OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

AUDIT REPORT

OAI-L-17-06

May 2017

MAINTENANCE AND TESTING OF INTRUSION DETECTION AND ALARM SYSTEMS

Department of Energy
Washington, DC 20585

May 31, 2017

MEMORANDUM FOR THE MANAGER, NATIONAL NUCLEAR SECURITY ADMINISTRATION PRODUCTION OFFICE
MANAGER, PACIFIC NORTHWEST SITE OFFICE
MANAGER, RICHLAND OPERATIONS OFFICE

FROM: Jack Rouch
Deputy Assistant Inspector General for Audits
Office of Inspector General

SUBJECT: INFORMATION: Audit Report on "Maintenance and Testing of Intrusion Detection and Alarm Systems"

BACKGROUND

The Department of Energy is responsible for some of the Nation's most complex and technologically advanced programs, including cutting edge work in basic and applied sciences, environmental cleanup, and nuclear weapons stewardship. Department Order 473.3A *Protection Program Operations* establishes requirements for the physical security of property and personnel at Department sites, including requirements for intrusion detection and alarm systems. These systems are intended to ensure breaches of security barriers or boundaries are detected and responded to appropriately. Maintenance and testing of these systems is vital to ensure continuous operation. Our Special Report on the *Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex* (DOE/IG-0868, August 2012) identified, among other issues, that periodic testing of security features was not properly performed at that site. Additionally, our Special Report on *Management Challenges at the Department of Energy – Fiscal Year 2017* (OIG-SR-17-02, November 2016) identified Safeguards and Security as one of the top management challenges for the Department.

Given the critical importance of physical security at Department sites, we initiated this audit to determine whether the Department effectively and efficiently managed the maintenance and testing of intrusion detection and alarm systems at selected sites.

RESULTS OF AUDIT

Nothing came to our attention to indicate that the Department had not managed the maintenance and testing of intrusion detection and alarm systems effectively and efficiently at the three sites reviewed. Generally, we found that the sites were in compliance with relevant regulations over

maintenance and testing of their intrusion detection and alarm systems. However, during the course of our review, we identified several opportunities for improvement at two of the three sites we visited. Specifically, at the Hanford Site (Hanford) we found opportunities for improvement related to:

- The collection and analyses of false[1] and nuisance[2] alarm rates (FAR/NAR) data;
- Documentation related to corrective actions taken on failures identified during testing of system elements; and
- The certification process of security system testers.

Additionally, we found that the Pantex Plant (Pantex) could improve its maintenance close-out procedures related to security work orders. Our audit identified no reportable issues at the third site, the Pacific Northwest National Laboratory.

Collection and Analyses of False and Nuisance Alarm Rates

We found that Hanford was not trending FAR/NAR data for all elements of its overall intrusion detection system as required by Department Order 473.3A. Specifically, while Hanford maintains two distinct sets of alarm systems, it was only tracking and analyzing FAR/NAR data for the Alarm Monitoring System that protects special nuclear material and facilities. All other facilities are protected within a separate security system, the Hanford Industrial Security Alarm Monitoring System,[3] (industrial alarms) that had not been subjected to the trending of FAR/NAR data.

FAR/NAR data and analyses are used to determine whether excessive false and nuisance alarms are reducing system effectiveness. For example, these analyses are used to ensure that when established alarm rate thresholds are exceeded, the site takes steps to correct the cause of the false or nuisance alarms. Even though industrial alarms are not in areas considered critical, collecting and analyzing failure and nuisance rates are essential in identifying trends and ensuring overall system functionality and performance. By excluding the industrial alarms from trending, Hanford's overall FAR/NAR site data is incomplete and not being used to ensure that sufficient attention is directed to all false and nuisance alarms, and that steps are consistently taken to address and correct the issues identified. Hanford officials informed us that security force officers can respond to all alarm types, depending on their daily assignments. However, officers could be burdened with high levels of FAR/NAR on the industrial alarms, which may ultimately affect their response to the Alarm Monitoring System alarms for special nuclear material and facilities.

[1] False Alarm: An alarm for which a specific cause is unknown but is not an attempt to defeat the detection system. False alarms can be an indication of electronic malfunction such as component failure, communications failure, loose connections, power faults, or many other issues.
[2] Nuisance Alarm: An alarm generated by a known stimulus such as wind, lightning, rain, animals, human failing to follow system procedures, alarm time-outs on doors, etc., but unrelated to an intrusion attempt.
[3] The industrial alarm monitoring system covers all Hanford facilities, not covered by the Alarm Monitoring System, based on a graded security protection level and designation strategy for each type of asset.

At the time of our site visit, contractor officials indicated they were unaware that the Department requirements for FAR/NAR data collection and analyses included industrial alarms. Subsequently, officials acknowledged they were not in compliance with the regulations and agreed to take immediate action. As a result of our review, Hanford implemented a formalized policy to collect and analyze FAR/NAR data on its industrial alarms. Officials have indicated that since implementing this formalized process, collected and analyzed FAR/NAR data for all alarms are now being presented at monthly security coordination meetings.

Testing Documentation

We also found that Hanford had not documented whether corrective actions had been taken in response to failures identified during testing of security systems. Specifically, while reviewing selected results of Hanford's effectiveness testing, we were unable to make a direct definitive link between an unsatisfactory test result and the subsequent corrective actions taken by site maintenance personnel.

In one instance, we found that the available testing documentation package did not provide sufficient detail on the deficiency or the corrective actions taken to correct it. In this example, we found that the site maintenance log noted that work had been performed on the security system sensor where the deficiency had been identified, but given that the testing documentation package did not include sufficient information consistent with record keeping provisions set forth in Department Order 473.3A, we were unable to make a determination on whether the maintenance work was triggered by the testing failure or a separate work request. Additionally, we noted that subsequent retesting had been conducted on the failed sensor and had produced satisfactory results. While these are positive indicators, because of the lack of documentation linking corrective actions to specific testing failures (as part of the testing process), we could not conclude, nor could Hanford clearly demonstrate that corrective actions had been consistently taken to address and correct all testing failures.

During the course of our review, officials indicated they had not considered the benefit of including this information in their testing documentation because security system testers typically team with security maintenance personnel and issues are immediately corrected or scheduled with a work package for correction. To address this concern, Hanford officials confirmed testing procedures within the Effectiveness Test Program and Security System Testing forms had been revised. Specifically, a field was included on the form to document the Technical Security Work Package number initiated to correct the security system failure identified during the testing process. We believe the revised procedures and testing form should provide the appropriate link between failures identified during testing and the associated corrective actions taken to correct the issue.

Tester Certification

We found that Hanford's security system tester certification process had not been updated to include all elements of the intrusion detection system at the site. Specifically, we identified one issue of a recently implemented system element installed at the site, which was not included within the site's certification process for testers. Hanford utilizes this certification process to

help ensure that security system testers are trained and qualified to perform their assigned work scope. This process aligns with Department Order 470.4B *Safeguards and Security Program* requiring safeguards and security personnel be trained to a level of proficiency and competency that ensures they are qualified to perform assigned tasks and responsibilities. Additionally, even though not required by Department Orders, we noted Hanford's policies and procedures for tester certification on site systems lacked a process for reassessing certifications when new or upgraded security technologies were installed on site. While we did not identify issues with the actual testing performed on the systems, the incomplete nature of the certification process, when new detection technologies are implemented, could hamper Hanford's ability to demonstrate that system testers are adequately trained and qualified to perform their assigned work scope.

We alerted Hanford's security contractor of this identified gap in the system tester certification process. Officials indicated that the policy for tester certification was currently due for revision and agreed with our conclusion. As such, officials took prompt action to update their policies and procedures in an effort to correct this deficiency. Specifically, officials indicated that they had revised Hanford's certification program to include all elements of the intrusion detection system components deployed onsite. Additionally, they added a requirement for security system testers to re-certify on an annual basis. We believe these actions should help ensure Hanford's security system testers are trained and qualified to perform their assigned work scope.

Maintenance Close-Out Procedures

We found that Pantex's Computerized Maintenance Management System contained a backlog of 56 open security-related work orders dating back to 2011, ranging in priority and risk. We found that these work orders remained in the system unnecessarily because Pantex does not have a process in place to ensure that all work orders are closed when work is completed or no longer needed. While these Computerized Maintenance Management System work orders are generally for lower priority security concerns, they are completed by Pantex's site craft shops (electrical, mechanical, etc.) and therefore are competing with other site priorities and resources. Without an accurate depiction of existing maintenance needs, it is difficult for the site to ensure that all work orders have been prioritized appropriately or addressed.

Further, we noted that Pantex officials were unaware of the status of the current backlog; however, after bringing it to their attention, officials reviewed the work orders and determined that, as of September 2016, only 17 of the 56 open work orders were still valid. Specifically, following discussions with individuals that submitted the work orders, Pantex officials determined the remaining 39 orders had been completed, were duplicative of other work orders, or were no longer needed. As a result, these 39 work orders were closed. As of April 2017, officials informed us that three work orders were still considered open. Subsequent to our visit, Pantex officials held a cause analysis meeting and determined that the expectations from site maintenance and individuals requesting work were not clearly understood. As a result, Pantex officials conducted training for these employees to clarify roles and responsibilities to ensure that security-related maintenance work is appropriately prioritized and performed in a timely manner. Additionally, Pantex officials indicated that they will continue to determine the validity of the open work orders noted above.

SUGGESTED ACTION

We recognize and appreciate the prompt action taken by Hanford and Pantex officials to correct the issues we identified. However, while the training provided by Pantex to its employees may help ensure that maintenance work is appropriately prioritized and performed in a timely manner, it may not fully address the management of security-related work orders. We therefore suggest that the Manager of the National Nuclear Security Administration Production Office direct Consolidated Nuclear Security LLC, the contractor responsible for managing Pantex, to develop a formal process to ensure that all Computerized Maintenance Management System security-related work orders are closed when work is completed. Pantex officials agreed a formal process is necessary to ensure that work orders are closed out within the system when work is completed or no longer needed.

Attachments

cc: Deputy Secretary
Chief of Staff

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective of this audit was to determine whether the Department of Energy effectively and efficiently managed the maintenance and testing of intrusion detection and alarm systems at selected sites.

SCOPE

This audit was conducted between March 2016 and May 2017 at Department Headquarters in Washington, DC and Germantown, Maryland; Hanford Site and Pacific Northwest National Laboratory in Richland, Washington; and Pantex Plant in Panhandle, Texas. The audit scope included a review of maintenance and testing activities regarding intrusion detection and alarm systems. The audit was conducted under Office of Inspector General project number A16PT022.

METHODOLOGY

To accomplish our audit objective, we judgmentally selected three Department sites based on several factors including; the size of the sites' security infrastructure, prior report and assessment coverage, and historical alarm rates. Because a judgmental sample of Department sites was used, the results were limited to the sites or locations selected. Additionally, we:

- Reviewed applicable laws, regulations, local policies, and procedures pertaining to the physical protection of interests under the Department's purview;
- Reviewed prior reports and assessments issued by the Office of Inspector General, Office of Enterprise Assessments, and site contractors;
- Held discussions with Department and contractor officials from the Department's Headquarters, Hanford Site, Pacific Northwest National Laboratory, and Pantex Plant concerning the management of intrusion detection and alarm systems;
- Analyzed the Hanford Site, Pacific Northwest National Laboratory, and Pantex Plant's operability and performance testing documentation; and
- Observed and conducted operability and alarm functionality testing on sampled items.

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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed the Department's implementation of the *GPRA Modernization Act of 2010* as it relates to our audit objective and determined that the Department

had not established specific Department-wide performance measures related to the maintenance and testing of intrusion detection and alarm systems. We did, however, identify measures, including goals and objectives which targeted security in general, which would include elements of the maintenance and testing of intrusion detection and alarm systems. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We relied on computer-processed data to achieve our audit objective. We conducted a limited reliability assessment of computer-processed data, which included comparing the data to source documents for accuracy, and we deemed the data to be sufficiently reliable for the purpose of our audit.

An exit conference was held with management officials on May 18, 2017.

PRIOR REPORTS

- Special Report on *Management Challenges at the Department of Energy – Fiscal Year 2017* (OIG-SR-17-02, November 2016). The Office of Inspector General annually identifies what it considers to be the most significant management challenges facing the Department of Energy. The Office of Inspector General's goal is to focus attention on significant issues with the objective of working with Department managers to enhance the effectiveness of agency programs and operations. In 2013, Safeguards and Security was elevated to the management challenges list primarily as a result of the events at the Y-12 National Security Complex, which highlighted the need for a robust security apparatus with effective Federal oversight. Additionally, the Department's management has continually identified issues in this area in its annual memorandums on Assurances of Internal Control. In fact, in its fiscal year 2016 memorandum, one site noted that the aging security alarm system does not provide sufficient functionality to ensure protection. Given the Department's unique mission and the potential catastrophic consequences of a security failure, Department management must ensure the safety and security of the Department's operations.

- 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.

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 OIGReports@hq.doe.gov and include your name, contact information, and the report number. Comments may also be mailed to:

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.