

Summary of Testimony of Glenn S. Podonsky
Director, Office of Security and Safety Performance Assurance
U.S. Department of Energy
Before the
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives
June 9, 2006

Background

- The Office of Independent Oversight, within the Office of Security and Safety Performance Assurance (SSA), is responsible for conducting independent evaluations of the effectiveness of cyber security policies, programs, and performance throughout the Department of Energy.
- The SSA oversight program evaluates the full range of DOE information systems, including unclassified, classified, and intelligence systems.
- Independent Oversight inspections evaluate both the management and technical aspects of cyber security, with a heavy emphasis on penetration testing. Penetration testing is conducted both internally and from outside DOE networks as part of announced and unannounced inspections.

Current Status of Department of Energy Cyber Security Programs

- Results of our independent oversight activities leading up to and including last fall's red team assessments have identified fundamental weaknesses in both the management processes and operational controls employed to protect the Department's unclassified information systems.
- While some DOE organizations have effective security controls, our overall assessment is that the Department's unclassified information assets have been operating at an elevated level of risk for compromise and disruption given today's threat environment.
- In contrast to the unclassified program, our inspections indicate that the information security program for national security systems is providing an adequate level of protection. A malicious insider represents the greatest threat to DOE's classified information.
- Since last fall, SSA has been working in partnership with the Chief Information Officer and Under Secretaries in an aggressive effort to improve cyber security within DOE. The cyber security revitalization plan is the logical next step in the process of institutionalizing a robust management and operational framework across DOE using the recommendations in the *Cyber Security Project Team Summary Report and Plan of Action*.
- The focus on cyber security by senior Departmental leaders and sharing of lessons learned from red team assessments has clearly raised awareness throughout DOE of the importance of cyber security, possible threat vectors, and increased expectations for performance.
- Numerous security controls have been added or upgraded at DOE Headquarters, the NNSA Service Center, and the National Training Center to strengthen the protection of their respective networks.
- Sites are continuing to evaluate the *Summary Report and Plan of Action* recommendations relative to their information processing mission requirements, threat environment, and competing priorities.

Conclusion

- The Department has made substantive progress in improving cyber security in the past six months. Progress is evident at both the program management and technical implementation levels.
- SSA is guardedly optimistic that the revitalization effort will be effective in fully addressing long-standing weaknesses in the Department's cyber security management processes, but success will require consistent and sustained effort at all management levels.
- SSA will continue to evaluate and report on progress in improving technical security controls through an aggressive cyber security penetration testing program.

Testimony of Glenn S. Podonsky
Director, Office of Security and Safety Performance Assurance
U.S. Department of Energy
Before the
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives
June 9, 2006

Mr. Chairman and members of the Subcommittee, thank you for inviting me to testify regarding the status of the Department of Energy's cyber security programs and ongoing efforts to revitalize those programs throughout the Department. Both the Secretary and Deputy Secretary recognize the importance of cyber security and have demonstrated exceptionally strong leadership in making cyber security one of the Department's highest priorities. The Department's new Chief Information Officer is leading this revitalization effort which we are guardedly optimistic will result in implementation of needed improvements across the Department's programs and sites.

The Department of Energy (DOE) relies upon an extensive array of information technology and computer resources to accomplish its national security, energy, science, and environmental management missions that range from the desktop computers used by Federal and contractor staff to some of the world's most sophisticated and complex supercomputers. It is of paramount importance that we protect the confidentiality, integrity, and availability of these resources utilizing sound risk management approaches given their critical role in enabling the Department to accomplish its vital missions. The threats to our information systems have never been greater and continue to grow in sophistication and intensity every day. Like all Federal agencies, the Department of Energy faces a constant challenge to identify, evaluate, and apply cyber security measures that will mitigate these threats and establish an appropriate protection posture for our information and information systems in this ever-changing cyber threat environment. Before I discuss the status of the Department's cyber security programs, I would like to provide an

overview of the Office of Security and Safety Performance Assurance's responsibilities, with a particular focus on our activities related to cyber security.

Overview of SSA Activities

As a direct report to the Office of the Secretary, the Office of Security and Safety Performance Assurance (SSA) is responsible for several major functions within the Department. These functions can be divided into two very distinct categories - the independent oversight of security and safety program implementation and responsibility for a wide spectrum of security-related functions including policy, training, security technology deployment, field assistance, classification and declassification, and nuclear material control and accountability. In the area of cyber security, our role is to serve as the independent oversight for the entire Department of Energy. Our Office of Independent Oversight conducts performance-based evaluations of safeguards and security, cyber security, emergency management, and environment, safety and health program implementation throughout the Department. Within this office, the Office of Cyber Security Evaluations executes one of the most aggressive and sophisticated cyber security corporate oversight programs in the Federal government that allows the Department to proactively self-identify and address weaknesses. The cornerstone of our cyber security oversight is a rigorous penetration testing program that is implemented in a variety of ways to achieve multiple objectives. These include:

- announced external and internal penetration testing of Departmental networks conducted in conjunction with announced cyber security inspections that evaluates a broad set of threats and is designed to assess protection boundaries, physical and logical security configurations and controls, access authorizations, and activity monitoring practices;
- unannounced remote penetration testing or "red teaming", which emulates a stealthy, methodical, and sophisticated external attacker attacking weak links in the network and is designed primarily to test intrusion detection and incident response capabilities; and
- Continuous scanning of all Department of Energy internet protocol addresses to identify vulnerabilities to internet-based threats on an ongoing basis.

In conjunction with our penetration testing activities, the Office of Cyber Security Evaluations conducts assessments of key management processes that are essential to an effective cyber

security program such as risk management, certification and accreditation, configuration management, and patch management. While our technical testing provides a good snapshot of the effectiveness of the network's cyber security protection posture, the programmatic evaluation allows an assessment of the direction and sustainability of the cyber security program along with identification of underlying root causes for implementation weaknesses identified through technical testing. The Office of Cyber Security Evaluations applies this same basic approach to assessments of unclassified, classified, and intelligence systems operated by the Department. Other cyber security performance testing conducted by our office includes evaluating the protection posture of telephone modems and identifying vulnerable wireless access points that could potentially provide an unprotected alternate pathway into one of our networks. Pursuant to the Federal Information Security Management Act (FISMA), the Office of Security and Safety Performance Assurance has been designated by the Secretary of Energy to conduct the annual assessment of the Department's information security program for national security systems. The Office of the Inspector General is responsible for conducting the annual evaluation of the Department's information security program for unclassified systems; however, Independent Oversight provides significant input in the form of our inspection results. We have an excellent working relationship with the Office of the Inspector General and coordinate extensively to eliminate any duplication of effort.

Current Status of Department of Energy Cyber Security Programs

Results of our independent oversight activities leading up to and including our recent red team assessments this past fall have identified fundamental weaknesses in both the management processes and operational controls employed to protect the confidentiality, integrity, and availability of the Department's unclassified information and information systems. While the perimeters of our sensitive unclassified networks are relatively well controlled and monitored, internal Departmental networks were found in many cases to have unpatched and/or unrecognized vulnerabilities, lack of segmentation or barriers, common local administrator passwords, poorly controlled inter-connections with other networks, and insufficient intrusion detection mechanisms. As demonstrated in the recent red team assessments, a malicious insider or sophisticated adversary that has managed to penetrate the network could take advantage of

these types of weaknesses to gain broad access and control over information technology resources. As a result, our overall assessment is that the Department's unclassified information assets have been operating at an elevated level of risk for compromise and disruption given today's threat environment.

At the most basic level, the Department's unclassified information systems suffer from a lack of defense in depth. It is no longer acceptable or prudent to rely on a single layer of protection at the perimeter of a network to ensure that the information contained therein or functions performed are protected from unauthorized access, disruption, or manipulation. Further, the technical implementation weaknesses we have observed are symptoms of inadequate management processes that are essential to an effective cyber security program such as configuration management, patch management, asset management, risk management, and vulnerability scanning. We have routinely identified weak certification and accreditation processes as an underlying root cause of many of the problems identified above.

The effectiveness of the Department's unclassified cyber security programs has been highly dependent on the knowledge and initiative of key network personnel utilizing "expert-based" approaches. This, in some cases, led to a lack of rigorous and repeatable processes that are necessary to form a solid program foundation. In addition, line managers have not been sufficiently involved to ensure the adequacy of controls and managing risk. As a result, the effectiveness of unclassified cyber security programs has been highly variable across DOE organizations. Of concern, Departmental cyber security management processes have been insufficient in the past to drive needed improvements throughout the Department.

Oversight activities have found that some DOE organizations have developed mature cyber security programs for their unclassified computers that include well constructed defense in depth security controls. It is clear that the sharing of lessons learned from the Red Team as well as the high level of focus on cyber security by senior Departmental leaders has clearly raised the awareness within the DOE cyber security community of increased expectations and threats. We have seen some initial progress in addressing identified cyber security concerns. For example, at DOE Headquarters, common local administrator passwords for system administrators have been

eliminated and access control converted to two factor authentication. Virtual local area networks have been deployed on the Headquarters network to provide a greater degree of network segmentation. Host-based intrusion detection has also been added to the Headquarters network as part of adding additional defense in depth. Additionally, the Department's Chief Information Officer is leading the recovery effort to respond to the security weaknesses at DOE Headquarters and the National Nuclear Security Administration (NNSA) Service Center. Additional plans have been developed to more fully evaluate and mitigate cyber security risks at DOE Headquarters through a broad modernization effort. While Independent Oversight has not yet assessed and validated the effectiveness of these new measures on the DOE Headquarters network through penetration testing, we believe that these represent positive steps.

In contrast to the unclassified program, our independent oversight activities indicate that the information security program for national security systems is providing an adequate level of protection. Established security controls have been found to be generally consistent with DOE's longstanding requirements for these systems. During Independent Oversight inspections over the past year, improvements were noted in a number of areas related to both technical security performance and site management practices. However, the Department faces continuing challenges in resolving longstanding weaknesses in policies governing the management of national security systems, continuing programmatic deficiencies, and adherence to some FISMA requirements. As a result, malicious insiders continue to present the largest threat to DOE's classified information.

Cyber Security Assistance Activities

In response to independent oversight findings, the results of other external evaluations, and especially recent penetration testing performance, the Deputy Secretary directed us to step out of our normal oversight role in order to lead an effort to develop a comprehensive plan of action to remedy existing management, operational, and technical weaknesses in the DOE unclassified cyber security program. To execute the Deputy Secretary's directive, the Office of Security and Safety Performance Assurance, together with the Office of the Chief Information Officer, led a team of Departmental cyber security professionals which developed a plan of action to remedy

long-standing weaknesses in the unclassified cyber security program. The recommendations issued by the team in the *Cyber Security Project Team Summary Report and Plan of Action* represent the consensus of senior representatives from the Office of the Chief Information Officer; National Nuclear Security Administration; Under Secretary for Energy, Science, and Environment (ESE); SSA; and others on a path forward for improving cyber security throughout the Department. Normally, it would have been preferable for the Department to focus first on establishing a robust management structure and governance process that would subsequently drive improvement in operations and security at the system administrator and computer user levels. However, the team felt it was important for sites to begin improving their protection posture immediately through prudent measures and give the management processes a chance to catch up before ultimately driving improvements through risk based decision-making. As a result, a set of programmatic and technical recommendations for improving cyber security throughout the Department were provided. It should be recognized that these recommendations are not mandatory but were offered as suggestions for each DOE program and site to assess for applicability and to make determinations based on cost, benefit, and feasibility of implementation.

As part of another initiative to help improve the Department's cyber security protection posture, the Office of Cyber Security Evaluations is partnering with the Office of Science in conducting site assistance visits at all Office of Science field sites to help them identify vulnerabilities and implement improved security controls and processes. Since last summer, ten site assistance visits have been completed; five more are scheduled to be completed this year. Other site assistance visits have been conducted or are planned with the Office of Environmental Management, the Office of Energy Efficiency and Renewable Energy, and the Power Marketing Administrations. We have also worked closely with the Office of the Chief Information Officer, the National Nuclear Security Administration's Service Center, and the Department's National Training Center to significantly strengthen their cyber security defenses by implementing more robust security controls following red team assessments conducted on their networks. We have shared the results of our red team assessments extensively through a variety of communications forums.

Revitalization Efforts

Recently, the Department has taken many important initial steps to upgrade its cyber security protection posture. For example, our new Chief Information Officer has proactively developed a cyber security revitalization plan that encompasses many of the recommendations from the *Cyber Security Project Team Summary Report and Plan of Action*. The revitalization plan is an appropriate next step in the difficult process to define a cyber security management and operational framework that can be institutionalized yet responsive to the dynamic world of cyber threats and counteracting security measures. The line managers who are responsible for implementing the technical controls necessary to reduce risk are taking immediate actions where feasible, but also must carefully evaluate and balance the need for any additional controls with their site-specific information processing mission requirements, threat environment, and resource limitations.

The Office of Security and Safety Performance Assurance continues to monitor progress in improving the Department's cyber security programs on a daily basis. We actively participate in and routinely provide feedback to the Office of the Chief Information Officer and other line managers through the Department's Cyber Security Executive Steering Committee and Cyber Security Working Group. We continue to conduct critical reviews of proposed changes in Departmental cyber security policies and guidance with an eye toward the likelihood that those policies will result in the desired level of protection when applied to the wide spectrum of information management and processing needs. We are reviewing site-specific progress in evaluating and implementing the recommendations of the cyber security project team and providing feedback to cognizant line managers in this regard as an integral part of our independent oversight inspections. The most important measure of progress, however, will be the degree to which the Department's information and information systems can prevent an intrusion or can rapidly detect and respond to an intrusion such that the damage to a system can be readily recognized, contained, and mitigated. A realistic evaluation of these capabilities can only truly be gained from the types of performance testing that are conducted as part of our independent oversight. To that end, we are continually developing new penetration testing tools

and attack techniques to keep pace with advances in technology and new approaches to exploiting human behavior.

Conclusion

The Department is making progress in improving its cyber security programs. The Office of the Chief Information Officer and program offices have laid the necessary groundwork upon which to build a robust and responsive program that assures that our information and information systems are adequately protected. We have already seen improvements in this area under the new Chief Information Officer's leadership and continue to be cautiously optimistic that historic, systemic problems with Departmental cyber security management processes will be addressed. Individual sites and both Under Secretarys for ESE and NNSA are working to reevaluate the need for improved security measures based on their mission requirements and accepted risk management principles. Our office will continue to implement an aggressive schedule of internal and external penetration and performance testing and use the results of those tests to aid the Office of the Chief Information Officer, program offices, and site managers in maintaining a protection posture that proactively manages and anticipates new and emerging threats and the use of new technologies by our adversaries. Thank you. This concludes my testimony.