STATEMENT OF HERBERT RICHARDSON
PRINCIPAL DEPUTY INSPECTOR GENERAL
U.S. DEPARTMENT OF ENERGY

BEFORE THE
U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

FOR RELEASE ON DELIVERY
Thursday, March 4, 2004

Mr. Chairman and members of the Subcommittee, I am pleased to be here today to respond to your request to testify regarding physical security at the Department of Energy's facilities. The Department's activities range from nuclear nonproliferation, to cutting edge research and development, to weapons programs. The sensitive and critical nature of the Department's work necessitates that its security operations be robust, and for the last several years, the Office of Inspector General has identified security as one of the most critical management challenges facing the Department. Therefore, our office devotes a significant portion of its resources to reviewing the effectiveness of those operations. Our work has been extensive and across the security spectrum, including physical security, personnel security, cyber security, and the protection of Department assets, such as computers, firearms, and nuclear materials.

The cumulative body of our work over the last several years demonstrates that, although the Department has taken a number of actions to enhance its security operations, particularly in response to the events of 9/11, there needs to be a continuing effort to ensure the integrity of the Department's security. Today, I will discuss recent Office of Inspector General reviews related to the Department's protective forces and access controls. The three reviews I will focus on address (1) improprieties in protective force performance testing at the Department's Oak Ridge complex, (2) inadequate internal controls over the reporting of security incidents at the Lawrence Livermore National Laboratory, and (3) issues concerning the Department's standardized core training curriculum for protective force personnel.

Protective Force Performance Test Improprieties (DOE/IG-0636, January 2004)

First, I will discuss an Office of Inspector General review of protective force performance test improprieties. On June 26, 2003, a protective force performance test was conducted at the Department's Y-12 National Security Complex. The purpose of the test was to obtain realistic data for developing the Y-12 Site Safeguards and Security Plan. The mission at the site includes a number of national security related activities, such as enriched uranium warehousing, weapon dismantlement and storage, and manufacturing of nuclear weapon components. These activities necessitate that the site have a protective force capable of responding to potential security incidents such as a terrorist attack.

Computer simulations conducted prior to the June 2003 performance test had predicted that the responder (defending) protective forces would decisively lose two of the four scenarios that comprised the test. When the responder protective forces won all four of the scenarios during the June 26, 2003, performance test, the Y-12 Site Office Manager became concerned that the test may have been compromised. The Manager initiated an internal inquiry, which raised issues related to responder protective force personnel having had access to the computer simulations of the four scenarios prior to the performance test. Subsequently, at the Y-12 Site Office Manager's request, the Office of Inspector General initiated a review to address these issues.

Our inspection confirmed that the results of the June 26, 2003, performance test may have been compromised. We determined that shortly before the test, two participating protective force personnel were permitted to view the computer simulations of the four scenarios. The two

individuals denied that the information to which they were given access affected their actions or directions to others who participated in the exercise. However, when we viewed the computer simulations, it became clear that the occurrence of certain specific events would identify which scenario was being initiated by the aggressor force. The responder protective force could use this information during the performance test to readily identify at the beginning of a scenario which target was being attacked and respond accordingly. The order in which the targets would be attacked was controlled test sensitive information. Therefore, in our judgment, the test results were tainted and unreliable.

Based on information developed during our review, the scope of the inspection was expanded to examine whether there had been a pattern over time of site security personnel compromising protective force performance tests. During our inspection, we interviewed over 30 current and former site security police officers (SPOs) and SPO supervisors. We received compelling testimony from a number of individuals that there has been a pattern of actions by site security personnel spanning back to the mid-1980's that may have negatively affected the reliability of performance tests at the Oak Ridge complex, including those conducted during Headquarters oversight reviews. Several individuals told us, for example, that controlled information was shared with SPOs prior to their participation in a given performance test, including the following:

- The specific building and wall to be attacked by the test adversary;
- Whether or not a diversionary tactic would be employed by the test adversary; and
- The specific target of the test adversary.

We did not find documentary evidence to support or refute the testimonial evidence. However, it was clear that if controlled information was, in fact, disclosed prior to the performance tests, the reliability of the information used to evaluate the efficacy of the protective force at the Oak Ridge complex was in question.

We made a series of recommendations to site management designed to enhance the integrity of future performance tests at the Oak Ridge complex. We also recommended that the Director, Office of Independent Oversight and Performance Assurance take action to ensure the integrity and realism of future performance tests at Y-12 and other Department facilities. Management concurred with our recommendations.

Reporting of Security Incidents at the Lawrence Livermore National Laboratory (DOE/IG-0625, November 2003)

Next, I will discuss our review of the reporting of security incidents at the Department's Lawrence Livermore National Laboratory. Livermore also performs activities that require extremely high levels of security. On May 5, 2003, Livermore reported to the Department that a set of master keys had been discovered to be missing on April 17, 2003. On May 30, 2003, Livermore reported to the Department that a master Tesa card, which is a plastic card-like key with a magnetic strip, had been discovered to be missing on April 12, 2003. These losses and the delay in reporting them raised security concerns; therefore, we initiated a review to determine the adequacy of internal controls for reporting and mitigating security incidents at Livermore.

We concluded that Livermore did not have adequate internal controls to ensure that security incidents involving missing master keys and master Tesa cards were reported within required timeframes and that timely follow-up actions were taken to identify and address potential security vulnerabilities resulting from the incidents. Specifically, we found that Livermore security officials:

- Misinterpreted fundamental Department reporting requirements for security incidents and did not immediately recognize the significant security implications of the missing master keys and master Tesa card;
- Did not report the security incidents involving the missing master keys and master Tesa card to the Department within required timeframes;
- Did not immediately assess potential security risks to identify vulnerabilities resulting from the missing master keys and master Tesa card; and
- Did not take timely action to mitigate the potential vulnerabilities resulting from the missing master keys and master Tesa card.

During our review, we learned that a May 2003 inventory by Livermore identified an additional three master keys and two master Tesa cards that were missing. Further, two of the three missing master keys had been reported to Livermore's Protective Force Division more than three years before, but the Protective Force Division did not conduct an inventory or determine why the keys were missing. We also noted that recent Department and Livermore oversight reviews

of Livermore's safeguards and security operations did not identify internal control weaknesses related to the control and inventory of master keys and master Tesa cards.

Livermore has initiated actions to replace or upgrade locks. The associated costs may be significant. We questioned the allowability of these costs because we believe that Livermore failed to ensure compliance with established internal controls over the master keys and master Tesa cards.

In response to our report recommendations, management identified corrective actions, including implementation of additional procedures and training. We believe, however, that management needs to do more to assure that Livermore places greater emphasis on the need to strictly follow its processes and procedures for reporting and mitigating security incidents.

The Department's Basic Protective Force Training Program (draft report)

Lastly, I will discuss a soon to be released audit report on protective force training. The Department employs approximately 4,100 contractor personnel dedicated to serving as uniformed security officers responsible for protecting Department sites. This includes approximately 500 officers hired subsequent to the events of 9/11 as part of the Department's efforts to enhance its security posture. The Department's significant security mission necessitates that its protective forces be adequately trained. The Department's policy is to train its security forces to deal with a broad spectrum of threats by providing a standardized, core training curriculum that ensures interoperability across the complex. We initiated an audit to

determine whether sites were meeting the Department's standardized, basic protective force core training curriculum. We did not specifically look at the appropriateness of the existing core curriculum.

We determined that 10 of the 12 sites included in our review had made significant modifications to the Department's established protective force core curriculum. Specifically:

- Each of the 10 sites eliminated or modified 2 or more blocks of instruction from the core curriculum. At 1 site, about 40 percent of the basic security police officer core curriculum, including courses in the use of shotguns and baton techniques, was eliminated;
- Seven sites used reduced force training methods for skills that some security experts characterized as critical, such as handcuffing, hand-to-hand combat, and vehicle assaults; and
- None of the 10 sites included instruction in rappelling, a core curriculum course for special response team training.

Further, we noted that Department managers had not always been informed of modifications in the core curriculum, which excluded them from reaching any judgment as to the impact of these actions on the Department's security interests. We noted that modifications to the core curriculum and training delivery methods occurred because site security managers questioned the applicability of certain courses or had safety concerns. The resulting variations were not always detected, or their impact on readiness assessed, because the Department did not require the sites

to report departures from the core training requirements to either the program offices or the Office of Security.

We concluded that modifications to the core curriculum may increase the risk that the Department's protective forces will not be appropriately and fully trained to carry out their security responsibilities. Also, in our judgment, the high number of modifications raises serious questions about the validity of the curriculum. Management generally concurred with our report recommendations.

CONCLUSION

In general, the Department has been receptive to our work and has concurred with our recommendations. However, a number of those recommendations are still awaiting the completion of implementation actions by the Department. We will continue to examine the Department's programs and operations for additional ways we can facilitate the enhancement of the Department's security posture and ensure the Department is fulfilling its critical role in this Nation's security.

Mr. Chairman and members of the Subcommittee, this concludes my statement. I will be pleased to answer any questions.