

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

April 27, 2004

Unclassified Congressional Testimony
Subcommittee on National Security, Emerging Threats, and International Relations
House Committee on Government Reform
April 27, 2004

Introductory Remarks

Mr. Chairman and honorable members of the subcommittee, I want to thank you for inviting me to testify today regarding the Department of Energy's processes for developing, evaluating, and implementing its Design Basis Threat, which it uses as a benchmark to develop and evaluate protection systems throughout the Department. We agree with the Subcommittee's assessment that the current threat environment facing the Department – and indeed facing the entire nation – represents a considerable potential risk to our facilities, assets, and personnel. Everyone in the Department having security responsibilities – from the Secretary to our armed protective forces and our individual employees – is aware that we live in dangerous times and that we have custody of particularly sensitive information, materials, and facilities that must be protected from a range of potential adversaries. We do not take our protection responsibilities lightly. The Secretary, Deputy Secretary, and NNSA Administrator are committed to meeting our protection challenges and have provided the impetus for numerous improvements in our protection programs, some of which I will discuss in this testimony.

The Subcommittee has asked that we specifically address several issues as they relate to the General Accounting Office's report: *Nuclear Security: DOE Needs To Resolve Significant Issues Before It Fully Meets the New Design Basis Threat*. In responding to the Subcommittee's request, I will start by addressing the specific issues highlighted in the GAO report, and will then describe the specific role of my organization, the Office of Security and Safety Performance Assurance, in the Department's implementation process for the revised Design Basis Threat. I will then describe what we consider to be a directly related and more important issue: the several key initiatives now underway that will significantly

aid our efforts to improve the performance of our protection programs and facilitate our efforts to fully implement the requirements of the revised Design Basis Threat on schedule. Let me begin then with the specific issues raised in the GAO report.

Issues Reflected In The GAO Report

First, I would like to say that we believe the GAO did a thorough and professional job in researching and writing this report, and we value and appreciate their effort. We agree that the issues raised in the report are legitimate and valid issues that we must address. As is acknowledged in the report itself, we ourselves first identified some of those very issues and have been working to resolve them.

Revised Design Basis Threat Development Period

The first GAO report issue that I will address involves the period of time it took – almost two years – to develop and issue the new Design Basis Threat. GAO attributes this development period to delays in the intelligence community’s efforts to develop an updated Postulated Threat, to DOE’s application of its rather lengthy policy development review and comment process to the revision of the Design Basis Threat, and to sharp debate within DOE and other agencies regarding the size and capabilities of future terrorist threats and the availability of resources to counter those threats.

The Department’s Design Basis Threat Policy is predicated on an interagency document titled *The Postulated Threat To U.S. Nuclear Weapons Facilities and Other Selected Strategic Facilities* (the Postulated Threat), developed jointly by DOE and other agencies, including intelligence agencies, and published by the Defense Intelligence Agency. Previous versions of the Postulated Threat were published as (interagency) policy, and consequently provided a substantial basis for our own Design Basis Threat policy.

Even before the terrorist attacks of September 11, 2001, there was considerable discussion within DOE of the need to update our Design Basis Threat. However, a thorough revision of the Design Basis Threat policy was dependent on the updating of its source policy, the Postulated Threat. In August 2001, shortly before the September 11th attacks, DOE initiated discussions with other agencies aimed at reviewing and revising the 1998 Postulated Threat. After September 2001, it was clear that the true nature of the terrorist threat was significantly different from that reflected in previous threat assessments, and the need to revise the Design Basis Threat to better reflect newly-recognized realities was beyond debate. There was a concurrent recognition among the agencies responsible for the Postulated Threat that it also needed revision, for the same reasons. However, the very events that highlighted the need to revise our threat policies – the terrorist attacks of September 11th – also resulted in the reallocation of the resources needed to revise the Postulated Threat to support real-time assessments of terrorist threats for national and international events. Consequently, efforts to revise the Postulated Threat were delayed for several months.

In January 2002 the Defense Intelligence Agency, assisted by DOE and other agencies, including intelligence agencies, resumed the effort to update the Postulated Threat. This effort took approximately one year and involved several revisions. During that period, DOE developed and internally circulated several drafts of a revised Design Basis Threat, each based on the (then) current version of the developing Postulated Threat. Each of these drafts was circulated among our appropriate program offices for review and comment. The Defense Intelligence Agency published the new Postulated Threat document in January 2003 as a report (a threat assessment) rather than as a policy as had been previous practice. DOE used the final version of the Postulated Threat to develop the final version of its revised Design Basis Threat, which was issued several months later in May 2003.

Even given the various circumstances and the complicated nature of this development process, and the necessity of knowing the ultimate parameters of the revised Postulated Threat before finalizing our revised Design Basis Threat, we acknowledge that this process took longer than we would have liked. The Secretary realized at the time that, even though this was a complicated development process with significant impact on future programs, operations, and budgets, progress was slow, and he monitored progress of the development effort through status briefings and updates. His concern about the pace of progress and the need to improve internal coordination of such matters was one of his motivations for creating the Office of Security and Safety Performance Assurance. It is important to note, however, that DOE did not wait for the publication of a revised Design Basis Threat to take action to increase security at our facilities. As described in the GAO report, on September 11, 2001, we recognized the changed nature of the threat and instituted a number of measures to increase physical security levels at our sites; many of those measures remain in effect. Some of those measures are manpower intensive and intended to be temporary in nature. Our deliberative process for implementing the requirements of the revised Design Basis Threat, now underway, will result in longer-term, more permanent, more sustainable, more robust, and more efficient and cost-effective upgrades to our protection systems.

Variations Between Threat Parameters in the Postulated Threat and the Design Basis Threat

The GAO report points out that although the magnitude of the terrorist threat described in the revised Design Basis Threat is greater than that described in the previous policy, it is smaller than that described in the current Postulated Threat. It also offers the opinion that the criteria DOE has selected for determining when a facility may need to protect against radiological, chemical, or biological sabotage may not be sufficient.

The differences in the parameters (e.g., numbers of terrorists, etc.) that appear in our Design Basis Threat versus those in the Postulated Threat result from the differing scopes and purposes of the two documents.

The interagency Postulated Threat is intended to serve as a reference for long-term planning and programming by U.S. security forces. It takes into account potential threats against U.S. assets worldwide, both inside and outside the U.S., and characterizes what that threat is expected to look like over a ten-year period. Given that scope, it assesses adversary capabilities in geographical areas where adversary groups are home-based, operate in locations where they receive a level of support from governments and societies, or operate in locations where there is little or no government control. In such environments, potential adversaries have expanded capabilities. Hence, the Postulated Threat identifies a range of adversary capabilities that is based on what is possible anywhere in the world.

The DOE Design Basis Threat has a different purpose. It is the design basis for DOE protection systems and a performance standard for established protection systems. As such, it defines specific adversary group sizes, equipment, and capabilities that must be countered with a high probability of success. Through extensive analysis using the best data available from the U.S. intelligence community, DOE analysts have established the current Design Basis Threat at a level that encompasses past terrorist events worldwide, requires sites located in the United States to design and analyze protection systems against specified adversary capabilities, and establishes a very high performance standard against that threat. In addition, the Design Basis Threat provides the protection strategy that must be used for each of several target types: examples of such strategies range from denial of access to establishing appropriate administrative controls. While the revised DOE Design Basis Threat takes into account a variety of sources and assessments, including the 2003 Postulated Threat, it is crafted to meet the Department's specific needs in relation to carrying out its protection responsibilities.

Regarding GAO's assertion that the criteria we are using to determine when facilities may need to be protected against radiological, chemical, or biological sabotage may not be sufficient, we can assure you that our intent is to employ appropriate criteria based on sound science. At present, much of that science is oriented toward establishing safe levels of release during normal operations and under accident

conditions. While the currently established criteria may not be the best for assessing malevolent acts, they do represent the current level of knowledge. For this reason, they were incorporated into the current Design Basis Threat while additional studies are conducted throughout the scientific community to determine whether they provide an appropriate level of protection against the actual threats depicted in the Postulated Threat and other intelligence community assessments. The Department is continually working with other government agencies to evaluate the criteria used for radiological, chemical, and biological sabotage determinations. In particular, the Department continually monitors government policy and legislation pertinent to toxicological sabotage and is committed to modifying our threat policy upon the issuance of new or revised standards. For example, we have developed a policy, currently in the final stages of comment and review, addressing the safeguarding of select biological agents and toxins. It is based on 42 CFR 73 and incorporates the best security practices of both DOE and the Centers for Disease Control.

We believe that the rationale used for the development of our current Design Basis Threat, described above, is sound and was the appropriate approach. However, we are continually looking for better ways to do things, and I have directed a review of this process to determine if this is still the best approach and if there is more we should be doing in this area.

Consequences and Effectiveness of Heightened Security Measures

While the GAO report credited DOE with taking immediate steps to improve physical security in the aftermath of the September 11th attacks, it indicated that those largely manpower intensive measures are expensive and have resulted in elevated levels of fatigue, retention problems, and reduced training for our protective forces. The report also indicated that the effectiveness of the increased Security Condition levels employed has not been assessed using formal vulnerability assessment tools such as computer modeling and force-on-force exercises.

DOE has recognized from the outset the large burden that was placed on our protective forces to implement the increased Security Condition levels in effect since the September 11th attacks. However, the situation required our line managers to act quickly to provide adequate protection for our facilities against the heightened threat, and that often meant employing measures that were designed for temporary use. The protection element that could be modified most quickly was the number of protective force members on duty. Therefore, unavoidably, some sites adopted measures that were costly, manpower intensive, and, over time, impacted the readiness levels of our protective forces. As the increased threat level continued, some sites took the initiative to modify other aspects of their protection systems to reduce some of the burden on the protective force. Additionally, the long process of hiring, clearing, and training new protective force personnel is providing some relief to the burden on our protective force personnel.

Acknowledging that the increased level of danger of a terrorist attack is not going to subside soon but will likely be with us for the foreseeable future, on September 8, 2003 the Secretary directed line managers and security professionals to emphasize finding or devising effective methods to make safeguards and security dollars go farther and to reduce the reliance on protective force manpower. He also directed my office to look hard at technologies that could be deployed to provide relief to the manpower burden issue and improve protection systems in other ways. I will discuss our efforts in that area in more detail later in my testimony.

The GAO was correct in asserting that when we implemented increased Security Condition levels, we had not formally analyzed or tested the effectiveness of those increased levels. However, our protection posture at higher Security Condition levels is more restrictive and more robust than our normal protection posture. Intuitively, therefore, we conclude that our protection posture at higher Security Condition levels will provide increased protection, but, in the press of time following September 11th, we did not apply our formal vulnerability assessment process to assessing the precise increase in protection before employing

them. Our formal vulnerability assessment process provides a comprehensive assessment of the protection system and is therefore very time consuming and expensive. Under normal conditions, DOE sites are required to employ it to ensure that their basic protection posture provides an acceptable level of assurance that it can defeat the applicable threat. As an essential element of Design Basis Threat implementation, DOE sites are now engaged in employing the rigorous vulnerability assessment methodology to evaluate every aspect of their protection systems, including the additional measures required to implement enhanced Security Conditions.

This additional vulnerability assessment effort requires more resources, and we recognize that one of our current weaknesses is a shortage of personnel formally trained to apply the very complex vulnerability assessment methodology. To address this need, I have directed our National Training Center (formerly the Nonproliferation and National Security Institute) to increase the output of security professionals trained in the application of this methodology.

Overarching Issues In Need Of Resolution

Finally, the GAO report noted that in order to meet the requirements of the new Design Basis Threat DOE needs to address several overarching issues, such as providing additional Design Basis Threat implementation guidance, creating implementation plans, and developing budgets to support those plans. The GAO report also expressed doubt that DOE's goal of meeting the requirements of the new Design Basis Threat by the end of FY2006 was realistic for some sites.

As the GAO acknowledged in its report, DOE had previously identified these specific issues and was already in the process of addressing them at the time GAO was collecting its data. In December 2003, formal training was provided to DOE vulnerability analysts in the improved vulnerability assessment process required to address the revised structure of the Design Basis Threat. In January 2004 the Deputy

Secretary issued additional guidance regarding the expectations and procedures for full implementation of the new Design Basis Threat. That guidance includes the requirement for each site to develop and maintain implementation plans that identify all tasks necessary to achieve full implementation of the Design Basis Threat and that establish realistic and measurable milestones necessary for the completion of all identified tasks. It further requires line managers, including Secretarial officers, to review and approve the implementation plans and to track the progress of implementation efforts. Progress toward achieving established milestones must be assessed, tracked, and reported on a quarterly basis, and quarterly reports must also include an assessment – based on the results of current vulnerability assessments, computer modeling, and performance testing – of the level of threat each facility is prepared to meet. Finally, the guidance requires our independent oversight organization to critically review site implementation plans, test the effectiveness of protection system changes that are implemented, and evaluate the ability of protection systems to protect against the level of threat claimed in the quarterly reports.

Sites have developed and submitted initial implementation plans, and these plans have been reviewed by the appropriate line managers, Secretarial officers, and by my office. In some cases, revisions to the initial plans were necessary to fully establish the analytical basis for the proposed actions and to supply additional detail regarding implementation schedules. These implementation plans are living documents. The initial plans reflect the best knowledge available at the time they were developed, and many were primarily based on existing vulnerability assessments updated by tabletop exercises, expert opinion, and performance testing. The results of ongoing vulnerability assessment activities, mission changes, consolidation of materials, or other factors may require modification of some aspects of some plans during the implementation period. Any necessary modifications to the implementation plans will be documented, approved, and incorporated into the plans through the quarterly reporting process.

Line management's review of the implementation plans and supporting documentation evaluated the projected costs associated with implementing the requirements of the Design Basis Threat. The plans include the justifications for needed upgrades and identify the most cost-effective upgrades necessary to achieve a high level of protection system effectiveness. The Department's FY2005 Congressional budget submission includes costs for planned security enhancements, and funds needed to complete full implementation of the Design Basis Threat, based on the results of vulnerability assessments now in progress, will be addressed in the FY2006 budget submission.

Regarding the ability of all sites to fully implement the Design Basis Threat by the end of FY2006, I must emphasize that we have established that as our goal and we have every intention of meeting it. The Department has made a very aggressive commitment in this case: we have identified what needs to be done, we have instituted a process to monitor progress toward individual milestones and toward the ultimate goal of full implementation, and DOE is committed to achieving all protection goals by the end of FY2006. If and when progress or the likelihood of progress falls below expectations, senior managers will take appropriate action. This approach has already led the Secretary to direct that special nuclear material be expeditiously moved from TA-18 at Los Alamos National Laboratory to the Nevada Test Site. If, as the end of FY2006 approaches, we assess that some facilities cannot fully and reliably perform to the requirements of the Design Basis Threat, the Department's managers will take immediate and appropriate action to mitigate urgent risks. These actions could include a wide range of management responses, including curtailment or modification of special nuclear material handling and operations, modifications to the protective posture, or any other compensatory actions necessary to protect our assets in accordance with the requirements of the Design Basis Threat.

SSA's Role in Design Basis Threat Implementation

While primary responsibility for implementing the requirements of the Design Basis Threat rests with our individual sites and their line management chains, the Office of Security and Safety Performance Assurance is responsible for assisting in this effort, monitoring progress, and validating the effectiveness of program enhancements. We have developed a three-phased approach to discharge this responsibility.

In Phase One, our Office of Security carefully reviewed the initial site implementation plans to determine if they fully met the requirements laid out by the Deputy Secretary in his January 2004 Memorandum. Whenever an implementation plan fell short of expectations in any way, the deficiencies were fully identified to the responsible program office so the plan could be appropriately amended. Phase One has been completed for the submitted plans.

During Phase Two, Office of Security subject matter experts review the supporting documentation accompanying each implementation plan. This activity typically includes analysis of vulnerability assessments to determine their accuracy, applicability, and appropriateness, and may include site visits as needed. If these reviews indicate the need for any modifications to the implementation plan, the Office of Security will work with the site to identify the specific modifications needed. Phase Two is well underway.

Phase Three involves ongoing technical assistance and validation efforts. The Office of Security will deploy multi-disciplinary safeguards and security teams – consisting of experts in physical security, protective forces, alarm command and control systems, and material management and control – to provide guidance and assistance on specific technical matters unique to each site. These teams will assist the sites and program offices in identifying appropriate ways to meet the long-term operational requirements of the Design Basis Threat. As I will discuss in more detail shortly, the Office of Security will also assist sites

in this effort by identifying and deploying existing technologies and developing and deploying new technologies that can increase the effectiveness and efficiency of protection systems. Additionally, the Office of Independent Oversight and Performance Assurance, through its program of scheduled oversight activities, will review progress toward achieving implementation plan milestones and will evaluate the effectiveness of protection program enhancements that have been implemented.

Key Efforts To Improve Security Performance in the Department.

In my testimony to this point I have addressed your specific interests in the issues raised and discussed in the GAO report. Those issues deal largely with events of the past. In my opinion, what the Department is currently doing to improve security programs and to facilitate the full implementation of the requirements of the revised Design Basis Threat are of more importance and relevance, and may be of greater interest to the members of the subcommittee.

The Department's senior leadership, including the Secretary, the Deputy Secretary, and the NNSA Administrator, is fully committed to properly discharging the Department's security responsibilities, including the timely and thorough implementation of changes necessary to meet the requirements of the revised Design Basis Threat. They have demonstrated this commitment repeatedly, over time, through a number of security-related initiatives. That commitment is reflected in Secretary Abraham's recent creation of my organization. While the Secretary properly holds line managers accountable for effectively implementing security programs, he recognized that the Department's efforts to improve protection programs could be accelerated and could yield more effective results if relationships and interactions between Headquarters elements and the field were improved. Secretary Abraham created my office – the Office of Security and Safety Performance Assurance – to implement his firm belief that Headquarters security resources, working closely and collegially with the field, could increase the timeliness and effectiveness of protection program upgrades and could ensure that appropriate security

technologies could be deployed where and when needed. His directions to me when he created the office resulted in four major new priorities for my office: to improve communications and cooperation between my organization and the field; to improve the quality of security policy and policy guidance; to evaluate and develop security-related technologies and make them available to the field in a timely manner; and to overhaul security training to ensure that national-level training resources are responsive to the needs of field organizations. We believe that improvements in these four areas are key not only to our current efforts to improve security and fully implement the requirements of the revised Design Basis Threat, but also to the future overall vitality and robustness of our protection programs. The importance of our initiatives in these areas and their pertinence to the interests of the members of the Subcommittee merit further discussion here, so I will more fully describe each.

Improved Communication Between Headquarters and The Field

First, we are improving the quantity and quality of (security-related) communication between my office (including my subordinate policy and independent oversight offices), other Headquarters staff and program offices, and field elements, including both line managers and security professionals in both Federal and contractor field organizations. It is critically important to our efforts to improve the effectiveness and efficiency of our protection programs that everyone in the Department with security program responsibilities fully understand each other's concerns and points of view, fully understand what is expected of them, and fully and openly share ideas, information, and lessons-learned to the benefit of the entire DOE community. The task of improving communications among individuals and organization is both easy and difficult. It is easy because the information that needs to be exchanged already exists, and simply has to be exchanged between the appropriate parties. It is difficult because the exchange of that information in some cases requires modifications of established patterns of interpersonal relationships, management-imposed information flow processes, and organizational relationships. We are working hard to ensure that all organizational relationships are mutually beneficial and supportive of

protection program needs. While numerous formal and informal communications mechanisms already exist, our goal is to make these more effective.

Improved Security Policy and Guidance

Our security policies and the accompanying implementation guidance are the foundations upon which our protection programs are built. We believe that our security policies across the board should be practical, based on real needs, implementable, and sufficiently clearly stated as to not be open to widely divergent interpretations. Some of our current policies fall short of this mark, and have been contributing sources to some of the delays we have experienced in improving our programs in some areas. A major contributing factor to the issues concerning policy was a past decision to prohibit policy developers from communicating directly with field sites. This speaks directly to the previously discussed focus area – improved communications. The Deputy Secretary recently directed a change to this ill-conceived practice, and we have established necessary dialogues to facilitate policy revisions and development. Our policy organization is already at work reformulating many of our security policies to make the needed improvements. Their instructions, as indicated above, are to ensure that policies are based on needs, practical, implementable, and clearly stated.

Introduction of Security-Related Technologies

The Secretary sees our ability to implement new security technologies as crucial to our ability to fully implement the requirements of the revised Design Basis Threat. We are convinced that improved technologies will be a long-term key in our efforts to improve the effectiveness, and particularly the efficiency of our protection programs. We have to move away – whenever possible – from manpower intensive responses to security concerns or elevated risks – the tendency to “add more guards.” Manpower intensive responses are very costly and often not extremely effective. Permanent use of

additional manpower involves long lead times to hire and clear personnel, and short-term use of additional manpower often involves oppressive levels of overtime, which degrades individual performance. The introduction of new technologies such as active and passive barrier systems and others, can act as force multipliers that reduce our dependence on increased manpower levels. My office is charged with evaluating or developing such security-related technologies, making them available to the field for implementation in a timely manner, and assisting the field as necessary in their implementation. The Department has the scientific and technical resources to address our technology needs, and in fact we do development work in this area for ourselves and for other agencies. The NNSA Administrator, Linton Brooks, and I intend to improve our internal efforts in this area and provide the field with technological options that they can use to reduce manpower and improve the effectiveness of their protection systems.

This effort is already underway. For example, a current project at Oak Ridge illustrates our efforts in this area and the potential for more effective employment of technology. My staff is cooperating with project staff at Oak Ridge to incorporate more and newer technology into the design of the protection system for a building where special nuclear material processing will be conducted to allow removal of the material and eventual decontamination and decommissioning of the building. Clearly, a substantial cost savings can be realized for this project if other methods can be substituted for the expensive protection measures normally applied to a permanent facility. We are confident that, working together, my office and the line managers responsible for these operations will be able to devise a solution that will provide cost-effective protection while significantly reducing protective force manpower requirements. Other complex-wide efforts, such as our drive to consolidate special nuclear materials, will also help to reduce the protection challenge and manpower requirements.

Improved Security Training

The final focus area for major overhaul is security training. My policy organization, through its National Training Center (formerly Nonproliferation and National Security Institute), is responsible for establishing security training standards and for providing safeguards and security related professional training of various types. We intend to increase the efficiency and effectiveness of those efforts by ensuring that the way training resources are employed is more responsive to the specific needs of field organizations. To that end, I have recently appointed a well-qualified manager in my organization as Director of the National Training Center, and I have given him specific guidance regarding my expectations for the employment of these substantial training resources. Even prior to that appointment, we were moving to respond to needs in this area. As I mentioned previously, late last year we conducted specific training in new vulnerability assessment methodologies, and a related priority is to respond to the needs of the field by training additional security professionals in that very complex process.

We are focusing considerable effort on these four areas, and I strongly believe that the Secretary's instincts will prove to be correct and that these initiatives will have a profound effect on our efforts to strengthen our protection programs. We are already at work improving our performance in these areas. Most of the necessary infrastructure was already in place, and in some cases we just need to change some of our practices and ways of doing business to achieve our desired goals.

Concluding Remarks

As I conclude my remarks, I want to emphasize my belief in the sincere intentions and unprecedented efforts of the Department's senior managers to improve our protection program performance. The Department's leadership understands and acknowledges that the goal we have set for ourselves – to fully implement the requirements of the revised Design Basis Threat Department-wide by the end of FY2006 –

is a lofty goal. It is a challenging goal. To meet it will require both continuing management attention and support and a significant effort by many people throughout the Department. The Department's leadership has declared its willingness and determination to take the steps necessary to meet this goal, and has backed its declaration with action. The Secretary's issuance of the revised Design Basis Threat and the Deputy Secretary's direction to the Under Secretaries to respond to it immediately (e.g., to apply it immediately to new facilities and operations, to the restart of dormant facilities and operations, and to all vulnerability assessments occurring after May 2003) reflects a commitment and a resolve to make positive changes to the Department's security programs. The Deputy Secretary's stringent guidance on the process for implementing the Design Basis Threat for facilities and operations that could not implement it immediately, and the Secretary's creation of my office to expedite security-related improvements are further confirmation of an unyielding intent to improve the Department's protection program performance.

We have made significant progress toward implementing the revised Design Basis Threat at many sites, we are currently on track, and managers have demonstrated their willingness to make hard decisions to support the effort. Without minimizing the magnitude of the task ahead, we believe that the Department is approaching the task with confidence and a determination to succeed. We fully intend to pursue our efforts to improve our protection programs until we achieve a Department-wide level of performance that meets our own expectations as well as the expectations of Congress and the American people. Thank you. This concludes my prepared testimony.