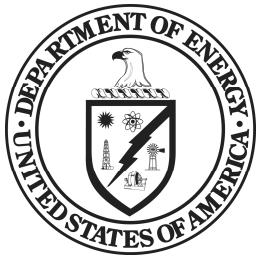

U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Special Report

Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex

DOE/IG-0868 August 2012

Department of Energy

Washington, DC 20585

August 29, 2012

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Special Report on "Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex"

BACKGROUND

The Y-12 National Security Complex is one of four production facilities in the National Nuclear Security Administration's Nuclear Security Enterprise. The site focuses on the processing and storage of uranium, an activity essential to the safety, security and effectiveness of the U.S. nuclear weapons stockpile. Y-12 maintains an extensive security mechanism that relies on a well-trained and extensively equipped protective force, advanced technology, and a variety of physical fortifications. During Fiscal Year 2012, Y-12 plans to devote about $150 million in taxpayer funds to ensure the security of its uranium inventory and physical plant. Y-12 has long enjoyed a reputation as one of the most secure facilities in the United States.

During the early morning hours of July 28, 2012, three individuals (hereinafter referred to as the trespassers), gained access to the area surrounding the Highly Enriched Uranium Materials Facility (HEUMF) at Y-12 and defaced the building without being interrupted by the security measures in place. In fact, the trespassers were not physically observed by the Y-12 Protective Force until after they had severed three separate fences surrounding the HEUMF. After receiving a call from the Oak Ridge Operations Center, Office of Inspector General (OIG) special agents arrived, arrested the trespassers and transported them to the Blount County Detention Facility. We initiated a joint criminal investigation of the trespass and, at the time of this report, were working closely with the Federal Bureau of Investigation and the U.S. Attorney for the Eastern District of Tennessee on this matter.

Because of the importance of ensuring the safe and secure storage of nuclear materials we commenced a special inquiry into the circumstances surrounding the Y-12 breach within days of the event.

PRELIMINARY RESULTS

During our review, we conducted interviews with Federal and contractor officials, security personnel, and alarm station operators. We also reviewed supporting information pertinent to the sequence of events on the night of the breach. Based on these inquiries, we found that the Y-12 security incident represented multiple system failures on several levels. For example, we identified troubling displays of ineptitude in responding to alarms, failures to maintain critical

security equipment, over reliance on compensatory measures, misunderstanding of security protocols, poor communications, and weaknesses in contract and resource management. Contractor governance and Federal oversight failed to identify and correct early indicators of these multiple system breakdowns. When combined, these issues directly contributed to an atmosphere in which the trespassers could gain access to the protected security area directly adjacent to one of the Nation's most critically important and highly secured weapons-related facilities.

Alarm Response

We found that the response to the security breach at Y-12 was inadequate in several material respects. Although immediately aware that a number of alarms had been activated at the HEUMF, a Protective Force officer was not promptly dispatched to assess the situation. When an officer finally arrived, the individual did not immediately secure the scene or neutralize the trespassers. This did not occur until a supervisor arrived and did so. In fact, the first responder remained in the patrol vehicle answering a cell phone call from a supervisor for a brief period. The officer, in a personal interview, told us that he did not notice the trespassers until they approached the vehicle and "surrendered" to the responder. Even when the officer exited the patrol vehicle, the officer did not move to secure the area, did not draw a weapon, and permitted the trespassers to roam about and retrieve various items from backpacks they had apparently brought into the area adjacent to the HEUMF. The responder also did not protect his weapon, thereby hazarding it to control by the trespassers. When the supervisor arrived on the scene, direction was given to the first responder to cover the supervisor until protective gear could be donned. However, the first responder did not provide cover and continued to look away from the trespassers at other areas of the site.

In addition, an officer stationed inside the HEUMF at a post directly adjacent to the trespassers' point of entry did not properly respond to the intrusion. In direct contrast to established policy, the officer used an unauthorized technology (a pan-tilt-zoom camera) to perform an assessment of the security zone that the trespassers penetrated. The officer did not detect the trespassers even though two members of the group had entered the security zone through a hole the group had cut in the outermost fence of the Perimeter Intrusion Detection and Assessment System surrounding the HEUMF and were in the process of cutting an adjacent fence. At the same time, another officer silenced a local alarm without looking out of a gun port or available viewing glass to assess the situation.

In short, the actions of these officers were inconsistent with the gravity of the situation and existing protocols.

After the arrival of a Protective Force supervisor, the Protected Area Sector Lieutenant ordered a lockdown of the entire Protected Area at Y-12. A number of protective measures were then deployed, including vehicle arrest systems, tactical response teams, and patrols by armored vehicles. Searches for other possible trespassers also commenced.

Maintenance of Security Equipment

Technology features critical to the security of HEUMF and other nuclear related facilities at Y-12 were inoperable and/or not properly maintained. Our inquiry disclosed that both Federal and contractor management officials at the site were aware that a substantial backlog of degraded and/or nonoperational security equipment existed. Gaps between the Department's requirements and NNSA policy for addressing critical security maintenance issues likely contributed to the backlog.

We found that security equipment repairs were not always treated as a priority at Y-12. Inoperative cameras, devices that contributed the delays in assessing alarms and identifying the trespassers in this case, were not considered to be critical security devices by Y-12. Rather, these devices were assigned a priority of "security significant," a rating that permitted repairs to be delayed. At least one other site with a weapons and nuclear material mission, NNSA's Pantex Plant in Texas, had classified cameras as "critical" elements of its security system. We discovered that the Department required that repairs of critical equipment be initiated within 24 hours. However, even if the cameras had been properly prioritized at Y-12, NNSA's policy in this area did not specify repair time requirements.

Although we did not verify the information because of the expedited nature of our review, NNSA Headquarters officials told us that similar NNSA sites appeared to follow the Department's policy in that they had repair rates for critical equipment of less than 24 hours. A senior contractor official at Y-12 told us that critical items were to be repaired within 5-10 days; however, we could not identify regulations/guidance or directives supporting that assertion. The same official later acknowledged that repair timeframes were treated as a goal rather than a requirement. As a consequence, important maintenance actions were significantly delayed and equipment was not returned to service in a timely manner. As it relates to this intrusion, one critical fixed camera that provided coverage of the penetration area had been out of service for approximately 6 months. We found this to be troubling.

Required, periodic testing of security features was also not properly performed. Notably, we learned that when equipment was tested officials only sought to determine that a "feed" was available from the device rather than determining whether all of the device's features were working. In this particular case, it is likely that had one of the device's features been operational, the trespassers would have been detected immediately after entering the security zone surrounding the HEUMF and prior to reaching the facility. When questioned, both security and maintenance told us that they had no idea of how long the feature had been out of service. At least one security officer told us that had this feature been operational, the trespassers would have been detected before they cut the innermost protective fence at the HEUMF.

Federal and contractor officials at Y-12 told us that the cameras had been reclassified as critical security elements within 24 hours of the event and that repairs of all critical equipment had commenced. During our tour of the HEUMF, we observed that the malfunctioning camera and security feature just discussed had been repaired and appeared to be functioning as intended. As a demonstration of the need for continuing vigilance in this area, we noted that a camera repaired after the breach malfunctioned within days of its repair.

Compensatory Measures

Over reliance on the use of compensatory measures to address equipment failures impacted system readiness at Y-12. When questioned as to why action was not taken to address growing maintenance backlogs, Federal officials told us that with the advent of NNSA's contractor governance system (Contractor Assurance System), they could no longer intervene. They contended that as long as the maintenance anomalies were identified and compensatory measures were in place, they could take no action to prompt the contractor to complete needed repairs. In these matters, a compensatory measure is generally defined as an off-setting control such as dispatching an officer to visually assess the situation/inspect an area where a security device had alarmed when the installed technology feature was inoperable. One of these same officials also indicated that they had been instructed not to evaluate and report on "how" the contractors were conducting business, but to focus instead on ensuring that the mission was accomplished. The other Federal official told us that risk management and cost considerations could lead to equipment not being repaired at all, and as a result, cause compensatory measures to become permanent. A senior NNSA Headquarters security official noted that the overuse of compensatory measures, coupled with issues with false alarms, may have led to complacency of the Protective Force and diminished security at Y-12. Our analysis suggested that compensatory measures should be targeted and that, in this particular instance, were not an adequate substitute for critical equipment that is out of service.

Interpretation of Existing Policy

Protective Force officers misinterpreted established policies regarding the use of technology to perform field assessments of alarm activations. NNSA's procedures in this area required that cameras used for such assessments be fixed in position, with fixed length lenses. Established guidance specifically noted that pan-tilt-zoom cameras, installed in a number of areas at Y-12, may only be used for such assessments if in a locked configuration. At least one reason for this distinction is that it may be possible for an adversary to follow the movement of a camera and out-maneuver it to avoid detection. Protective Force officials, however, told us that they believed that it was acceptable to use non-fixed cameras for assessments of security events. In this particular case, the pan-tilt-zoom camera that was used for the event actually revealed an image of the trespassers as they breached security barriers; one that was unfortunately not detected by the officer operating the camera.

Communication

We also observed that several troubling communications deficiencies surfaced during the security breach. As one example, security police officers on the night of the incident incorrectly assumed that trespassers who were beating on the external wall of the HEUMF with a hammer were plant maintenance workers. The officers noted that they were often not alerted to scheduled maintenance, and that workers would appear in the security area outside the facility without warning. According to the officers, the arrival of maintenance workers in the hours of darkness and without warning was not unusual. In comments on a draft of this report, NNSA raised questions about the accuracy of this statement. In response, we contacted the Plant Shift Superintendent’s office for clarification. Officials within the Superintendent's office confirmed that workers such as roofers, utility repair persons and fire personnel performed work early in the

morning. However, they explained there was an established process for work approval which included involvement from Management and Operating (M&O) and Protective Force contractor personnel. Thus, there appeared to be a breakdown in communications on this point that we could not reconcile.

In addition, Protective Force officers were not advised of equipment outages when they assumed watch. Officers told us that they often did not learn of equipment outages until they tried to access the equipment to do a field assessment of a security event. The officers explained that knowing what equipment was non-operational at the time they assume their posts would be beneficial when they were called on to respond to alarm activations.

The Protective Force relied heavily on communication via cell phones rather than radios. Although generally prohibited by site security plans, both the first and second responders to the July 28 intrusion were dispatched via cell phone. Directives, to which site contractors were required to adhere, mandated that the digital, encrypted radio system for the Oak Ridge Reservation was to be used as the primary means of communication by the Protective Force. Confusion regarding these explicit requirements, however, may have existed because the NNSA policy did not specifically indicate that the reservation's radio system was to be the primary means of communication. Use of the radio system permits all members of a group to share information and provides for recording of conversations for subsequent analysis. Conversely, cell phone communication channels are not encrypted and are subject to eavesdropping, a weakness that could result in the disclosure of classified and/or critical security information. In this particular case, the lack of a complete record of vital communication may have adversely impacted management's ability to objectively and comprehensively analyze the events that unfolded on July 28.

Funding and Resource Allocations

Contractor officials expressed concern that constrained Federal funding had negatively impacted security controls at Y-12. For example, NNSA made a decision to eliminate some security features surrounding the HEUMF prior to completion of construction in 2008. Plans to install an additional delaying barrier were abandoned during construction. One official told us that the decision to exclude the delaying/prevention barrier was appropriate because of the security features of the HEUMF. Other officials told us that the feature, in place in the Protected Areas at other sites, was omitted because of budget considerations. The installation of barriers similar to those used in other portions of the Protected Area (as shown in photograph 1) would have complicated, delayed or perhaps even prevented the intrusion by the trespassers.

Photograph 1-Delay Barriers

(Source: NNSA Production Office Public Affairs)

Contractor officials told us that fiscal pressures impacted Protective Force patrols at Y-12. As with the rest of its complex, Y-12 was directed by NNSA in December 2011 to plan for reduced security funding. Headquarters NNSA officials told us that the reductions were primarily being made because of changes in the site footprint and new and enhanced technology. In response, the security contractor eliminated nightly interior patrols and reduced the number of roving patrols. The security contractor had also recently announced its intention to reduce Protective Force personnel levels by 70 people through voluntary and involuntary separations. Protective Force contractor officials indicated that the planned staff reductions were cancelled in response to the recent intrusion.

Officials noted that resources provided for maintenance were not sufficient to ensure that all needs were met. In particular, workers were responsible for maintaining existing facilities as well as completing the installation of technology required for the site's $85 million Security Improvement Program (SIP). Yet, as we were told, there was no increase in staffing levels. Contractor officials noted that maintenance assets were diverted to install security technology components. As a result, corrective maintenance backlogs grew and equipment repairs could not be completed in a timely manner.

Contract Management

NNSA's prime contract structure at Y-12 impeded the integrated management of the safeguards and security function. It also resulted in bifurcated lines of contractor accountability and responsibility. Specifically, NNSA's prime contract with the M&O contractor tasked it with the overall management and operation of safeguards and security activities at Y-12, including physical security systems and systems performance testing. However, Protective Force operations were specifically excluded from the M&O contractor's work scope. Instead, NNSA had a separate prime contract to provide Protective Force staff and training. Thus, physical security systems and security personnel were managed by completely different organizations.

The fractured management structure appeared to have led to conflicting priorities. For example, during implementation of the ongoing Y-12 SIP, the Protective Force contractor told us that it had surfaced a large number of concerns related to implementation of various security features, leading to its recommendation to delay implementation in some cases.

According to the M&O SIP Project Manager, a separate working group comprised of representatives from both the M&O and Protective Force contractors was formed to evaluate the Protective Force's concerns and inform the SIP Project Team of those that needed to be addressed within the project's scope. The working group identified a number of issues it considered to be security significant that required resolution. Nonetheless, the Project Manager determined that many of those issues did not impact the protections of the site's materials and, therefore, should be considered enhancements to be addressed by the M&O contractor's Security Systems group at a later date. The Project Manager was unable to tell us exactly how many items had been addressed at the time of the Y-12 incident.

Federal Oversight

Contractor governance and Federal oversight failed to identify and correct early indicators of the multiple system breakdowns that contributed to the incident. Specifically, since at least 2010, contractor governance reporting systems and Federal oversight efforts indicated that the site's physical security systems were functioning as intended. For example, site office quarterly reports provided to the Defense Nuclear Security Chief indicated positive performance of site physical security systems and the Protective Force. According to senior NNSA officials, the site office quarterly reports were based on the results of the contractors' self assessments. Similarly, NNSA's assessments of the contractor's physical security and Protective Force performance were rated at high levels based on analyses of the quarterly reports. In fact, senior NNSA officials told us that, prior to the recent incident, the site was considered to be one of the most innovative and higher performing sites in the complex. In commenting on a draft of our report, NNSA noted that a performance assessment performed in May 2012 by the Office of Health, Safety and Security indicated that the systems in place facilitated a high probability of detection of intruders. While we do not disagree with this statement, we noted that the review in question involved only the Y-12 alarm system and did not address the entire site security apparatus.

Despite the positive reports provided by the contractor and endorsements from Federal site managers, there were actually a number of known security-related problems at Y-12. For example, maintenance backlogs of critical security equipment were allowed to increase even though the M&O contractor had not performed any analyses to measure the effect of these problems and repair needs on the overall security posture. In particular, we learned that even though both contractor and Federal officials received a daily report of all degraded equipment, they did not perform the evaluations necessary to determine whether the outages, when considered in aggregate, would have impacted security for a significant segment of a facility or area.

As noted in previous OIG Management Challenges reports, Security and Safeguards across the complex warrant special attention by the Department. Our FY 2012 report found that both the OIG and the Government Accountability Office have identified that the Department's extensive Protective Force contingents were not uniformly managed, organized, staffed, trained or compensated throughout the complex. Given the exposure to risk in this area and the reality of the recent situation at Y-12, we believe that heightened and continued focus on Security and Safeguards is necessary.

Favorable Actions

Following the incident, Y-12 and NNSA took a number of actions designed to improve security at the site. For example, Y-12 implemented features designed to help reduce false alarms. Also, NNSA moved the site Protective Force contract from Federal control to the M&O contractor for Y-12. The site began installing additional fortifications around the HEUMF designed to further delay potential intruders. Finally, the NNSA issued a show cause letter to the M&O contractor

directing it to provide information as to why its contract should not be terminated in response to the demonstrated security weaknesses. As previously noted, the site has also initiated and in many cases completed repairs of most critical security equipment.

NNSA officials indicated they are in the process of completing a formal root cause analysis of the intrusion. They expected the report to be available soon and noted their intent to use it to solidify their overall corrective action approach. Finally, an extensive security evaluation, including performance testing, is scheduled to be conducted in the near future to validate the efficacy of corrective actions taken.

Additionally, officials told us that NNSA has recently established the NNSA Production Office (NPO) in order to provide more consistency in the oversight and administration of the Y-12 and Pantex production sites. Further, officials indicated that as a result of the recent security incident, they were reviewing the current oversight model to determine the reasons the governance model did not identify the weaknesses that contributed to the security incident at Y-12. Finally, management informed us that the NPO believed that approval of compensatory measures should have mirrored the process used at Pantex requiring Federal approval of such measures. For that and other reasons, officials were evaluating the process for reviewing and approving compensatory measures at Y-12 and plan to issue improved guidance in the near future.

Impact and Path Forward

The successful intrusion at Y-12 raised serious questions about the overall security approach at the facility. It also suggested that current initiatives to reduce Federal oversight of the nuclear weapons complex, especially as they relate to security functions, need to be carefully considered. Some observers went so far as to express the view that there were security culture problems at Y-12 creating an environment in which the July 28 intrusion could occur.

We perceived there to be a level of confidence in the quality of the Y-12 security apparatus that was unjustified. This may have led to a sense of complacency that was inconsistent with: (1) the unique status, mission and sensitivity of operations at Y-12 and its vital national security role; and, (2) the enormous investment of funds and resources in the security apparatus at the Y-12 complex to ensure its secure operations.

In addition to the issues described in our report, we provided management with additional, detailed information that was not included in our report due to security considerations. Other than pursuing our on-going criminal investigation activities, we plan to monitor the Department's progress in completing its formal root cause analysis of the event. If the situation warrants, we will issue supplementary reports on this matter.

RECOMMENDATIONS

Ironically, the Y-12 breach may have been an important "wake-up" call regarding the need to correct security issues at the site. Given the unprecedented nature of this security event, prompt

and effective corrective actions are essential. In that respect, in addition to the actions recently initiated, we recommend that the Under Secretary for Nuclear Security/Administrator, National Nuclear Security Administration:

1. Verify that all critical security equipment at Y-12 has been repaired and is operational;

2. Provide additional guidance on prioritizing equipment repairs and maintenance, and on the appropriate use of technology and communications protocols;

3. Determine whether critical security resource allocations are sufficient to meet demonstrated requirements;

4. Perform periodic in-depth reviews of contractor's security performance using a risk-based approach;

5. Evaluate the accuracy, quality, and completeness of information provided by contractors as part of the governance system and effect changes as necessary;

6. Clarify the NPO's authority under the governance model;

7. Ensure that NNSA Headquarters officials have full and complete information on the status of Y-12 security operations; and,

8. Prepare a lessons learned report that can be shared across the complex.

We noted that the senior leadership of both the Department and NNSA, recognizing the gravity of the security event at Y-12, has been personally involved in related fact finding and root cause identification efforts, including seeking solutions to any contributing institutional problems. As of the date of issuance of this report, inquiries concerning the July 28 Y-12 intrusion continue at a number of levels, both Federal and contractor. The Department's security apparatus has been charged with conducting a full scope review of the event and related circumstances and, ultimately, evaluating the status of the security posture at other agency facilities.

MANAGEMENT REACTION

NNSA management agreed to implement the report's recommendations. Management outlined a number of corrective actions it had initiated or completed. NNSA also indicated that in light of the problems at Y-12 it was conducting a complex-wide assessment of physical security to identify any corrective measures necessary to protect the Nation's most sensitive nuclear materials.

OFFICE OF INSPECTOR GENERAL RESPONSE

Management's comments were responsive to the report and its recommendations. As noted in the report, we will continue to monitor NNSA's progress in completing its analysis of the event and will issue supplementary reports if warranted.

Attachments

cc: Deputy Secretary
Associate Deputy Secretary
Administrator, National Nuclear Security Administration
General Counsel
Chief of Staff

RELATED REPORTS

- Special Report on *Management Challenges at the Department of Energy – Fiscal Year 2012* (DOE/IG-0858, November 2011). As part of our annual report to identify the most significant challenges facing the Department of Energy (Department), we identified eight challenges and three areas for the "watch list" for Fiscal Year (FY) 2012. Specifically, the report identified contract and financial assistance award management as a management challenge and safeguards and security as an area that warrants special attention from Department officials. We also noted in our report that there may be significant economy of scale cost benefits associated with protective force contract consolidation that could encourage a more uniform and consistent approach to protective force organization, management, training, and equipment purchases.

- Special Report on *Management Challenges at the Department of Energy* (DOE/IG-0844, November 2010). As part of our annual report, we identified seven challenges and placed three areas on our "watch list" for FY 2011. Specifically, we noted that because of the number of contracts handled by the Department and the complexity and importance of the Department's numerous multi-million dollar projects, combined with new challenges created by the American Recovery and Reinvestment Act, contract and financial assistance award management was a significant management challenge. In addition, it was stated in our report that special emphasis on safeguards and security has remained a vital aspect of the Department's mission. In order to faithfully execute its mission of ensuring the safety of the country's nuclear weapons, the Department employs numerous security personnel, protects various classified materials and other sensitive property, and develops policies designed to safeguard national security and other critical assets. Ensuring that these safeguards are both efficient and effective require continuing focus to address this critical challenge.

- Inspection Report on *Y-12 National Security Complex Accountable Classified Removable Electronic Media Program* (INS-L-09-03, March 2009). The inspection was initiated to determine whether Y-12's accountable classified removable electronic media (ACREM) was managed, protected, and controlled consistent with applicable requirements. This review found that an unmarked hard drive had not been properly marked as Secret/Restricted Data and placed into accountability as ACREM, as required, and that 332 metallic flat discs and data tapes located in an ACREM safe may not have been properly controlled as ACREM. Since corrective actions were taken, no recommendations were made; however, we suggested that the Y-12 Site Office take action to ensure timely destruction of unneeded media was accomplished.

- Inspection Report on *Incident of Security Concern at the Y-12 National Security Complex* (DOE/IG-0785, January 2008). This review was initiated because we received an allegation that unauthorized portable electronic devices (including laptop computers) were introduced into a Limited Area which employs physical controls to prevent unauthorized access to classified matter or special nuclear material at Y-12 and that this breach in security was not properly reported. Our inspection substantiated the allegation and identified additional concerns related to the incident. Specifically, we found that Y-12 personnel discovered that an Oak Ridge National Laboratory employee had brought an unclassified laptop computer

into the Limited Area without following proper protocols, the cyber security staff had not properly secured the laptop, the incident was not reported until six days after it was discovered, and as many as 37 additional laptop computers may been improperly introduced into the Limited Area. We made several recommendations to further enhance the security of information systems and responses to incidents of security concern. In response, management identified corrective actions taken, initiated, or planned.

- Inspection Report on *Review of the Department of Energy's Canine Program at Selected Sites* (DOE/IG-0755, January 2007). We reviewed the Canine Programs at selected Department sites to determine whether they provided an adequate level of protection for personnel and facilities. During our inspection, we found that half of the canine teams observed failed the explosive detection portion of the operational evaluation, each of the canines observed failed to respond to at least one of the handlers commands, and the canines were not receiving the minimum number of hours of weekly training for explosive detection that were specified in the contractor's standards. Accordingly, we made recommendations to address the issues and enhance security and the comments and planned actions received were responsive to our recommendations.

- Inspection Report on *Concerns with Security Barriers at the Y-12 National Security Complex* (DOE/IG-0741, October 2006). Because we received an allegation that weapon port openings in newly constructed concrete security barriers at Y-12 were designed without the space required to accommodate the sight system of protective force weapons, we initiated an inspection. During our review, we substantiated the allegation and found that the original measurements of weapon ports in 90 concrete security barriers were undersized and unable to adequately accommodate the sight system on the protective force weapons. The weapon ports were subsequently modified. However, we concluded that based on the timing of the available information, the Protective Force contractor had the opportunity to send information to the managing and operating contractor correcting the sizing specification prior to construction, but failed to do so. Also, we found that the managing and operating contractor received payment of $525,000 for completion of three security upgrades even though two were completed after the date specified in the performance based incentive. We made several recommendations that included recouping amounts paid to the contractors and ensuring the items found in our inspection were addressed.

- Inspection Report on *Security Access Controls at the Y-12 National Security Complex* (DOE/IG-0691, June 2005). We initiated this inspection because we received information that non-U.S. citizens were improperly allowed access to a leased facility at the Y-12 complex. During our inspection we found that 16 foreign construction workers, using false documents, had gained access to the Y-12 site on multiple occasions and that control procedures at Y-12 facilities were not implemented. While we recommended that the Y-12 Site Office ensured that the revised access policy was fully and consistently implemented, we also recommended officials determine actions that may have been warranted Department-wide.

- Inspection Report on *Protective Force Training at the Department of Energy's Oak Ridge Reservation* (DOE/IG-0694, June 2005). This inspection was initiated because we received an allegation that a security police officer was given credit for training that was not received at the Oak Ridge Reservation. The inspection concluded that there were

material shortcomings in the implementation of the protective force training program. Specifically, we found that personnel spent about 40 percent less time on combat readiness refresher training than that specified in the training plan, planned training time was formally reported as actual training time, personnel routinely worked in excess of the maximum threshold for safe operations of 60 hours per week, and personnel signed attendance rosters for training not received. Because of the importance to the Nation's security, several recommendations were made to ensure the protective force is properly trained.

- Inspection Report on *Protective Force Performance Test Improprieties* (DOE/IG-0636, January 2004). The inspection was initiated at the Y-12 Site Manager's request to examine whether there had been a pattern over time of site security personnel compromising protective force performance tests. Our inspection confirmed that the results on a performance test may have been compromised as two protective force personnel were inappropriately permitted to view the computer simulations of four scenarios on the test. In addition, we were provided information that inappropriate actions had occurred going back to the mid-1980s in connection with performance tests at the Department's Oak Ridge complex. NNSA concurred with our findings and recommendations made in our report and provided a series of corrective actions that had been initiated or planned.

MANAGEMENT COMMENTS

Department of Energy
National Nuclear Security Administration
Washington DC 20585
August 28, 2012

OFFICE OF THE ADMINISTRATOR

MEMORANDUM FOR GREGORY H. FRIEDMAN
INSPECTOR GENERAL

FROM: THOMAS D'AGOSTINO
ADMINISTRATOR

SUBJECT: Response to the Inspector General's Special Report on "Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex

As Secretary Chu has made clear, the incident at Y-12 was a completely unacceptable breach of security and an important wake-up call for our entire complex – one we must correct and learn from to assure the absolute protection of this Nation's most sensitive nuclear materials. We have taken swift and decisive action to strengthen security and to replace key personnel, but these steps are just the beginning of the structural and cultural changes that we intend to make.

More specifically, in the days following this incident, the General Manager of the plant along with the leaders of the guard force were removed, and the guards who failed to detect the breach were suspended. Security cameras have been fixed, guard patrols have been increased, and the entire workforce is undergoing additional security training.

We have also issued a notice that requires the Y-12 contractor to show cause why termination proceedings should not be instituted for their management and operations contract for Y-12. We have also taken steps to consolidate responsibility for site operations and security under a single contract, so that there can be no more confusion between contractors about who bears responsibility for maintaining and integrating the physical and human security infrastructure that protects this facility.

We believe this incident raises important questions about the security of Category I nuclear materials across the DOE complex. To that end, we are conducting a complex-wide assessment of the physical security measures, personnel training and procedures, and chain of command to determine any corrective measures that may be necessary to protect this Nation's most sensitive nuclear materials.

We appreciate the timely and important work of the Inspector General in this case, fully endorse and will implement all of the recommendations in this report. Some have been acted on already and I will personally hold our team accountable for implementing the remaining items.

IG Report No. DOE/IG-0868

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report that would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact our office (202) 253-2162.

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://energy.gov/ig

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.