U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

# AUDIT REPORT

## Security Improvements at the Y-12 National Security Complex

DOE/IG-0944

August 2015

**Department of Energy**
Washington, DC 20585

August 28, 2015

MEMORANDUM FOR THE SECRETARY

Greg Friedman

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report: "Security Improvements at the Y-12 National Security Complex"

## BACKGROUND

The Y-12 National Security Complex (Y-12) is a manufacturing facility that plays a vital role in the Department of Energy's nuclear security and weapons enterprise. Activities at Y-12 include retrieving and storing nuclear materials, helping fuel the Nation's naval reactors, and performing complementary work for other Government and private-sector entities. In June 2004, the Office of Inspector General's report on *Management of the Department's Personnel Security and Access Control Information Systems* (DOE/IG-0651) recommended that the Department develop a comprehensive framework for managing and integrating personnel security and access control systems.

In response to the report, the National Nuclear Security Administration (NNSA) indicated that it intended to implement the Argus security system to provide integrated access and physical security controls at Y-12. To help meet its security goals, Y-12 focused its planned Security Improvements Project (SIP) on replacing its aged and obsolete security system with Argus. The project was completed in 2013 at a cost of more than $50 million.

Because of the sensitivity of Y-12 and the material it houses, we initiated this audit to determine whether the complex fully and effectively implemented improvements to meet its security needs.

## RESULTS OF AUDIT

Our review found that the SIP was implemented within the established schedule and budget, and it achieved all baseline requirements. However, we found that the SIP was not scoped or funded to address all Argus implementation issues at Y-12. As a result, while Y-12 spent more than $50 million to upgrade its physical security system, it had not met NNSA's mandate to develop and implement a comprehensive method for managing and integrating the site's security and access control systems. In particular, our review revealed the following:

- Although Y-12 initially identified the need to streamline its physical security environment, we found that officials had not utilized all available Argus functionality to achieve this goal. For instance, Y-12 was only using Argus' Homeland Security Presidential Directive 12 (HSPD-12) technology to manage physical access to approximately 1 percent of the site. In addition, NNSA could not fully fund all available Argus functionality. As a result, Y-12 was forced to rely on its existing Identity Verification System, which could not be integrated with Argus, to provide access control to the rest of the site.

- While the Argus implementation originally proposed to meet NNSA's mandate by updating all security infrastructure components, officials did not replace certain system components, such as the legacy alarm wiring cabinets and sensors. This resulted in compatibility issues and significantly increased the number of false or nuisance alarms that operators received. Alarm station operators told us they were not able to efficiently perform their duties because they had to repeatedly address nuisance alarms.

- Local site map design issues within Argus resulted in various errors that negatively affected the efficiency of Y-12's security and alarm operations. For instance, the system's site-level maps included many unnecessary elements, such as parking lots, which cluttered the visual fields, negatively affecting operator response time and hampering situational awareness. Location labels within the maps were also different from the legacy system information, creating a significant learning curve for the console operators.

NNSA and Y-12 officials encountered a number of challenges that affected the ability to fully implement needed security upgrades. Perhaps one of the most significant challenges was the need for NNSA officials to balance the requirement to install Argus with available resources. This ultimately drove decisions regarding the system's implementation approach and limited the use of HSPD-12 technology to enhance physical access controls throughout the site. However, even within the confines of the effort's funding limitations, we found that management weaknesses existed that contributed, at least in part, to the issues identified with the implementation of the security enhancements. In particular, a lack of effective communication and cooperation between operations personnel and project managers contributed to the identified system issues.

Y-12 officials told us that they gained a better understanding of the shortcomings with their implementation of the Argus system and had initiated steps to achieve full system functionality. In addition, Y-12 hired a team of subject matter experts in 2012 to review its Argus implementation. This team of experts issued a report that identified the need to reengineer certain components of the original installation. While reengineering appeared to be necessary to address existing system shortcomings, such actions will take considerable time and resources. In the intervening period, Y-12's security posture will be challenged by prolonged high rates of nuisance alarms and a series of security processes that are overly complicated.

Site officials indicated that until funding is available and deficiencies in the legacy infrastructure can be addressed, they will continue to compensate for the deficiencies by using additional personnel at significant additional cost. In light of the issues identified, we made several recommendations that, if fully implemented, should aid NNSA and Y-12 in further improving the site's security posture.

MANAGEMENT RESPONSE

Management concurred with the report's recommendations and indicated that corrective actions had been initiated or were planned to address the issues identified in the report. Management's response, planned actions, and estimated timeframe for completion are responsive to our recommendations. Management's comments and our responses are summarized in the body of the report. Management's formal comments are included in their entirety in Appendix 3.

Attachments

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

# AUDIT REPORT: SECURITY IMPROVEMENTS AT THE Y-12 NATIONAL SECURITY COMPLEX

## TABLE OF CONTENTS

**Audit Report**

**Appendices**

## DETAILS OF FINDING

In June 2004, the Office of Inspector General's report on *Management of the Department's Personnel Security and Access Control Information Systems* (DOE/IG-0651) recommended that a comprehensive framework for managing and integrating personnel security and access control systems be developed across the Department of Energy (Department). In response, National Nuclear Security Administration (NNSA) management indicated that the Argus system, which was developed by the Lawrence Livermore National Laboratory, would be the standard system for integrating alarm monitoring and access control at its sites. To meet this mandate, in 2004, the Y-12 National Security Complex (Y-12) focused its Security Improvements Project (SIP) on replacing its legacy alarm system through the implementation of Argus.

Our review found that the SIP was implemented within its established schedule and budget and met all of its baseline requirements. However, the Argus system as installed at Y-12 did not fully meet the site's security needs and, in some cases, had not been effectively implemented. Y-12 spent more than $50 million to upgrade its physical security system; however, the site had not met NNSA's mandate to develop and implement a comprehensive method for managing and integrating the site's security and access control systems. In particular, while the need to streamline the physical security environment had been identified, we found that NNSA was not able to fully fund all available Argus functionality and as such, continued to rely upon a separate system to provide access control to the areas of the site not controlled by Argus. In addition, the use of legacy infrastructure components with Argus resulted in compatibility issues that significantly increased the number of false and nuisance alarms. Furthermore, local system map design and labeling issues resulted in various errors related to the site's security environment that affected operator response time and situational awareness, and affected the efficiency of the site's security and alarm operations.

### Access Control Systems

Although Y-12 had identified the need to streamline its physical security environment, we found that it had not utilized all available Argus functionality. As a result, Y-12 officials maintained a separate system to provide access control to certain areas of the site not controlled by Argus. For instance, even though Y-12 officials required that Argus provide Homeland Security Presidential Directive 12[1] (HSPD-12) functionality, we found that the site was only using this technology to manage physical access to approximately 1 percent of its buildings. In addition, Y-12 upgraded its in-house developed Identity Verification System at a cost of more than $1 million to provide automated access control to areas protecting special nuclear material that were not controlled by Argus. The Identity Verification System could not be integrated with Argus, which resulted in an increased workload for the security console operators. By not implementing an integrated solution, Y-12 not only limited Argus' usefulness as a comprehensive security solution, but also

[1] HSPD-12 required the use of identification that meets the Presidential Directive's Standard for Federal employees and contractors in gaining physical access to federally controlled facilities. The Standard required that identification be (a) issued based on sound criteria for verifying an individual employee's identity; (b) strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) rapidly authenticated electronically; and (d) issued only by providers whose reliability has been established by an official accreditation process.

performed work that was contrary to NNSA's mandate to install an integrated access control and intrusion detection system. Had Y-12 fully implemented the Argus system, the site's security needs may have been more effectively and efficiently met.

### Legacy Infrastructure

Although originally proposed to meet NNSA's mandate by updating all security infrastructure components, Y-12 ultimately did not replace the site's legacy alarm wiring cabinets and other system components (such as sensors) when installing Argus. The legacy alarm cabinets provided the wiring to all alarm sensors controlled by the site's security system. Argus' increased sensitivity as compared to the legacy system resulted in an increase in false or nuisance alarms of nearly 25 percent upon implementation. Steps were taken to reduce the false/nuisance alarm rate subsequent to an intrusion at the site in July 2012. However, our analysis of 27 months of alarm data (May 2012 to July 2014) determined that these types of alarms, on average, accounted for more than 35 percent of those received, assessed, and closed by the alarm station operators on a monthly basis. As such, the operators stated that they were less able to efficiently perform their duties because they were repeatedly distracted by false/nuisance alarms.

NNSA management acknowledged that false and nuisance alarms were driven by the legacy alarm sensors, which were not replaced during the Argus implementation. Management also stated that NNSA continued to replace the sensors that have historically demonstrated a higher false or nuisance alarm rate. We are encouraged by management's efforts in this area and suggest efforts continue to aggressively monitor and reduce alarm rates, to include any ongoing Argus sensitivity issues and replacing system components that are contributing to increased alarm rates.

### System Mapping and Labeling

Local site map design issues within Argus resulted in various errors that negatively affected the efficiency of Y-12's security and alarm operations. For instance, the system's site-level maps included many unnecessary elements, such as parking lots, which cluttered the visual fields, affecting operator response time and situational awareness. Location labels within the maps were also different from the legacy system information, creating a significant learning curve for the console operators. Although management stated that these issues had not been raised prior to placing the system into the production environment, we obtained evidence that concerns were raised as early as June 2011—almost 6 months prior to the start of system transition. In addition, the system owner was provided a list of almost 150 discrepancies in September 2011. One month later, the list had grown to almost 200 issues, 36 of which were deemed to be critical to the system's functionality. However, when the issues were brought to the project manager's attention, they were deferred to be addressed after the transition was complete and the system was in production. Security officials were also asked not to raise the issues at the daily project meetings. Remediation for a number of the issues began after the start of our test work. In particular, the maps were updated to remove many of the unnecessary elements. However, at the time of our review, nearly half of the significant issues had not been resolved.

## Funding and Management Challenges

NNSA and Y-12 officials encountered a number of challenges that affected the ability to fully implement needed security upgrades. According to NNSA officials, the need to balance the requirement to install Argus with available resources ultimately drove decisions regarding the system's implementation approach. In particular, despite NNSA's mandate to install Argus, it only made $80 million available for the project. This decision required reduction of the project's scope to exclude certain infrastructure upgrades such as wiring cabinets and sensors. Replacement of these elements would have allowed installed Argus components to function more effectively. Such decisions also limited the use of HSPD-12 technology throughout the site.

Even within the confines of NNSA's funding limitations, we found that management weaknesses contributed, at least in part, to the issues identified. For example, although NNSA had developed an analysis to identify remaining gaps in upgrading the security posture at Y-12, a detailed plan and schedule for implementing the enhancements had not been developed. In addition, a review conducted by the site identified the need to rework its Argus implementation. The review estimated that approximately $300 million will be needed to fully address the site's security needs and implement Argus as its integrated access control and physical security solution. However, in commenting on our report, NNSA officials stated that the actual cost to fully implement Argus was unknown. Plans, schedules, and cost estimates are critical for ensuring the site's remaining security needs are effectively addressed.

In addition, NNSA developed a *Stakeholders Communications Plan for the Y-12 National Security Complex Security Improvement Project*, which was meant to provide a communication strategy to support effective decision making and exchange of information concerning the project. However, we identified concerns related to a lack of effective communication and cooperation between operations personnel and project managers that contributed to decreased system functionality. For example, some system users asserted that the project's timely implementation was frequently put ahead of system performance, resulting in operating inefficiencies related to system mapping and labeling and false/nuisance alarms. Management stated that trade-offs must be made to balance timely implementation with the significance and impact of issues raised. It acknowledged that some users may have interpreted this as putting timely implementation ahead of performance. While we recognize that timely implementation and system performance can be conflicting objectives, we disagree that the degree of reduced system performance experienced constituted a reasonable trade-off for timely implementation. In either case, the system's performance was so poor that both current project management and a consulting team of subject matter experts determined the need for extensive reengineering. Management and experts concluded that significant additional funds would be required to upgrade the site's security infrastructure, including installation of hardware such as badge readers, cabling, and alarm cabinets. While not all of the team's conclusions were related to issues initially raised by the system's users, they are lessons that should be considered and applied to future upgrades.

## Future Upgrades

As noted, the Y-12 Argus system was not implemented to function as the site's comprehensive access control and security monitoring solution, as required by NNSA.  In late 2012, Y-12 spent nearly $1.3 million for a consultant to review the system's implementation and determine what steps should be taken to ensure that it provided full functionality to the site.  The review determined the need to reconfigure and deploy the system as an integrated security and access control solution with the level of functionality and interaction needed.  For example, much of the Argus system was built upon the site's aging legacy infrastructure, which will need to be modified and replaced to enable the system to fully meet the site's security needs in the most efficient manner.  In the meantime, the system's operators continue to compensate for the system's shortcomings with an already limited workforce.

Prolonged high rates of false or nuisance alarms could lead to morale problems among system operators.  In particular, the site's alarm station operators are charged with receiving, assessing, and providing disposition for alarms received to ensure the protection of Y-12's personnel and materials.  Due to the importance of their role in the overall security mechanism, management must ensure that this group does not become complacent and maintains a high morale.  We recognize the ongoing challenges NNSA faces in implementing Argus at Y-12.  However, given the high importance of the Y-12 mission and in the wake of a physical security incident at the site in 2012, NNSA should aggressively develop and fully implement a plan to achieve that goal and address any remaining issues in this area.

## RECOMMENDATIONS

To help improve the management of physical security, we recommend that the Administrator, National Nuclear Security Administration direct the NNSA Production Office, in conjunction with Y-12 National Security Complex Management, to:

1. Identify, consider, and address all critical security needs not addressed in the Argus implementation through the development and full implementation of comprehensive analyses, plans, schedules, and budgets;

2. Identify, evaluate, and repair or replace all security system components that are contributing to high false or nuisance alarm rates; and

3. Ensure the appropriate dissemination and use of lessons learned, as outlined in this report and in the SIP completion report.

## MANAGEMENT RESPONSE

Management concurred with each of the report's recommendations and indicated that corrective actions had been initiated or were planned to address the identified issues.  For instance, management commented that NNSA and Y-12 officials are working to identify, prioritize, and address the security needs of Y-12 within programmatic constraints.  In addition, management noted that it is taking an active role in monitoring and trending alarm maintenance timelines and associated compensatory measure data to identify and resolve problem areas.  Furthermore, management stated that it will review and consider the findings of this report, along with other lessons learned reports already produced, in any future Argus installations.

## AUDITOR COMMENTS

Management's response, planned actions, and estimated timeframe for completion are responsive to our recommendations.  Management's comments are included in Appendix 3.

# OBJECTIVE, SCOPE, AND METHODOLOGY

## Objective

To determine whether the Y-12 National Security Complex (Y-12) fully and effectively implemented improvements to meet the site's security needs.

## Scope

The audit was performed between January 2013 and August 2015 at Y-12 in Oak Ridge, Tennessee. The audit was limited to a review of security improvement efforts at Y-12. The audit was conducted under Office of Inspector General project number A13TG015.

## Methodology

To accomplish our objective, we performed the following:

- Reviewed applicable laws and regulations pertaining to project management;

- Reviewed applicable standards and guidance issued by the National Institute of Standards and Technology, the Office of Management and Budget, and other applicable Federal laws and regulations;

- Reviewed applicable standards and guidance issued by the Department of Energy (Department), as well as prior reports issued by the Office of Inspector General;

- Obtained documentation from and held discussions with officials from Y-12, the Lawrence Livermore National Laboratory Security and Protection Program, and the National Nuclear Security Administration Production Office to gain an overall understanding of the Argus implementation and the site's ongoing security requirements;

- Interviewed personnel involved with the implementation to understand the Security Improvements Project's life cycle; and

- Reviewed the Argus security system, including the procurement, implementation, and operational status of the system.

We conducted this performance audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Accordingly, we assessed significant internal controls and Y-12's implementation of the *GPRA Modernization Act of 2010* and determined that it had established performance measures for physical security at the site. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We did not solely rely on computerprocessed data to satisfy our audit objective.  We confirmed the validity of data, when appropriate, by reviewing supporting source documents and confirming identified weaknesses with responsible on-site personnel.

Management waived an exit conference.

## PRIOR REPORTS

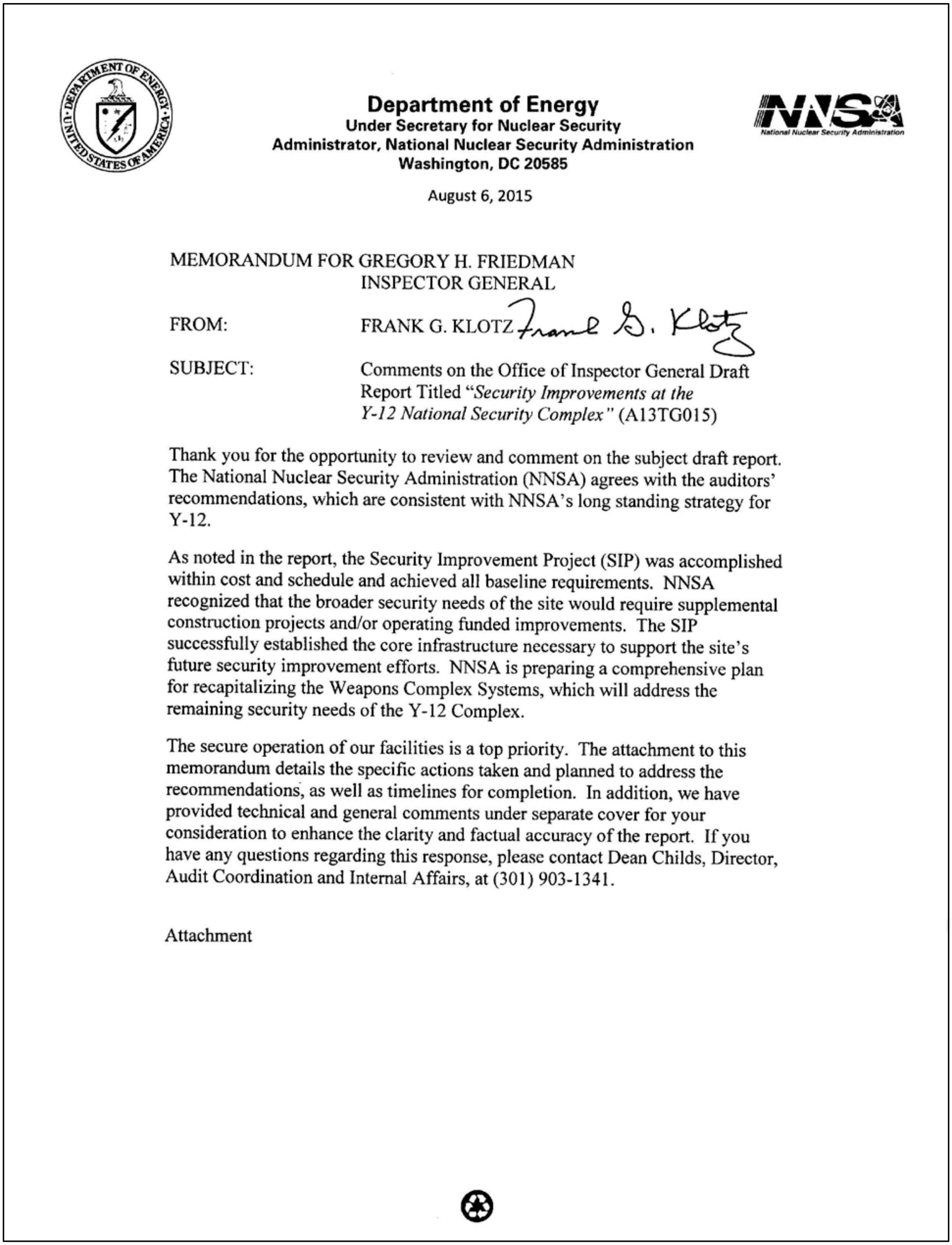
- Audit Report on *Security at the Nevada National Security Site* (OAS-L-15-06, May 2015). During the course of our audit, nothing came to our attention to indicate that security at the Nevada National Security Site was not generally managed effectively. However, we identified an important security infrastructure project that experienced significant schedule delays and cost increases. The project, Argus, is the National Nuclear Security Administration's (NNSA's) recommended enterprise security system, which integrates access control, intrusion detection, and video assessment of alarms to protect and control high-consequence assets. We determined that the Argus project experienced schedule delays and cost increases as a result of inadequate project management and funding issues. NNSA project management officials told us that action has been taken to address the project management issues and that funding for the Argus project has been requested in the fiscal year 2016 budget request.

- Special Report on *NNSA's Management of the $245 Million Nuclear Materials Safeguards and Security Upgrades Project Phase II* (DOE/IG-0901, January 2014). The review found that the Nuclear Materials Safeguards and Security Upgrades Project suffered from a number of project management weaknesses that ultimately resulted in increased costs of as much as $41 million and delayed completion by nearly a year. Specifically, neither NNSA nor the Los Alamos National Laboratory had ensured that work scope was fully and accurately planned; construction contractors were promptly required to correct inferior work; and management systems provided a transparent, clear, and consistent view of the project's schedule and cost performance. Management information systems also failed to provide accurate and complete information about the funds available to complete the remaining work scope.

- Special Report on *Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex* (DOE/IG-0868, August 2012). The inquiry found that the Y-12 National Security Complex security incident represented multiple system failures on several levels. For example, the inquiry identified troubling displays of ineptitude in responding to alarms, failures to maintain critical security equipment, overreliance 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. The security breach occurred because of maintenance issues, overuse of compensatory measures, misinterpretation of established policies, communication deficiencies, constrained Federal funding, and a fractured management structure, including contractor governance and Federal oversight.

- Audit Report on *Management of the Department's Personnel Security and Access Control Information Systems* (DOE/IG-0651, June 2004). The Department's information systems modernization initiatives were not designed in a manner that would adequately address long-standing economy and efficiency issues related to its personnel security and physical access systems.  Specifically, the audit found ongoing system development efforts or management initiatives would not significantly improve the ability of its corporate personnel security system to track visitor site access; reconcile with contractor clearance tracking systems; enable field sites to generate customized reports or increase user system access; eliminate costly development and maintenance of numerous separate, site-level personnel security information systems; and reduce overlapping or redundant physical access control systems that did not communicate with each other, including those at some facilities located in close proximity to one another.  Fulfillment of its long-term objectives in this area were at risk because the Department had not developed a comprehensive framework for modernizing its personnel security and access control information systems and did not always follow sound system development practices.  Absent a coordinated approach, the Department was unlikely to achieve its objective to improve the cost-effectiveness and efficiency of these critical systems.

## MANAGEMENT COMMENTS



**Department of Energy**
**Under Secretary for Nuclear Security**
**Administrator, National Nuclear Security Administration**
**Washington, DC 20585**

National Nuclear Security Administration

August 6, 2015

MEMORANDUM FOR GREGORY H. FRIEDMAN
INSPECTOR GENERAL

FROM: FRANK G. KLOTZ Frank G. Klotz

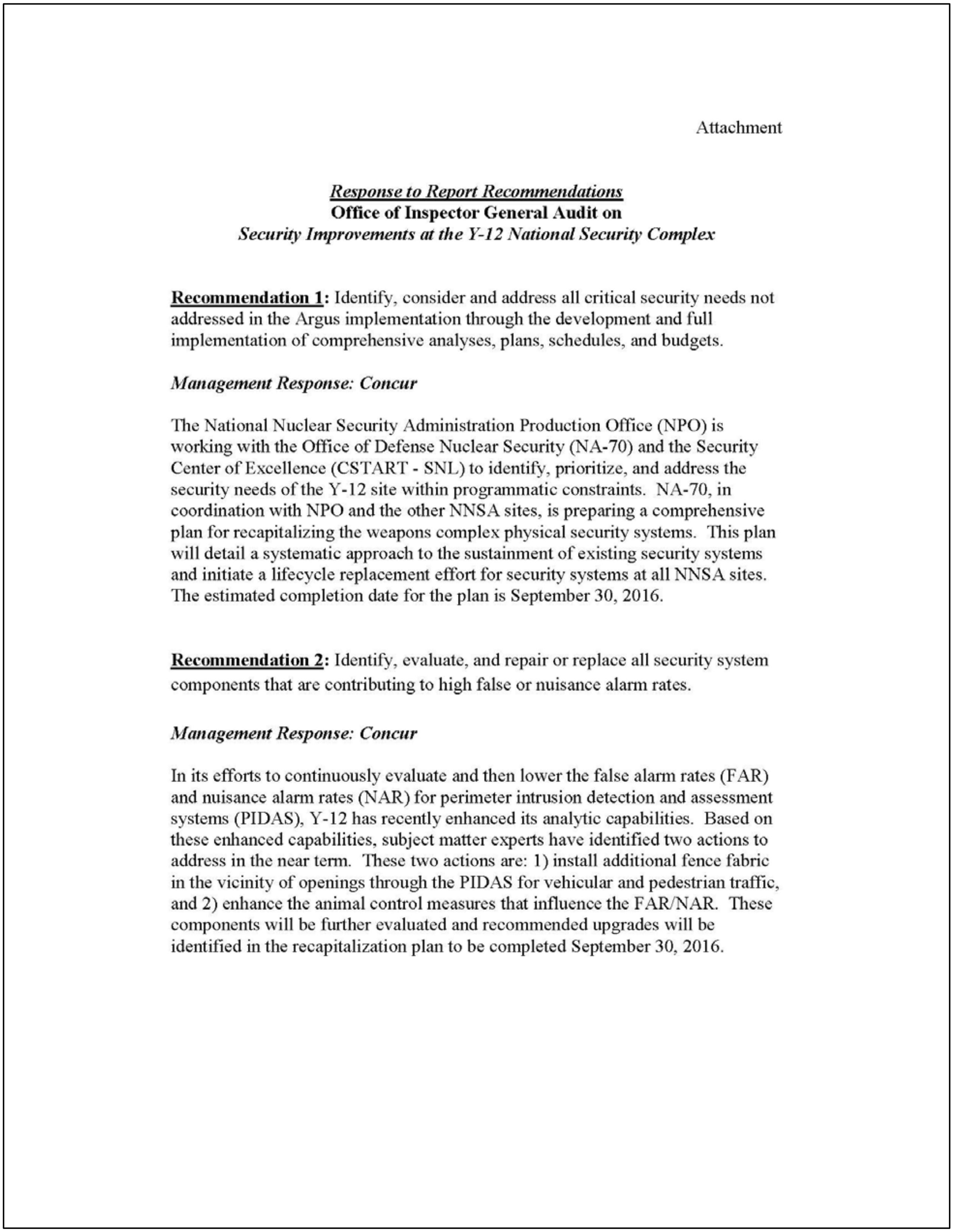
SUBJECT: Comments on the Office of Inspector General Draft Report Titled "*Security Improvements at the Y-12 National Security Complex*" (A13TG015)

Thank you for the opportunity to review and comment on the subject draft report. The National Nuclear Security Administration (NNSA) agrees with the auditors' recommendations, which are consistent with NNSA's long standing strategy for Y-12.

As noted in the report, the Security Improvement Project (SIP) was accomplished within cost and schedule and achieved all baseline requirements. NNSA recognized that the broader security needs of the site would require supplemental construction projects and/or operating funded improvements. The SIP successfully established the core infrastructure necessary to support the site's future security improvement efforts. NNSA is preparing a comprehensive plan for recapitalizing the Weapons Complex Systems, which will address the remaining security needs of the Y-12 Complex.

The secure operation of our facilities is a top priority. The attachment to this memorandum details the specific actions taken and planned to address the recommendations, as well as timelines for completion. In addition, we have provided technical and general comments under separate cover for your consideration to enhance the clarity and factual accuracy of the report. If you have any questions regarding this response, please contact Dean Childs, Director, Audit Coordination and Internal Affairs, at (301) 903-1341.

Attachment



Attachment

***Response to Report Recommendations***
**Office of Inspector General Audit on**
***Security Improvements at the Y-12 National Security Complex***

**Recommendation 1:** Identify, consider and address all critical security needs not addressed in the Argus implementation through the development and full implementation of comprehensive analyses, plans, schedules, and budgets.

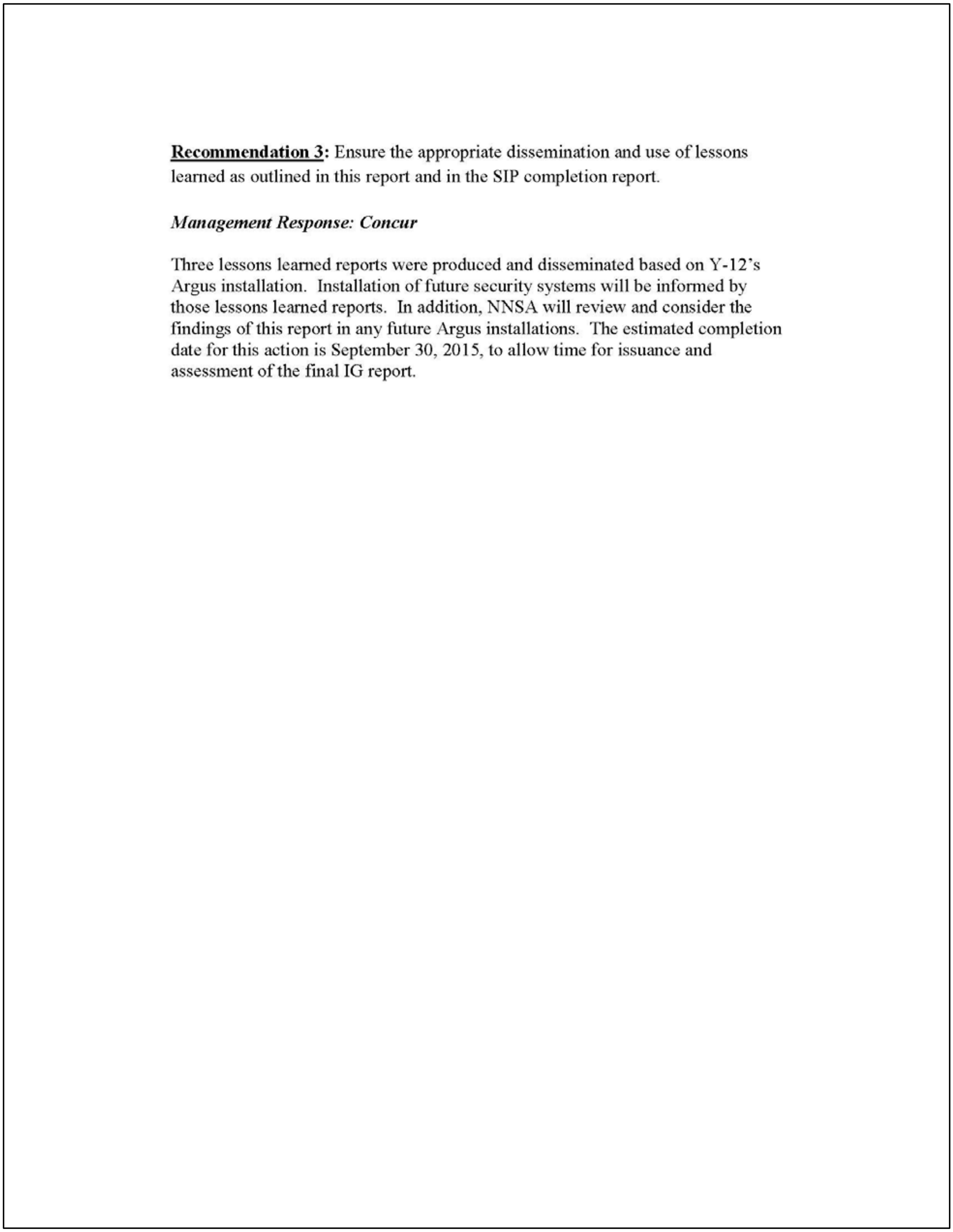
***Management Response: Concur***

The National Nuclear Security Administration Production Office (NPO) is working with the Office of Defense Nuclear Security (NA-70) and the Security Center of Excellence (CSTART - SNL) to identify, prioritize, and address the security needs of the Y-12 site within programmatic constraints. NA-70, in coordination with NPO and the other NNSA sites, is preparing a comprehensive plan for recapitalizing the weapons complex physical security systems. This plan will detail a systematic approach to the sustainment of existing security systems and initiate a lifecycle replacement effort for security systems at all NNSA sites. The estimated completion date for the plan is September 30, 2016.

**Recommendation 2:** Identify, evaluate, and repair or replace all security system components that are contributing to high false or nuisance alarm rates.

***Management Response: Concur***

In its efforts to continuously evaluate and then lower the false alarm rates (FAR) and nuisance alarm rates (NAR) for perimeter intrusion detection and assessment systems (PIDAS), Y-12 has recently enhanced its analytic capabilities. Based on these enhanced capabilities, subject matter experts have identified two actions to address in the near term. These two actions are: 1) install additional fence fabric in the vicinity of openings through the PIDAS for vehicular and pedestrian traffic, and 2) enhance the animal control measures that influence the FAR/NAR. These components will be further evaluated and recommended upgrades will be identified in the recapitalization plan to be completed September 30, 2016.



**<u>Recommendation 3</u>:** Ensure the appropriate dissemination and use of lessons learned as outlined in this report and in the SIP completion report.

***Management Response: Concur***

Three lessons learned reports were produced and disseminated based on Y-12's Argus installation. Installation of future security systems will be informed by those lessons learned reports. In addition, NNSA will review and consider the findings of this report in any future Argus installations. The estimated completion date for this action is September 30, 2015, to allow time for issuance and assessment of the final IG report.

# FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

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