

STATEMENT OF

GLENN S. PODONSKY

DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSURANCE

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,  
AND INTERNATIONAL RELATIONS

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

JUNE 22, 2004

Statement of Glenn S. Podonsky  
Director, Office of Security and Safety 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 22, 2004

**Introductory Remarks**

Mr. Chairman and honorable members of the subcommittee, I want to thank you for again inviting me to testify regarding safeguards and security programs in the Department of Energy. In previous testimony before this subcommittee on April 27<sup>th</sup> of this year, we presented detailed information regarding our process for developing and implementing the Department's Design Basis Threat; responded to the specific issues raised by the General Accounting Office in its draft report: *Nuclear Security: DOE Needs To Resolve Significant Issues Before It Fully Meets the New Design Basis Threat*; and described the role of my office, the Office of Security and Safety Performance Assurance, in the implementation of the Design Basis Threat and in other key efforts to improve security performance in the Department.

The information presented at the April 27<sup>th</sup> hearing remains valid, and therefore we offer no substantial amendments to that information today. However, significant activity having potentially far-reaching effects on the Department's protection programs has occurred in the two months that have elapsed since that previous testimony. Specifically, on May 7<sup>th</sup> Secretary Abraham delivered a major speech outlining his vision for the future of the Department's protection programs, and at the same time he announced a number of initiatives aimed at

implementing that vision. The Secretary's newly announced security initiatives will impact most major elements of our protection programs both in the Department at large and in the National Nuclear Security Administration, and it is those initiatives that we would like to address today.

### **The Secretary's Security Initiatives**

Since assuming responsibility for the Department's management over three years ago, our senior managers have demonstrated a keen interest and close involvement in DOE's protection programs – and have not been shy about promoting actions to strengthen the programs and eliminate program weaknesses. Their personal interest and involvement has resulted in a number of actions that addressed a number of security concerns facing the Department. Understandably, senior management interest and involvement in security matters became even more focused after the terrorist attacks of 9/11. Since then, our understanding of the natures of the various threats we face has evolved, our protection program requirements have been adjusted to deal with the increased threats, we have changed some of our organizational relationships to improve security-related communication and cooperation between Headquarters and field elements, and our sites have taken the initiative to implement many local security measures to counter the increased threat. Our experiences in dealing with elevated threats and enhanced security postures since 9/11, and particularly our experiences with the immediate and long-term effects of manpower-intensive security enhancements, have led us to conclude that there are a number of additional steps we can and should take to increase the efficiency, effectiveness, and sustainability of our protection programs; hence, the Secretary's 14 new security initiatives. The complete set of new initiatives, as announced by Secretary Abraham, can be grouped into four broad program areas:

information security; new security technology solutions; consolidation of materials; and strengthening security human capital expertise. Together, they directly or indirectly impact every aspect of our protection programs.

### Information Security

Much of what we do today is inextricably tied, in one way or another, to computers. A great deal of the information we possess, including classified information, is created on computers and/or stored on computer media. Most of our unclassified networks interface with the Internet. The fast pace of technological development of computer hardware and software seems to be equaled by the pace of development of methods to exploit that hardware and software for nefarious purposes. Cyber attacks, from large-scale information warfare campaigns to individual hacker vandalism, have become constant. The Department has been the target of cyber attacks in the past, and we will be targeted in the future. In fact, there is no doubt that many of our DOE computers and networks are under some level of cyber attack at this very moment. If we are to continue to operate effectively in the twenty-first century, we have to actively protect the confidentiality, integrity, and availability of all of the information on our automated systems, and we have to be able to do that even while we are under cyber attack. Consequently, we have to be on the cutting edge of cyber security. We need to employ tools, systems, procedures, and configurations that will provide the maximum degree of reliability and protection for our computer systems. Recognizing the urgency of this imperative and the potential consequences of falling behind in this area, the Secretary has resolved that even though the Department has made significant progress in cyber security programs in the past few years, we need to do more to

ensure that our protection systems keep abreast of emerging threats. Therefore, three of the new security initiatives focus on cyber security. These initiatives are specifically aimed at reducing the exposure of classified information stored on computer media; enhancing various individual aspects of our cyber security programs; and increasing the scope and volume of self-testing programs we use to identify (and eliminate) our own cyber vulnerabilities before an adversary does. While these initiatives include some longer-term developmental activities, many can be implemented in the near term, and some are already being implemented. The cumulative effects of these initiatives will significantly enhance our cyber protection abilities.

#### New Security Technology Solutions

In previous testimony before this subcommittee we stated that the DOE could and should make better use of security technologies to enhance our protection systems, and that evaluating new technologies and making them rapidly available to the field was one of my office's main focal areas. Properly applied, appropriate technologies can act as force multipliers to assist our protective forces by reducing the burden of routine activities, reducing the risk to them in case of an attack, and, through enhanced recognition combined with additional barrier delays, provide additional response time to meet and defeat an attack. Two of the Secretary's security initiatives are aimed specifically at enhancing our protection programs through increased use of technology.

One is directly responsive to several recent security incidents – specifically, replacing mechanical lock and key systems in security areas with modern, keyless entry control systems.

There have been relatively few actual incidents, but a recently concluded review by my Office of Independent Oversight and Performance Assurance clearly indicated the need for action to enhance the present level of control and accountability afforded keys and locks in the near term and the urgent need to move forward to implement the Secretary's initiative. Although simply replacing one type of lock with another may seem narrowly focused and easily achievable with current technology, this initiative is, in fact, a massive undertaking for an organization like DOE with the number of locks and keys currently in use at our security areas. The decision to move forward on this initiative represents a significant commitment on the part of the Secretary and the Department.

The other security technology initiative is a much broader and, in some ways, even more ambitious effort aimed at identifying, evaluating, or developing useful technologies and facilitating their timely implementation at appropriate DOE sites. We are particularly interested in evaluating and deploying emerging technologies that can help our protective forces better ascertain and thwart the ever-changing threats to our national security assets. We are examining emerging technologies being developed by the scientific community to determine if they have security utility, and if their benefits can be harnessed and applied within DOE. Examples of efforts currently underway include the development of an active denial system that will flood an area with microwave energy making it impossible for adversaries to carry out their objectives. Unlike a similar long range "battlefield" system being developed by the military, our effort focuses on a much shorter range version that can be deployed on the inside of facilities to provide a formidable barrier where special nuclear materials exist.

We are also investing in remotely controlled weapons that can be pre-positioned within secure areas, and activated by personnel located in hardened shelters where they are less susceptible to direct fire. One example of such a remotely controlled weapon is the TRAP system that we have identified for near-term deployment at several DOE sites. Test systems equipped with laser engagement systems have been tested in DOE facilities and have been found to be very effective. We have conducted a number of computer simulations of various deployment strategies for this system and these simulations have indicated that the TRAP system can be a substantial contributor. We are proceeding toward final deployment of this system as quickly as possible.

We are also investigating new sensor technologies to allow us to identify and engage adversaries farther from their target. We are investigating an acoustic device to assist us in conducting rapid, but thorough, searches of vehicles entering DOE sites. We are also working closely with the Department of Defense to bring some very promising beyond-the-fence early warning sensors into DOE. These sensors will help us scan areas outside of our perimeters to detect an attack long before the adversary can reach our most critical areas. The result will be an ability to identify and engage the adversary much earlier, giving us more time to bring the right weaponry and personnel to the fight.

In this area of technology application as well as in cyber security, we intend to stay on the cutting edge. The key to success in utilizing emerging security technologies to enhance DOE security, however, is not so much the availability of technology as our ability to identify appropriate technologies and field them in a timely manner. I am working with some of our most talented people to develop a better management model for identifying and fielding new

technologies than we have used in the past. If we are going to be successful in deploying technologies, we must be very innovative in our approach to this problem.

### Consolidation of Materials

Special nuclear materials are among the most important national security assets entrusted to the Department's care. During the Cold War years, when we were engaged in building the nation's nuclear stockpile and in many other urgent national security-related activities, we needed and maintained large amounts of special nuclear materials at many sites throughout the complex. While we still need special nuclear materials at some sites to accomplish ongoing national security missions, both the amount of materials needed and the number of locations where they are needed have substantially decreased. Protecting these materials is among our most difficult security challenges, but we must protect these materials, since the consequences of their loss are unacceptable. We can greatly reduce the difficulty, risk, and costs associated with this mission by disposing of material we no longer need and consolidating the remainder in as few locations as operationally feasible. We have already made significant progress in consolidation efforts at sites that are being de-inventoried and decommissioned. However, much material that could be consolidated remains at sites where it is no longer needed for current or anticipated missions. This is largely because there is no place we have permission to send it or no authorized method of transporting it. We must resolve this issue. Additionally, we need to identify actual future needs for these materials, and identify what more we can do in the way of modifying or relocating operations to facilitate both mission requirements and further consolidation of materials. Since reduction/consolidation of special nuclear materials has perhaps the greatest

potential impact on our future protection requirements and programs, the Secretary has identified six separate initiatives related to this subject. These initiatives range in scope from developing plans for terminating a specific material-using reactor operation to determining the long-term needs and future configuration of the weapons complex. This group of initiatives goes directly to the heart of the challenges we face in our efforts to reduce and consolidate our special nuclear materials inventories and to protect these materials while in storage and in transit.

### Strengthening Security Human Capital Expertise

Of all the components of our protection systems, the human component is the most critical, and the performance of our people will largely determine the success or failure of our protection efforts. Not to ignore the fact that virtually all of our Federal and contractor employees have security responsibilities, when we speak of security personnel in this context we refer to two groups of people: the people who design, implement, maintain, manage, and oversee the various elements of our protection programs; and the protective force personnel who are on the ground 24/7 guarding and defending our assets. The robustness and ultimate viability of our protection programs rests largely in the abilities and performance of these two groups of people. We have recognized the need to augment our current population of security specialists and to recruit and train the next generation of security specialists who will plan and manage our future protection systems. This need was reinforced by the recent findings and conclusions of a commission, headed by Admiral Henry Chiles, established by the NNSA Administrator to examine the security expertise issue within the NNSA. The Chiles Commission report clearly outlined a number of needs in this area, and recommended several actions to address these needs. The

Secretary has directed that these recommendations be extended, as appropriate, across the entire Department. Success in implementing this initiative will greatly strengthen the management and oversight of our safeguards and security programs.

Complex-wide, our protective forces have largely borne the brunt of our post-9/11 enhanced security efforts, many of which have been manpower intensive. The resulting overtime burden on protective force personnel has often been significant, and, to relieve that burden, training has often been reduced – sometimes to the minimum levels required to maintain essential minimum qualifications. We rely on our protective forces too much to allow this situation to continue. Although we have been successful in relieving this situation somewhat through additional hiring, expediting the security clearance process, employment of technology, and other efforts, we still see a need to strengthen and standardize protective force capabilities across the complex. Our Independent Oversight organization recently completed a comprehensive review of DOE protective forces that described current strengths and weaknesses exhibited by these forces. The review team found that line managers are supporting protective force tactical needs through efforts to procure enhanced weapons, ammunition, and equipment, and that performance during force-on-force performance tests indicated that our ability to protect special nuclear materials, always robust, continues to improve. However, there were also some systematic weaknesses identified that were fundamental in the formulation of the Secretary’s announced vision of raising the training standards and performance standards of our protective forces to rival those of elite military forces.

While only three of the Secretary's initiatives deal with investing in safeguards and security human capital, I believe that the long term effects of our efforts here can rival the security impact of our technology-related initiatives. We don't have all the answers in this area yet, but we anticipate that the results of early actions on these initiatives will show us how to further strengthen the human components of our protection systems.

### Implementing the Secretary's Security Initiatives

We understand that we will face some real challenges in managing and implementing these initiatives. They cover a broad range of activities, and they vary greatly as to the magnitude of effort each will require. For example, in anticipated level of effort they range from 90-day tasks to multi-year projects. However, we have already begun work on all of these security initiatives. The Secretary has formally tasked the appropriate organizations to plan for and begin implementation of the initiatives. The Department has developed Implementation Plans for each of the Secretary's fourteen security initiatives, which will be used to guide each activity through completion. But beyond plans, which are necessary prerequisites for these significant efforts, we have begun action on many of these initiatives. For example:

A review of our Design Basis Threat and associated threat assessments is already staffed and underway, and will be concluded by August 6<sup>th</sup> of this year. This is a multi-faceted review that focuses on five primary areas. First, the review is evaluating any changes in applicable intelligence information relating to adversary team sizes, compositions, and capabilities as well as any changes in radiological, chemical, and biological sabotage criteria that have occurred in

the past year since the publication of the DOE Design Basis Threat in May 2003. Second, the review is addressing recent concerns raised by Congress regarding protection strategies for special nuclear material that may be of improvised nuclear device concern in relation to the protection afforded other high-equity Departmental assets. Third, the team is examining whether GAO concerns regarding DBT implementation by FY2006 remain valid in light of recent budget request modifications. Fourth, the team is addressing any concerns with the 2003 DBT expressed by the field; and determining if any technical clarifications of the DBT or implementing guidance are necessary. Fifth, the team is examining the Department of Defense DBT and the associated implementation processes to ascertain if elements should and can be incorporated into the DOE DBT. The review team has completed the initial phase (identification and collection of relevant data) relating to each focus area. The DBT review team has entered the second phase (data analysis) of each focus area. By August 6th the review team will present recommendations to the Secretary, for his decision, regarding any needed changes to the Design Basis Threat or to its implementing guidance.

Our Independent Oversight organization is already taking action to increase the level of cyber security testing, including additional Red Team testing activities, enhanced classified system testing activities, and expanded and continuous scanning and penetration testing of unclassified networks. Our Office of Cyber Security and Special Reviews, utilizing its Cyber Security Testing Network facilities located in Germantown, Maryland and Columbus, Ohio, has begun enhanced red-team testing at DOE sites. Red team testing at one site has been completed and testing at another is well under way. We have also begun mapping DOE computers exposed to the Internet (mapping the DOE network perimeter), and demonstrating the capability to use

penetration testing tools and methodologies on classified networks. Additionally, we are benchmarking ourselves against the National Security Agency and will take advantage of some of that agency's training in approaches to exploitation of cyber system weaknesses.

The Department's "Consolidation of Nuclear Materials Task Force" has been formed and is at work pursuing its goals, which include: identifying opportunities for relocating/consolidating nuclear materials to reduce the number of potential targets; identifying legal, regulatory, and other issues that may impede relocation/consolidation of nuclear materials; identifying program efficiencies that can be achieved; and recommending short term (12 months) and long term (beyond 12 months) solutions to relocation/consolidation. The Task Force is due to issue its report with short term and long-term recommendations in August of this year. However, we are not waiting for the task force to complete its work and present its recommendations before we take action in cases where we have already identified material that we can or must relocate or consolidate. For example, the Secretary has already directed the removal of special nuclear material from TA-18 at Los Alamos National Laboratory; initial special nuclear material shipments are scheduled to begin in September.

NNSA has appointed an implementation team and commenced work to determine how best to implement the Chiles Commission's recommendations for improving our security human capital resources. In support of our human capital improvement initiative, our National Training Center has identified course and curriculum development actions that will be necessary to support additional professional training for security specialists and security managers. Some of these courses will be developed and available within six months.

While we need to be more aggressive in identifying and deploying current and emerging security technologies, the Department has already been active in this regard. The Department has fielded some countermeasures to possible adversary use of weapons of mass destruction, particularly to their use of chemical agents. We have fielded and will continue to field chemical agent protective personal protective equipment, around-the-clock chemical agent detectors, chemically hardened patrol vehicles, and chemically hardened protective force “ready rooms.” We have already applied keyless access technologies at some of our most sensitive facilities and installation of such technologies is proceeding. The Department has already deployed diskless workstations in many of our classified networks where the capabilities of the currently available workstations are sufficient to perform necessary computational tasks.

This list of examples is not exhaustive, but it does serve to illustrate our commitment to security enhancements throughout what is already a very robust protection system.

Before I conclude my testimony, I would like to share an exciting development that we believe will significantly enhance our protective force performance testing and exercise programs. Our Office of Safeguards and Security Evaluations has, for over two decades, used force-on-force performance testing to evaluate protective force tactical capabilities and site protection strategies. Site protective forces have similar exercise programs, which they use for training purposes and to validate protection strategies and tactical plans. Recognizing the importance of an active tactical exercise program to the development and maintenance of protective force tactical

capabilities, subsequent to 9/11 the Secretary directed our sites to increase the frequency of their exercise programs.

Force-on-force exercises are very complex activities requiring substantial planning and resources. One aspect of the site protection program that we review very carefully during every safeguards and security inspection is the ability of the site to conduct an effective force-on-force performance-testing program. We have discovered that these exercise programs vary widely in quality throughout the complex. Some sites have not developed expertise, protocols, and databases adequate to support effective scenario development, exercise control, or evaluation. As a result, performance-testing programs at these sites are unable to properly evaluate their current forces or to support the evolution to an elite force.

We believe rigorous force-on-force performance testing against tough, skilled aggressor forces is one of the most important elements in measuring the effectiveness of our protective forces and in carrying us forward to an elite protective force. We are determined to do our part in advancing the Department's ability to conduct effective and informative force-on-force performance tests, as well as improving our ability to analyze the results of those tests. Therefore, we have decided to establish a Performance Test Center within the Office of Safeguards and Security Evaluations to facilitate our expansion of independent oversight performance testing activities and to establish standard protocols and databases that will be available to all sites for use in their internal exercise programs. This center will maintain standard protocols for all aspects of performance test planning, conduct, and safety for the entire DOE safeguards and security community. It will maintain databases and libraries necessary to support all aspects of

performance test planning, conduct, and control; scenario development; simulation; evaluation; and safety. For example, it will maintain databases on facility characterizations, ballistics effects, explosives effects, barrier delay times, chemical/biological effects, adversary capabilities, terrorist tactics and techniques, and simulation effects, to name a few. It will maintain safety tests and safety plans and protocols associated with appropriate weapons, ammunition, pyrotechnics, and equipment used in performance tests.

The center will work with the field and with our National Training Center to agree upon and formulate standardized versions of common activities, such as rules of engagement for exercise players, Controller rulings for various events, and minimum Controller training requirements. My staff is already working on the first initiatives that will be associated with the center, which include establishing common protocols for conducting rigorous performance tests across DOE and developing a database containing effects of explosives and other postulated adversary breaching techniques against common DOE defensive barriers. We are also laying the groundwork to provide input to the National Training Center curriculum on how to conduct force-on-force exercises and on how to role-play a determined adversary as realistically as possible. We expect to have some of the structural elements of the center, such as computer tactical scenario simulators, modeling software, and other basic analytical tools, in place by January 2005. This center will significantly streamline and enhance our own performance testing capabilities, and can provide similar benefits to sites that choose to draw on its resources for their internal exercise programs.

## **Concluding Remarks**

In previous testimony before this committee, which dealt primarily with our revised Design Basis Threat, we expressed the belief that the Department's senior leadership was dedicated to improving our protection programs and was willing and determined to take the necessary steps to achieve that objective. Subsequent actions, including the Secretary's decision to implement fourteen far-ranging security initiatives and his direction to get to work quickly on all of them, have reinforced that belief. While at this point it is too early for these recent initiatives to have yet produced significant tangible results, the eventual fruits of these initiatives will be significant improvements in our protection programs.

We are confident that special nuclear materials and classified information are adequately protected throughout the complex. We also understand that portions of our protection programs need to be improved, and that the changing nature and capabilities of the threats we face may require further strengthening or realignment of protection program elements in the future. Implementation of the security initiatives we have discussed above will better enable us to respond to these needs. We of course have to follow through on these initiatives to ensure that they yield the expected concrete improvements in our protection programs. We believe that our line managers and staff are prepared to do so, and that the Department's senior managers will ensure that we do so.

Thank you. This concludes my prepared testimony.