

**UNCLASSIFIED TESTIMONY
GLENN S. PODONSKY
DIRECTOR
OFFICE OF INDEPENDENT OVERSIGHT AND PERFORMANCE ASSURANCE
U.S. DEPARTMENT OF ENERGY
BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND
INTERNATIONAL RELATIONS
COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES**

June 24, 2003

Introductory Remarks

Thank you, Mr. Chairman, for inviting me to testify today. My office – the Office of Independent Oversight and Performance Assurance – is responsible for evaluating the Department’s environment, safety, and health; emergency management; cyber security; and safeguards and security programs. We report directly to the Secretary of Energy and have no responsibilities for managing DOE sites or for developing policy. As a result, we are able to perform independent assessments of the effectiveness of programs and provide unbiased information to the Secretary and DOE line managers.

In the area of security programs at nuclear weapons complex facilities, we perform regular inspections of all DOE sites that have special nuclear materials and classified information related to the nuclear weapons programs, including all NNSA sites. We inspect the sites against DOE requirements, including the DOE design basis threat policy. However, we also examine the effectiveness of DOE policy in providing protection for our national assets and from time to time identify opportunities to improve DOE security policies.

The focus of my testimony today will be on the current status of security programs at the nuclear weapons production facilities and the national laboratories that design nuclear weapons. However, a brief review of the evolution of the security program is necessary to place the proper context on current security programs. DOE first established an Independent Oversight program twenty years ago. At that time, DOE security systems were in very bad shape. Some nuclear facilities did not even have functional intrusion alarm systems. Protective forces were understaffed, poorly trained, poorly conditioned, and poorly managed. DOE sites were not able to defeat the threat in many cases, as evidenced by numerous performance tests conducted by Independent Oversight and other groups. Recognizing the inadequate levels of security, during the late 1980s, DOE invested close to a billion dollars in improved physical security systems and protective force training. These investments resulted in dramatic improvements in security. However, at several sites, the alarm systems installed 15 years ago are at or near the end of their expected life, and now require extensive maintenance and/or replacement.

During the mid-1990s, budgets for security were reduced significantly at most DOE sites from the high levels required to improve our security posture to a steady-state level, and as part of a widespread effort to more efficiently manage overhead costs. These reductions were a result of

the end of the Cold War and an increased focus on environment, safety and health programs. The impact of these changes caused significant reductions in protective forces and decisions not to upgrade or replace security hardware. In most cases, sites compensated for the smaller number of protective force personnel by consolidating nuclear materials into fewer areas and other means, such as more use of electronic access control systems to replace guards. In the 1998 timeframe, Independent Oversight reviews and other external assessments revealed that the security reductions at a number of sites had gone too far—the protection effectiveness was not where it needed to be. However, we are not implying that sites had reached the poor levels of security that were evident in the early 1980s. However, the cost cutting measures went too far and the protection effectiveness was not where it needed to be. At DOE's direction, sites began to rebuild their protection programs including additional personnel, better equipment, and increased training. However, the ramifications of the reductions in the security budgets took several years to overcome, considering the time needed to obtain budget approval for new protective personnel, obtain security clearances, get personnel trained, and test and fine tune response plans.

Another important trend that has impacted security is the proliferation of computers, electronic data files, and the Internet. DOE experienced a number of security lapses in the late 1990s involving classified or sensitive information, such as the well-publicized loss of the hard drive at the Los Alamos National Laboratory. Many of these security lapses were partially attributable to the fact that DOE policies and practices in the cyber security arena did not always keep pace with changing technology. Independent Oversight has made cyber security a major focus area for over five years now, and DOE took a number of important steps to enhance policies and practices in the protection of information.

The tragic events of September 11, 2001 happened at a time when DOE was still rebuilding its protection programs. DOE, like everyone else, took 9-11 as a wake up call. Since then, DOE has increased security through a number of measures, and has additionally reassessed the design basis threat. However, these represent only the immediate first steps in enhancing DOE security. Historically, roles and responsibilities for security have been unclear in some areas and too fragmented for effective operation in others. Secretary Abraham personally directed that the DOE design basis threat be strengthened. The design basis threat, which was issued May 20th, provides the basis for establishing and assessing protection effectiveness at DOE sites. Secretary Abraham and Ambassador Brooks are addressing the overall management structure for security, but much remains to be done before DOE has a coherent management structure in place to support an effective corporate approach to security.

Independent Oversight Approach and Recent Actions

Our assessment of the current status is based on the inspections that we have performed in the past two years. Since 9-11, Independent Oversight has conducted reviews at all major NNSA production sites and weapons laboratories with the exception of Sandia National Laboratories and the Nevada Test Site. We are currently performing a limited scope review at Sandia National Laboratories and will conduct a comprehensive inspection this fall. We plan to inspect the Nevada Test Site in the near future, after we complete a DOE-wide review of protective forces, which was directed by Secretary Abraham. During that time, we have also conducted

inspections of four other non-NNSA sites that have significant quantities of nuclear material and classified information.

Our inspection process has always included assessments of the effectiveness of physical security, including alarm systems, protective forces, training and equipment, and information security including protection of documents and electronic data. We also look at protection program planning, including the site vulnerability assessments, to include the effectiveness of contractor and line management feedback and improvement programs to include the contractor self-assessments and the DOE field element survey programs.

Unlike most inspection programs, Independent Oversight has always made extensive use of performance tests in all areas that we assess. These tests range from relatively straightforward tests of the calibration of security systems, such as intrusion alarms and metal detectors, to large and complex tests of the integrated effectiveness of security systems using engagement simulation systems, more commonly known as MILES gear. We do extensive testing of cyber security systems using the same techniques that hackers use. We have demonstrated our capabilities to Congressional committee members on past occasions and have established a cyber security laboratory that allows us to continually develop and modify our techniques to keep pace with changing technologies and ever-evolving hacker methods.

Although we have been conducting large-scale force-on-force performance tests using the DOE Composite Adversary Team for over 15 years, the 9-11 events prompted us to redouble our efforts in this important area. Since 9-11, we have substantially increased the number of tests we perform. We have also increased the skills and the amount of specialized training of our Composite Adversary Team to include terrorist tactics and advanced training used by the U.S. Special Forces and foreign special operations units. We have also increased our organizational capability to perform effective tests by obtaining specialized expertise from nationally recognized experts in tactical operations and counter terrorism.

OA has also supported the development of the revised design basis threat. Other DOE organizations have responsibility for the revised design basis threat and will discuss its status. Independent Oversight is now considering how it will perform performance testing under the new design basis threat.

Current Status of Security at the Department of Energy

Based on our inspections and performance tests, I will now provide a brief overview of the status of security programs across the DOE nuclear weapons complex.

Starting out with some generally positive aspects:

- As a result of the increased security measures put in place following the attacks of September 11, 2001, DOE sites have significantly increased the level of security. They have increased the number of protective force members on duty at any given time and have further limited routine access to key areas of the sites. To accommodate the increased workload, many sites have hired and continue to hire additional personnel for their protective forces. They have also added additional barriers and hardened fighting positions.

- The classified cyber security program is maturing. After experiencing a number of problems with complex issues of protecting classified information on computer networks, DOE's performance has been steadily improving in this area for the past several years. Our inspections have found only minor issues within this program in recent inspections. However, we have seen examples of backsliding and complacency, and will continue to focus on this important area.
- Our inspections have also indicated that the protection afforded classified documents is generally consistent with national policies. Protection of classified non-nuclear parts, such as the electronic components of nuclear weapons, has greatly improved but still needs continued attention to ensure that interim measures are replaced with permanent solutions. In addition, DOE has established some more stringent requirements for certain higher priority assets (such as electronic media with particularly sensitive information) in recent years. Our inspections indicate these new requirements are an improvement but implementation is not yet uniformly effective.

Notwithstanding these positive aspects, significant work remains and our inspections have identified a number of weaknesses that need additional attention:

- The recent hiring of additional protective force personnel and the heightened security levels has created an interim set of problems. New protective force members have received mandatory training and testing (e.g., physical fitness and firearms) but the security clearance process has significantly delayed the deployment of these newly hired protective force members. Some sites have also had to defer critical performance tests because manpower is stretched to the limit.
- DOE sites have primarily responded to the need to enhance security post 9-11 by using manpower intensive measures. While appropriate as an interim solution, additional attention is needed to establish and implement more effective solutions by enhancing the integration of manpower and technology, more effective barriers, further consolidation of security assets, and extensive performance testing to ensure system effectiveness.
- Unclassified cyber security continues to be a challenge for some sites. While most sites have robust protection of their unclassified networks against both external and internal attack, some sites have not adequately addressed certain threats such as the potential for an authorized user to elevate his access privileges to gain access to potentially sensitive information on the network. We have noted recurring deficiencies with the adequacy of controls for foreign nationals on DOE computer systems; there are instances where sites did not have sufficient controls to ensure that the ability of foreign nationals to access information was thoroughly reviewed and controlled. In addition, some sites have not fully recognized and addressed the inherent risks associated with the recent proliferation of wireless technology in computer systems.
- The recent NNSA reorganization has the potential to streamline and clarify security responsibilities, and we have noted some recent improvements in this area. However, the new site offices do not yet have the staffing and expertise to be able to effectively discharge their responsibilities in the security oversight arena.

- Weaknesses in feedback and improvement processes are a long-standing concern, both within the DOE line and contractor organizations. Effective contractor self-assessments are a foundation to the ongoing effectiveness of security programs. OA inspections indicate that some aspects of contractor self-assessments are improving but there are often weaknesses in corrective action management processes, including insufficient root cause analysis. As a result, deficiencies recur. Similarly, on the DOE line management side, the reviews are not always sufficiently rigorous and do not include sufficient performance testing in some areas. The near-term staffing and expertise issues associated with the NNSA reorganization exacerbate these weaknesses.
- Protection strategies and effectiveness will need to be reevaluated when the revised design basis threat is fully implemented. DOE sites' vulnerability assessments have largely been conducted using the previous design basis threat or been deferred until a new design basis threat was prepared. Similarly, the force on force performance testing conducted by Independent Oversight has been conducted using the old threat in most cases. While it is clear that every site has increased its level of protection in response to the September 11, 2001, attacks, few of these enhanced protection schemes have been fully performance tested or subjected to quantitative vulnerability analysis to assess their effectiveness under the current concept of the threat, because the new threat policy had not been published. Therefore, the determination of whether the current programs are sufficient has largely been deferred until the new design basis threat was published.

The weaknesses in feedback and improvement and clarity of security roles and responsibilities are longstanding and have been identified on many past inspections. Progress in these areas, however, has been inconsistent and sporadic. We believe that well defined responsibilities and effective feedback programs are the lynchpin to effective security programs.

The Secretary, Deputy Secretary, and the NNSA Administrator are placing significant emphasis on reorganizing the management structure to clarify responsibilities and increase accountability. They have demonstrated personal involvement in enhancing security after 9-11 and in response to recent security lapses. For example, the Administrator for the NNSA personally requested that we perform an accelerated review at Sandia to address concerns with protective force operations. The current efforts are promising but significant continued attention and evaluation is imperative to ensure that they are sustained and the intended improvements are realized at the field level.

Closing Remarks

In closing, much has been accomplished but much more work remains to be done. This is especially true considering the more stringent design basis threat and to ensure that longstanding weaknesses in role and responsibilities and feedback programs are fully addressed. The recent strong and aggressive senior management focus on security will result in program improvements, but this effort will need to be sustained to address the challenges DOE faces.