strongly Agree |
|---|---|
| 42. Education and training opportunities are sufficient to create a security workforce capable of meeting emerging security challenges | O O O O O |
| 43. New hires who do not have specialized backgrounds are provided timely training | O O O O O |

*RESPONSES ARE NOT FOR ATTRIBUTION*

## D. General Questions

44. Are you in the contractor or federal workforce? O Contractor O Federal

45. Your location plant, lab, or Site Office (SO):

| | | |
|---|---|---|
| O LANL/SO | O KC/SO | O HQ |
| O LLNL/SO | O Y-12/SO | O Albq Service Center |
| O Sandia/SO | O SR/SO | O Other _____ |
| O Pantex/SO | O NTS/SO | |

46. Do you intend to remain in the nuclear-weapons security work until you retire? No O Yes O

47. In what year are you eligible to retire? Year _____

48. For how many years have you been involved with nuclear weapons security? Years _____

49. How many years have you worked, in total, outside of the nuclear security field? Years _____

50. Would you recommend your organization as a good place to work, and why?

Strongly Disagree Strongly Agree

O O O O O

51. What recommended changes would you make to better meet NNSA's future security challenges?

# Appendix D
# Workforce Demographics and Skills Mix

To provide a factual basis for its assessments and recommendations, the team created a comprehensive census of the NNSA workforce. This census updates the 2002 Spracklen Survey of the NNSA S&S workforce to January 2004.

This appendix is based on the reported data for 145 individuals who were in the NNSA S&S workforce in January 2004. The data include workforce locations, areas of expertise, grade levels, years of experience in NNSA, retirement eligibility and planned retirement dates, and educational background.

A comparison of the current census with the data in the 2002 Spracklen Survey indicates that the field workforce (including the former Operations Offices in Albuquerque, Nevada, and Oakland and the Site Offices at the seven NNSA sites) has been reduced by about 10 percent in the year and a half between the initial census and the update.[1]

## CURRENT STAFFING LEVELS AND AUTHORIZED BILLETS

Table D-1 reports the current manpower in the NNSA S&S organization by location, the effects of the planned transfer of billets, and NNSA's targeted end-state. The final column provides an accounting of the implied gaps (both surpluses in numbers and shortfalls) across the complex of onboard personnel compared with the billets authorized for each location.

Column one shows that current manpower in the NNSA S&S organization is 145.25. (The one-quarter of a person is reported because one NNSA official at the Savannah River Site Office has one-quarter time allocated to S&S functions.)

[1] At the time of the Spracklen Survey, the field workforce was 148. The comparable count in the updated census is 129 people in the Service Center and Site Offices—a reduction of 19 people in the field. The team's updated data now include NNSA headquarters, with its 16 billets, bringing the total NNSA personnel onboard to 145.

*Table D-1. Current Staffing Levels and Ceilings (January 2004)*

| Location | Personnel onboard now | Billet transfers | Current personnel net of transferred billets | Authorized billets[a] | Gaps |
|---|---|---|---|---|---|
| Headquarters | 16 | — | 16 | 17 | –1 |
| Service Center | 45[b] | +15 | 60 | 55 | +5 |
| Nevada | 21[b] | –7 | 14 | 13 | +1 |
| Livermore | 23 | –8 | 15 | 16 | –1 |
| Sandia | 11 | — | 11 | 12 | –1 |
| Y-12 | 10 | — | 10 | 12 | –2 |
| Los Alamos | 7 | — | 7 | 10 | –3 |
| Amarillo | 8 | — | 8 | 9 | –1 |
| Kansas City | 4 | — | 4 | 5 | –1 |
| Savannah River | 0.25 | — | 0.25 | 0.25 | — |
| Total | 145.25 | — | 145.25 | 149.25 | –4 |

[a] Source: Toby Johnson, "Safeguards and Security Overview," Briefing to the Security Workforce Expertise Study Team, September 9, 2003.

[b] Nevada's data submission did not include people scheduled to transfer to the Service Center who had not yet made the move. For a consistent snapshot that reflects where the people are today, we added them back into Nevada's onboard manpower and deleted them from the Service Center submission.

## Effect of Planned Transfers

The planned consolidation of Service Center personnel from Nevada and Livermore entails the transfer of 15 billets to Albuquerque (see column 2). Nevada has formally transferred its 7 billets to Albuquerque, but the people holding these billets still remain in Nevada. Livermore has not yet made the formal transfer of its 8 billets.[2] To achieve consistent reporting across the sites of the billets affected by the transfers, we adjusted the Nevada and Albuquerque personnel numbers, so the numbers presented here provide a snapshot of where the people currently are located.

Column three presents a projection of NNSA manpower following the transfer of billets—assuming for the moment that all of the people filling the billets were to move with the billets. Under this assumption, the total manpower stays constant at 145.25, but individual site totals change to reflect the transfers. NNSA authorized billets equal 149.25, as shown in column four. Hence, across the entire organization, current manpower is 4 people below authorized billets.

[2] The people in billets transferred from NSO to the ASC have not physically moved yet. According to one DOE official, some will move in March with the remaining moves expected by the end of July.

This gap does not tell the entire story of the near-term manpower situation, however. Taking into account the effects of transfers on individual's decisions to remain in NNSA employment is also necessary. There are 15 billets scheduled to move from Nevada and Livermore to the Albuquerque Service Center. The people in these billets are still in Nevada or Livermore, and, in the coming months, many may choose to leave NNSA or retire rather than make the move. (The updated data indicate that 11 of the people in these transferring billets currently are eligible for early retirement.) NNSA asked for a declaration of intent from these people, but the team does not yet have the results.[3]

The team's federal workforce survey provides some insight into the choices that will be made by the 15 employees asked to move. The survey asked whether respondents have been asked to move as part of the reorganization; it also asks workers to rate their willingness to move. Of the survey respondents who indicated they had been asked to move, about 70 percent indicated they would be unwilling or very unwilling to move; about one-quarter indicated a strong willingness to move. This suggests that NNSA can expect to lose a substantial fraction of the 15 who currently hold the jobs being transferred to Albuquerque. We can reasonably assume that 10 of the 15 will decide to change jobs or retire when asked to move in the coming year.[4]

## Near-Term Implications for NNSA Recruitment Needs

These data indicate that NNSA is currently 4 people below its targeted authorizations. The transfers scheduled over the coming year could cause as many as 10 additional people to depart. These two factors yield a combined deficit of 14 people below NNSA's targeted end strength. The hiring program needed to replace these people is of a scale that far outstrips NNSA's recent experience.

# WORKFORCE EXPERTISE AND DEMOGRAPHICS

The census of the NNSA workforce provides additional insight on its makeup. Table D-2 describes the workforce for major areas of expertise.

[3] Declarations are made at Site Offices. No single source exists on who declared; this information still resides with the sites, and declarations are non-binding until August 3, 2004. Those declaring transfers will not likely move until FY05.

[4] Those who retire now will reduce DOE's exposure to subsequent retirements, so the shortfall resulting from the departures associated with the transfers should count as reducing the potential retirement pool. These departures, then, do not create an additional hiring need beyond that estimated for projected retirements, but they do accelerate these retirements, thus accentuating NNSA's near-term hiring challenge.

*Table D-2. S&S Personnel in Major Areas of Expertise (January 2004)*

| Area of expertise | Total | With degrees | By grade | | | | | | Can retire in 2009 or earlier | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | SES | GS-15 | GS-14 | GS-13 | GS-12 and < | EN/EJ | No. | % |
| FRAM Skill Areas | | | | | | | | | | |
| Personnel security | 44 | 18 | — | 1 | 5 | 13 | 26 | 0 | 35 | 80 |
| Classification | 13 | 10 | — | — | 3 | 2 | 3 | 4 | 12 | 92 |
| Physical security | 16 | 9 | — | — | 6 | 7 | 2 | 1 | 12 | 75 |
| MC&A | 7 | 6 | — | — | 1 | 3 | 1 | 2 | 3 | 43 |
| Cyber | 14 | 10 | — | — | 5 | 5 | 3 | 1 | 8 | 57 |
| Info security | 16 | 9 | — | — | 3 | 9 | 4 | 0 | 11 | 67 |
| Technical security | 3 | 3 | — | — | — | 1 | — | 2 | 1 | 34 |
| Management and other areas | | | | | | | | | | |
| General engineering, security specialist, multiple areas[a] | 19 | 13 | — | 1 | 9 | 2 | 5 | 2 | 15 | 79 |
| Management and administration | 14 | 12 | 2 | 6 | 4 | 0 | 1 | 1 | 9 | 64 |
| Total | 146 | 90 | 2 | 8 | 36 | 42 | 45 | 13 | 106 | 73 |

[a] Four in this category listed "general engineering" as their area of expertise. Seven listed "security specialist," five listed multiple specialties, and the remaining three listed program support specialist, team lead, and weapons program specialist.

The columns provide the following information:

1. "Areas of expertise" includes the seven areas of technical expertise that are incorporated in NNSA's FRAM and adds two categories: management and administration and "general engineering, security specialist, and multiple areas of expertise."[5]

2. "Total" equals the number of personnel assigned to each area of expertise.

3. "With degrees" provides the number of staff members in each area of expertise with a college degree.

4. "By grade" shows the number of personnel in each grade.

5. "Can retire" shows the number of people who will be eligible for early retirement by 2009 or earlier. Eligibility does not mean that an individual necessarily will retire, but it does introduce a risk that must be managed.

[5] We created these categories to enable a complete and mutually exclusive categorization of the workforce. This approach provides an unambiguous classification of personnel in the technical areas.

## Retirement Eligibility and Longer-Term Recruitment Needs

As summarized in Table D-2, 106 of the existing federal staff of 145 will be eligible to retire in the next 5 years (in 2009 or earlier). The number of actual retirees will depend on two main factors.

First, as discussed earlier, some will retire this year as part of the NNSA restructuring. We expect about 10 of the 15 employees being asked to transfer in the coming year to choose to leave NNSA employment. Of these, most are already eligible to retire. So we can expect an immediate reduction in the total workforce and in the pool of future eligible retirees. If 10 leave this year, and all are retirement eligible, NNSA will still be left with 96 employees eligible to retire by 2009.

Second, many individuals will choose to work beyond their retirement eligibility age. From the earlier Spracklen Survey, 63 of those eligible to retire in 2009 or earlier said they would not retire when they become eligible. So, if 10 leave this year, and all 63 of the remaining 96 stay, then 33 can be expected to retire after the coming year and before 2009. These projections could, of course, change for better or worse as the time approaches, depending on workplace and general economic factors.

If these two factors—restructuring and planned work beyond retirement—both act in NNSA's favor to minimize the number of staff that will need to be replaced in the coming 5 years, 43 new staff members will still need to be brought onboard over the next 5 years (10 this year and 33 thereafter)—*a replacement in 5 years of one-third of a workforce that has been largely stable for the last decade*.

So, the security community faces a tremendous challenge, and added workload. Identifying, recruiting, and hiring new employees will require considerable energy. And major efforts will be needed to train them, especially those brought in at entry levels.

## Current Skills Mix

We observed the following on the current skills mix:

- Forty-four people have skills in personnel security. Presumably, all of these personnel spend much of their time in this field, with one or two exceptions. Only 18 of the 44 have a bachelor's degree or higher (3 have an MA or MS). This is the lowest graded of the specialty areas: more than half (26) are graded at GS-12 or below. The Los Alamos and Y-12 Site Offices do not have personnel security specialists. This is particularly surprising for Los Alamos, where significant problems in prescreening have been reported. Eighty percent of these people are eligible to retire by the end of 2009.

- The classification workforce is the most senior group, with 90 percent eligible to retire in the next 5 years. People in these positions require a strong technical background and experience due to the technical nature of the judgments they are required to make. A long-term transition strategy for replacing this aging workforce is needed to ensure continuity.

- Only seven people are listed as MC&A specialists, four at the Service Center and the remainder at Livermore, Y-12, and Pantex. Sandia, Los Alamos, and Nevada lack a specialist.

- Cyber is a relatively highly educated and young area of expertise, where not more than half will be eligible to retire in the next five years.

- Only three people are listed as specialists in technical security, all with a BA, BS, or higher degree. The experience level runs from 10 to 25 years. Apparently, no next-generation person who has stayed with the program in the intervening years has been trained in this area. These security specialists are located at Pantex, Y-12, and Nevada. Two people with multiple areas of expertise list technical security as one of their areas.

- The general engineering, security specialist, multiple specialties area is included in Table D-2 to capture the workforce that did not report areas of expertise within the categories specified in the FRAM. Four in this category listed "general engineering" as their area of expertise; seven, "security specialist"; five, multiple specialties; and the remaining three, program support specialist, team lead, and weapons program specialist. Many of the people in this category hold mid-level management positions and bring technical expertise to the weapons program beyond that of the technical experts identified above.

- The management and administration category includes Site Office directors, senior managers within headquarters, and administrative staff. Most of NNSA's most senior billets are allocated to this area: two SES, six GS-15, and four GS-14. Many of the people in this category bring technical expertise to the weapons program beyond that of the technical experts identified above.

- No one is listed as specializing in vulnerability assessment. (One of the people reporting multiple areas of expertise lists vulnerability assessment as an area of expertise. That person, who is assigned to the Livermore Site Office rather than a more central location, has 36 years of experience, was expected to retire in 2002, and does not appear to have anyone else in training in this area.) Vulnerability assessment is an area of expertise that cuts across the other areas and therefore is not one of the seven skill areas being tracked in the FRAM.

Discussions pointed out the ability to expertly review and critique the contractor's vulnerability assessment work as a particularly weak area of NNSA security personnel. The federal security force should be able to thoroughly review the contractors' vulnerability assessment work to understand the risk and cost implications of proposed solutions to potential vulnerabilities.

## Skills Mix and Recruitment and Training

Regarding future skill requirements, four of the expertise areas (technical security, cyber security, MC&A, and classification) have a very high level (about 90 percent) of technical content. Presently, 37 people fill these positions, 29 of whom hold degrees.[6]

In addition, over half the physical security specialist positions require extensive technical knowledge in areas such as civil engineering, blast assessment, and threat and vulnerability assessment. In most cases, the incumbent needs a technical degree, other training, or substantive experience to compensate for the lack of a technical degree. Currently, 9 of the 16 physical security specialists have degrees.

NNSA has no overall targets for complex-wide staffing in these critical skill areas; under current management practices, the site managers determine the appropriate mix of skills within their assigned allotment of personnel, so security headquarters managers do not regularly track or assess the mix of skills in the workforce.

The Spracklen Survey did, however, provide a one-time assessment of workforce needs for each area of expertise based on a systematic inventory of security functions performed within NNSA. It thus provides the only systematic and comprehensive perspective on NNSA's workforce needs in these highly skilled areas of expertise.

The results of the Spracklen Survey were incorporated in developing the NNSA FRAM and have subsequently provided general benchmarks used by many of the sites for assessing their skill mix requirements. However, the team was told that the Spracklen Survey and FRAM do not directly link with the current skills mix goals of managers in the complex today. A top-down ceiling on the total workforce—rather than a process that uses the workload as the basis for determining the needed numbers of people in each skill area—drives the current skill mix goals. Within the available ceiling, the sites adjust their workforce, practices, and contract support as best they can to accomplish their tasks. As one NNSA official explained, the Spracklen study provides a useful perspective on skill mix needs,

[6] Individuals listed in the "general engineering, security specialist, and multiple areas" category, as well as in the management category, provide additional expertise. Nevertheless, these individuals are not dedicated to these highly technical areas, and no doubt have other duties.

but it does not dictate current site manpower goals, nor does it have official standing within the NNSA.

The workload-driven Spracklen Survey and the ceiling-driven current skills mix targets provide very different views of the needs for additional hiring of people to fill critical areas of expertise.

Table D-3 summarizes the target skill levels for the highly skilled areas discussed above that resulted from the Spracklen Survey and compares them with the current numbers of personnel onboard. Relative to the skill levels projected in the Spracklen Survey, NNSA is significantly short of technical people, by 10 people of a population of roughly 55 technical experts—assuming the 4 surplus personnel in cyber could be readily moved into another of these areas.

*Table D-3. Current Personnel versus Spracklen Study Benchmark in High-Technology Areas of Expertise*

| Area of expertise | Total on board (January 2004) | Spracklen Study "to-be" skill mix (summer 2002) | Gap |
|---|---|---|---|
| Classification | 13 | 16.5 | –3.5 |
| Physical security | 16 | 20 | –4 |
| MC&A | 7 | 9.25 | –2.25 |
| Cyber | 14 | 10 | +4 |
| Technical security | 3 | 7.75 | –4.45 |
| Sum of negatives | | | –14.5 |
| Net of cyber (+4) | | | –10.5 |

In executing the required staffing reductions since the Spracklen Study was completed, the NNSA no doubt has tried to adjust its workload requirements by reengineering tasks and by obtaining expert contract support to augment federal technical staffs. At the same time, many of these skill areas are one-deep at some sites, and the staffs are stretched very thin. These combined facts suggest that the current NNSA workforce lacks sufficient depth across the complex in these key skill areas.

NNSA, then, clearly has hiring needs in the coming years. This hiring opportunity gives it the means to implement a systematic program for hiring and training personnel in these highly technical areas. A complex-wide focus on managing the workforce in these technical areas would provide NNSA the ability to manage the one-deep challenge facing certain sites and an opportunity to develop effective succession strategies. These will be especially important in areas where the numbers are small and the current workforce is very senior.

# Appendix E
# Federal Pay Benchmarking

This appendix compares the pay available under DOE's federal salary-grade structure with the competitive pay available in national labor markets. For entry-level personnel, we based the comparisons on two information sources: the January 2003 Foushée Group survey of security compensation for entry-level security positions and a survey of starting salaries for college graduate engineers.[1] For senior NNSA technical, managerial, and executive personnel, we compare federal pay with the Foushée Group survey for senior security personnel in comparable positions.

## ENTRY-LEVEL PERSONNEL

Table E-1 compares government pay scales for GS-5, GS-7, GS-9, and Excepted Service grades 1 and 2 with Foushée survey data for entry-level security professionals. The GS pay bands are determined by "steps" within the grades. Promotion to higher steps can be awarded by a supervisor or may accrue from job tenure.

*Table E-1. Entry-Level Federal and Security Industry Pay*

| GS-and Excepted Service pay ranges available ($) | | | | | | Foushée pay data ($) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Range | GS-5 | GS-7 | GS-9 | 1 | 2 | A | B | C | D | E | Range[a] |
| Top | 34,052 | 42,177 | 51,599 | 40,860 | 59,253 | 50,124 | 50,970 | 51,236 | 49,000 | 50,576 | 75 |
| Step 5 | 29,687 | 3,6771 | 44,983 | — | — | 44,685 | 45,936 | 47,347 | 45,283 | 46,314 | Median |
| Bottom | 26,195 | 32,447 | 39,690 | 23,797 | 36,052 | 41,600 | 41,005 | 45,112 | 41,181 | 42,970 | 25 |

Note: A = network security specialist (level I); B = computer and information security specialist (level I); C = security clearance specialist (level II); investigator (level I); business unit security manager (level I).

[a] Includes 75th and 25th percentile levels.

The bands for the Foushée survey salaries range from the 75th percentile, to the median, to 25th percentile. The comparison with national market pay for entry-level engineering graduates provides a benchmark for assessing NNSA's competitiveness in recruiting personnel with strong technical credentials.

Normal federal policy is to offer GS-5 grades to college graduates (GS-7 grades to those with exceptional credentials). Within grades, managers have the

[1] Foushée Group, Inc., *Security Compensation Survey Report: 2003*, Foushée Group, Inc., 4107 Lawrenceville Highway, Suite E, Tucker, GA, 30084. Phone 770-492-0950 or www.Fousheesurvey.com. These data are used with permission of Steve Walker, Partner at the Foushée Group.

flexibility to offer up to a step 5 if needed to be competitive, so we show this pay level in the table as well.

The pay comparisons support the NNSA manager concerns that GS-5 and GS-7 are not competitive in the national job market. GS-5 step 5 is roughly $30,000, and GS-7 step 5 is about $37,000. These pay rates are below the bottom 25th percentile for every representative entry-level security position in the right half of the table.

Table E-2 shows a parallel comparison of federal pay with the entry-level pay for graduate engineers. This represents the pool of talent for which NNSA will compete to obtain technical expertise.

*Table E-2. Entry-Level Federal versus Engineering Pay*

| GS-and Excepted Service pay ranges available ($) | | | | | | Entry-level engineering pay survey ($) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Range | GS-5 | GS-7 | GS-9 | 1 | 2 | A | B | C | D | E | Range |
| Top | 34,052 | 42,177 | 51,599 | 40,860 | 59,253 | — | — | — | — | — | — |
| Step 5 | 29,687 | 36,771 | 44,983 | — | — | 38,943 | 47,692 | 48,695 | 47,200 | 51,000 | Average |
| Bottom | 26,195 | 32,447 | 39,690 | 23,797 | 36,052 | — | — | — | — | — | — |

Source: Graduating Engineering and Computer Careers On-Line.

Note: A = civil engineer; B = electrical engineering; C = computer sciences; D = mechanical engineer; E = nuclear engineer.

The pay comparisons indicate that GS-9 step 5 is about $45,000, which is competitive with entry-level pay in both the security workforce market and the engineering market. Similarly, Excepted Service grade 2 spans the range of entry-level pay offered in the national security workforce and engineering markets.

We find that the standard government policy of offering GS-5 or GS-7 grades for entry-level positions will not suffice to attract the needed technical talent into the NNSA S&S program. NNSA must use Excepted Service hiring authority or create the flexibility to offer GS-9 positions to recent engineering graduates to compete in national job markets.

# TECHNICAL AND MANAGERIAL PERSONNEL

Table E-3 compares government pay scales for GS-12 through GS-15 grades against the reported market wages for several representative categories of technical security managers. These comparisons suggest that the GS-15 grade and the higher steps of the GS-14 grade are competitive with reported market wages for security managers, GS-13 can be marginally competitive at the very top steps, and GS-12 is not. Consider the four managerial positions shown: the reported median salaries for managers in network security, computer and information security, corporate investigations, and corporate protective services range from about $87,000 to $100,000 per year. The top step in each of the GS grades is $123,000 for GS-15; $105,000 for GS-14; $89,000 for GS-13; and $75,000 for GS-12.

*Table E-3. Federal versus Security Industry Pay: Technical and Managerial*

| Federal pay ranges available ($) | | | | | | Foushée data ($) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Range | GS-12 | GS-13 | GS-14 | GS-15 | ES 4 | A | B | C | D | E | Range |
| Top | 74,826 | 88,973 | 105,145 | 123,682 | 117,527 | 82,643 | 100,002 | 105,381 | 117,156 | 115,000 | 75 |
| Step 5 | — | — | — | — | — | 72,738 | 88,200 | 86,983 | 100,158 | 93,086 | Median |
| Bottom | 57,556 | 68,443 | 80,880 | 95,136 | 73,467 | 76,514 | 95,062 | 98,745 | 110,314 | 106,541 | 25 |

Note: A = senior nuclear accountability specialist (HQ); B = manager, corporate investigation; C = manager, network security; D = manager computer info and security; E = senior manager, protective service.

Currently, NNSA has 59 federal personnel in billets that are graded GS-14 and above (including 13 that are in Excepted Service), and 87 personnel in billets graded GS-13 and below. (See Appendix D.) Our benchmarking with the NRC security workforce (and other government organizations) suggests that some other organizations with highly technical security requirements employ a larger fraction of GS-14 and -15 billets than does NNSA. From the data presented here, this would make a larger fraction of these organizations' billets more competitive with the prevailing national salaries. In contrast and due to other factors, however, the Naval Nuclear Propulsion Program runs a very effective security operation that employs relatively more GS-13 and below billets than NNSA.

In summary, we find that the government's pay scales at the GS-14 and GS-15 levels are competitive with the prevailing pay for security managers. The ability to recruit management-level security professionals will require targeting available billets to the areas of greatest need within the complex—for example, by the aggressive use of Excepted Service authority.

## TOP MANAGERS AND EXECUTIVES

Table E-4 tentatively compares government SES and executive pay scales with prevailing market wages for top security managers. Again, the bands shown for government salary reflect the different levels available within each executive pay category. The reported executive salaries provide the 75th percentile pay level, the 25th percentile, and the median.

These data seem to suggest that the higher levels of SES salaries are roughly compatible with the prevailing market salaries for some of the top executive positions. Agencies with a certified performance appraisal system can pay up to $154,000. The median reported salary is about $140,000 for a top security executive (international) or a top security executive (domestic).

*Table E-4. GS, SES, and Executive Service Pay and Security Industry: Top Managers and Executives*

| Federal pay ranges available ($) | | | | | | Foushée data ($) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Range | GS-14 | GS-15 | ES 5 | SES | EL I | A | B | C | D | E | Range |
| Top | 105,145 | 123,682 | 136,000 | 157,000 | 174,500 | 115,000 | 114,582 | 159,780 | 155,624 | 190,750 | 75 |
| Step 5 | — | — | — | — | — | 93,086 | 95,324 | 124,800 | 128,690 | 163,764 | Median |
| Bottom | 80,880 | 95,136 | 103,700 | 103,700 | 127,300 | 106,541 | 105,415 | 140,000 | 140,121 | 106,541 | 25 |

Note: A = senior manager, protective service (HQ); B = senior regional manager, domestic security; C = top security executive (domestic); D = top security executive (international); E = top global security executive.

Non-salary compensation is significant for the top security executives in the private sector, so their total compensation package can be substantially higher than indicated by the salary data. The Foushée Survey indicates that the median top security executive (international) bonus equaled $36,000, or about 25 percent of base salary. Similarly, the reported bonus for the median top security executive (domestic) was about 21 percent of base salary. Only Executive Level I pay ($174,000) matches the total compensation available to for this level of top executive.

We find that the government's pay scales at the GS-15, Excepted Service grade 5, SES, and Executive Service are competitive with the prevailing pay for senior security managers, although not with the most senior executives. As with technical personnel, the ability to recruit management-level security professionals will require targeting available billets to the areas of greatest need within the complex.

# Appendix F
# Education and Training Programs

## FINDINGS

The study team asked the federal and contractor officials at each site to comment on the educational and training programs available to develop their security professionals. The study team also visited NNSI and was briefed on its activities and proposed training and education initiatives.

DOE uses several institutions for the education and training of its security workforce. These institutions cover a wide range of subjects necessary to educate and train the next generation of security professionals. With some additional development and collaboration, they could support the needed initiatives for the education and training of DOE S&S employees, including formal qualification standards and professional certification.

Three institutions are directly involved in the education of DOE S&S personnel today:

- NNSI provides training and education tailored to the needs of DOE's nuclear program responsibilities, as well as to the Department of State, Department of Justice, and others. It has a full-time faculty of 65 professionals, covering security management, technical, and procedural courses, often designed in collaboration with DOE customers. It offers both on-site and distance learning courses in about 180 technical and management areas, as well as broad career development curricula through the Advanced Development and Professional Training (ADAPT) program and the Professional Enhancement Program (PEP). Roughly 60 DOE federal employees and contractors have completed the ADAPT program, and about 120 have completed the PEP.

- The SANS Institute provides on-line training and seminars in about 14 technical and management areas. In 1999, SANS founded GIAC, the Global Information Assurance Certification, which offers certifications that address multiple specialty areas: security essentials, intrusion detection, incident handling, firewalls and perimeter protection, operating system security, and more. Both federal and contractor specialists in cyber security use SANS training and seek SANS certifications.

- The American Society for Industrial Security (ASIS) is the primary professional organization for security practitioners. Its members represent all sectors of private industry and government. Since the 1970s, ASIS has offered the "Certified Protection Professional" (CPP) credential, which requires professional experience and completion of a proficiency exam. The CPP is not required for advancement in the federal or contractor workforces, but both federal and contractor security professionals sometimes seek the CPP as a valuable step in their professional development. ASIS offers two additional credentials: PCI, Professional Certified Investigator and PCP, Physical Security Professional.

Experts within the Sandia National Laboratories have collaborated with several universities to develop course materials and curricula for security engineering programs. Participants include Arizona State University, Indiana University of Pennsylvania, and DeVry University. These university programs offer the opportunity for in-depth engineering training in technical areas such as facility design for security, sensors, and alarms. University programs through the National Security Agency's "Centers of Excellence" programs also offer engineering training for information assurance.

# Appendix G
# Clearances

Service Center personnel are aware of the seriousness of the backlog of cleared cases and have made a number of excellent recommendations, some of which have been adopted by NNSA/DOE. NNSA and DOE headquarters have also obtained legislative authority for the Secretary of Energy to use OPM resources in addition to the FBI. Nevertheless, with DSS cases going to OPM, even with the accompanying personnel resources, we anticipate a continuing increase in the OPM and NNSA backlog for the foreseeable future.

We recommend consideration of the following in a 60-day study:

- Innovative nonstandard risk-based approaches and novel methods available outside DOE, such as DoD's ACES tool, to reduce the reinvestigation backlog.
- Internet tools, an e-clearance approach, and the RIC program proposed by the Service Center.
- A direct funding link between NNSA and OPM to dedicate additional resources to reducing the NNSA backlog to a more manageable level.
- The efficiency of processing at the Service Center.[1] Develop a long-term IT plan using advanced computing capability modeled after OPM and DSS.
- The allocation of personnel resources, to ensure that the number of federal employees addressing clearance issues is appropriate (of the 144 federal employees in NNSA, 43 have a personnel security specialty).

The RIC program mentioned above uses a creative, risk-based approach with computer-based interviews and background investigation tools. Service Center management anticipates that adoption of this approach could allow granting of an interim Q clearance in 90 days.

[1] The Service Center still uses paper forms, but OPM is rapidly moving to electronic processing of clearance applications.

# Appendix H
# Security Budgeting

In FY06, NNSA intends to move from direct funding of security activities through budgeted line items to an approach that includes some security activities in the contractor's indirect funding. The two reasons for this approach are as follows:

- NNSA has experienced situations in which the direct funding of security has not provided the flexibility needed to allocate sufficient resources to emerging security challenges.

- More fundamental, indirect funding supports NNSA's philosophy of integrating security management within the overall DOE mission.[1] Indirect funding of security operations permits (and forces) laboratory directors and plant managers to evaluate security risks and programs within the same context as programmatic operations and operations in other functional areas.

We discussed these alternative funding approaches with NNSA officials and contractor managers during our site visits. Indirect funding was the long-standing approach used in the weapons program prior to the late 1990s. The concern with a return to that is approach is that the flexibility it provides line managers could lead to a downgrading of the priority given to security. Security officials argue that, under the old system, resources commonly were diverted from security to meet other programmatic pressures. Indeed, the ability of NNSA headquarters to prevent the reallocation of security funds for other uses by field managers was one reason given for adopting the direct funding approach.

At the same time, the team repeatedly heard that the fences on security funding associated with the direct funding of the program, while designed as a safeguard

[1] The Commission on Science and Security took a very strong stand in support of the return to indirect funding. Its report concluded, "While the security staff must meaningfully engage in the deliberations over budget allocations, line management must control the resources required to execute their entire mission. The commission believes that the idea of a line-item security budget, one administered by someone other than the laboratory director (the line manager), is a particularly bad idea. It interferes with risk-management decisions—the tradeoffs—that the laboratories must make. It also restricts the ability of managers to move monies when needed … [Furthermore a] separate budget should not be confused with transparency. DOE management, the Office of Management and Budget, and Congress have every reason to want to see and understand where security budgets will be spent, including in future years, and such transparency must be provided. Transparency and central control, however, are two very different concepts." 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*, (Washington, DC: Center for Strategic and International Studies, April 2002), p. 25.

for security programs, had instead created a hurdle to obtaining the additional resources needed to strengthen security following the September 11 terrorist attacks. More flexibility to reallocate resources to security, without formal reprogramming approvals, would have better enabled laboratory directors and plant managers to address new security requirements and emerging security challenges.

In addition, federal managers briefed the study team on ongoing improvements in NNSA's management structures and practices that they believe address the concerns that security needs will be undermined by the planned return to indirect funding for security activities.

This visibility will be essential for maintaining the proper focus on and priorities of weapons complex security. The federal managers believe their strengthened resource allocation advisory responsibilities, combined with their local oversight roles, will provide the feedback loop needed to enable the Administrator to appropriately align resources with security needs. NNSA's improvements in future-year resource allocation processes are designed to increase visibility and accountability and reduce stovepiping. Site Managers are active advisors to the Administrator in this process. Site Managers also emphasized the importance of resource decision making in their major new responsibilities in the emerging NNSA management structure. They have responsibility for evaluating risks at their sites and for determining when the degree of risk is acceptable. This role encompasses responsibility for performing site surveys and surveillances, approving contractor security plans, and approving work authorization documents. These activities will provide the federal manager with extensive visibility into contractor security programs, budgets, and activities, as well as an understanding of security strengths and vulnerabilities.

# Appendix I
# List of Documents

## General Information

### PANEL CHARTERS

- Security Workforce (Chiles) Project Plan and Site Visit Schedule
- Physical Security (Mies) Project Plan and Site Visit Schedule

### TEAM MEETING NOTES

- Security Workforce Team Meetings
  - September 9, 2003 Chiles Panel Meeting Minutes-at LMI
  - October 7, 2003 Chiles Panel Meeting Minutes-at LMI
  - December 4, 2003 Chiles Panel Meeting Minutes-at LMI
- Physical Security Team Meetings

### BACKGROUND MATERIALS

- NNSA Safeguards and Security Strategic Plan, June 03
- NNSA Security R and D Review, 17 July 2002
- Hamre Implementation Status
- Design Basis Threat Briefing, 9 September 2003
- Personnel Security Division Briefing, 8 September 2003
- Request to Fund the Service Center Personnel Security Support Contract, 19 September 2003
- Issue Paper on Alternatives to the Accelerated Access Authorization Program
- Security Skill Community - Security/CI Professional Health Program Briefing, 11 December 2003
- Chiles Terms of Reference

- White Paper on Safeguards Security Policy Development within the National Nuclear Security Administration (NNSA)
- National Industrial Security Program Report, 2002 (Information Security Oversight Office)
- NNSA Service Center Rapid Interim Clearance Briefing, February 2004
- Inspection of Department of Energy Fresh Pursuit Policies and Practices, June 2002
- Independent Oversight Safeguards and Security Inspection of the Sandia Site Office and the Sandia National Laboratories - New Mexico, 24 October 2003
- Independent Oversight Safeguards and Security Inspection of the Los Alamos Site Office and Los Alamos National Laboratories, Volume I, 29 January 2003
- Independent Oversight Security Inspection of the Office of Transportation Safeguards, 25 October 2002
- Independent Oversight Security Inspection of the Albuquerque Operation Office, 25 October 2002
- Independent Oversight Safeguards and Security Inspection of Amarillo Site Operations and the Pantex Plant, 28 May 2002
- Independent Oversight Safeguards and Security Inspection of the Oakland Operations Office and the Lawrence Livermore National Laboratory, 12 April 2002
- Independent Oversight Inspection of Safeguards and Security at the Y-12 National Security Complex, Volume I, 28 November 2001
- Office of Independent Oversight and Performance Assurance Special Review of Security Measures at TA-18, Los Alamos National Laboratory, 31 October 2000
- Safeguards and Security Follow-up Inspection of Sandia National Laboratories, 18 October 2000
- Independent Safeguards and Security Follow-up Inspection of the Lawrence Livermore National Laboratory, 29 September 2000
- Independent Safeguards and Security Inspection of the Pantex Plant, 17 April 2000

- Independent Safeguards and Security Follow-up Inspection of Los Alamos National Laboratory, 14 January 2000
- Independent Safeguards and Security Follow-up Inspection of the Lawrence Livermore National Laboratory, 14 January 2000
- Independent Safeguards and Security Follow-up Inspection of the Transportation Safeguards Division, 14 January 2000

## GAO REPORTS

### Best Practices

- GAO-03-893G: A Guide for Assessing Strategic Training and Development Efforts, July 03
- GAO/OCG-00-14G: Human Capital - A Self-Assessment Checklist for Agency Leaders, September 00 version 1
- GAO-04-127T: Succession Planning and Management, 1 October 03
- GAO-03-120: Strategic Human Capital Management, Jan 03

### Reviews

- GAO/T-RC-00-123: Nuclear Security- Security Issues at DOE and Its Newly Created National Nuclear Security Administration

## DATA ANALYSIS

- NNSA Experience and Retirement
- Workforce Retirement Eligibility

## DOE DIRECTIVES

- DOE O 360.1-1 B Federal Employee Training
- DOE O 473.2 Protective Force Program
- DOE O 470.1 Safeguards and Security Program Planning
- DOE M 473.2-2 Protective Force Program Manual
- DOE M 473.1-1 Physical Protection Program Manual

NNSA STAFFING POLICES AND PROCEDURES

- NNSA Staffing Principles, Chapter 6
- BOP-003.0303: NNSA Contracting Authorities, 10 January 03
- Functions and Activities by Location, 1 July 03 rev 2
- NNSA Functions, Responsibilities, and Authorities Manual, Change 1, August 03
- LASO Managed Staffing Plan Briefing, 28 May 03
- Kansas City Managed Staffing Plan Briefing, 9 July 03

ORGANIZATIONAL REALIGNMENT

- Realignment Timeline
- Organizational Realignment Package

NNSA ADMINISTRATOR STATEMENTS

- Lintgrams, 21 March 2003 - 3 February 2004
- Final Oral Statement of Ambassador Linton F. Brooks, Acting Under Secretary for Nuclear Security and Administrator NNSA/DOE before the Subcommittee on Energy and Water Development, Committee on Appropriations, U.S. House of Representatives, 19 March 2003
- Statement of Linton F. Brooks, Acting Under Secretary of Energy and Administrator for National Security, NNSA/DOE before the Subcommittee on Strategic Forces, Committee on Armed Services, 8 April 2003
- Statement of Linton F. Brooks, Acting Under Secretary of Energy and Administrator for National Security NNSA/DOE, before the Subcommittee on Energy and Water Development Committee on Appropriations, U.S. Senate, 10 April 2003
- Oral Statement of Ambassador Linton F. Brooks, Under Secretary for NNSA/DOE, before the Subcommittee on National Security, Emerging Threats and International Relations, Committee on Government Reform U.S. House of Representatives, 24 June 2003
- Testimony of Linton F. Brooks, Under Secretary for Nuclear Security and Administrator for NNSA, Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International

Relations—Hearing on Emerging Threats: Assessing Nuclear Weapons Complex Facility Security, 24 June 2003

## Foushee Group Inc: Security Compensation Survey Report, 2003

## NNSA: Safeguards & Security Workforce Analysis and Report, January 2003 (updated workforce data collected in January 2004)

## NNSA: Functions, Responsibilities, and Authorities Manual, May 03

## NNSA Service Center: Staffing, Retention, & Training of Security Professionals, 21 October 03

## DOE Nonproliferation and National Security Institute Information Binder

- PDP Project Management Plan
- President's Management Agenda
- DOE Strategic Plan
- DOE Strategic Security Plan
- DNSFB 93-3
- Lintgram
- Workforce Analysis and Planning
- Safeguards and Security TQP
- Professional Enhancement Program

## Y-12 Site Visit for Security Workforce Team

- Strategic Plan for Y-12 National Security Complex, July 2003
- Y-12 Safeguards and Security Briefing
- Answers to Questions posed by the Chiles Team
- Y-12 Site Office Organization Chart
- Functional Skill Requirements

- YSO Roles and Responsibilities by Position
- Management System Description
- Pro-Force Personnel Counts
- Y-12 Site Office Workforce Analysis and Staffing Plan Report, July 03
- Y-12 Safeguards & Security FY03 Goals and Objectives
- Y-12 Site Safeguards & Security Plan
- Y-12 Incidents of Security Concern
- Assessment Reporting and Deficiency Processing, 22 July 02
- Performance Analysis Matrix, 5 August 03
- Cyber Security Organization Chart & Personnel Roster

## Los Alamos National Laboratory Site Visit for Security Workforce Team (3 binders)

PROTECTION TECHNOLOGY LANL BINDER - OCT. 20, 2003

LANL MANAGEMENT BIOGRAPHIES BINDER, 20 OCTOBER 03

SITE VISIT BINDER

- Los Alamos National Lab Strategic Goals, 17 October 03 (blue folder)
- Site Visit Agenda and Attendee List
- Site Visit Notes
- Protective Force Management Overview, 20 October 03
- LANL Workforce Review Briefing, Erickson, 20 October 03
- LANL Safeguards & Security Briefing, Gibbs, 20 October 03
- 2003 Overview of LANL by University of California and LANL
- DOE IG 0471: Summary Report on Inspection of allegations relating to the Albuquerque Operations Office Security Survey Process & the Security Operations' Self Assessments at Los Alamos Laboratory, May 00

## Sandia National Laboratory Site Visit for Security Workforce Team

- Site Visit Notes
- Site Visit Agenda
- Safeguards and Security Briefing, Miyoshi, 29 October 2003
- Site Office Briefing, Loftis, 29 October 2003
- Sandia Safeguards and Security Organizational Chart
- Sandia Training Approach Briefing
- Fiscal Year 2004 Performance Evaluation Plan

## Lawrence Livermore National Laboratory Site Visit for Security Workforce Team

### SITE VISIT BINDER

- Site Visit Agenda
- Site Visit Notes
- Livermore Site Office Briefing, Connolly, 14 November 03
- Livermore Laboratory Organization Charts
- Recruiting and Retention Programs

### LLNL ADDITIONAL INFORMATION BINDER

- Memorandum on Relocation of Personnel Security
- Integrated Safety and Safeguards & Security Management Plan (ISSSMP)
- Livermore Site Office Site-Wide Security Plan, May 2003
- Memorandum on Approval of Managed Staffing Plan
- Assessment Management Plan
- Safeguards & Security Division, Daily Oversight Activities, June 2003

- Livermore Site Office Business Management Division, Major Activites
- Safeguards & Security Personnel Experience

## Pantex Site Visit for Security Workforce Team

- Site Visit Notes
- Pantex Site Office Briefing
- Site Office Safeguards and Security Core Competencies
- Pantex Site Office *ADAPT* Qualification Standard for Information Security
- Pantex Site Office Qualification Card for Information Security
- Pantex Site Office *ADAPT* Qualification Standard for Material Control & Accountability
- Pantex Site Office Qualification Card for Material Control & Accountability

## Commission on Maintaining US Nuclear Weapons Expertise - Report to Congress & the Secretary of Energy, 1 March 99

## CSIS Panel Rpt: Science & Security in the 21st Century - Report to the Secretary of Energy on DOE Labs, April 02

# Appendix J
# Abbreviations

| | |
|---|---|
| AAAP | Accelerated Access Authorization Program |
| ACES | Automatic Continuing Evaluation Study |
| DoD | Department of Defense |
| DOE | Department of Energy |
| FRAM | Functions, Responsibilities, and Authorities Manual |
| GAO | General Accounting Office |
| ISA | iterative site analysis |
| IT | information technology |
| MC&A | materials control and accountability |
| NNSA | National Nuclear Security Administration |
| NNSI | Nonproliferation and National Security Institute |
| OPM | Office of Personnel Management |
| S&S | safeguards and security |
| SSSP | site safeguard and security plan |