OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

INSPECTION REPORT

OAI-M-17-09

July 2017

ALLEGED TESA ACCESS ISSUES AT LAWRENCE LIVERMORE NATIONAL LABORATORY

Department of Energy
Washington, DC 20585

July 21, 2017

MEMORANDUM FOR THE MANAGER, LIVERMORE FIELD OFFICE

FROM: Michelle Anderson
Deputy Inspector General
For Audits and Inspections
Office of Inspector General

SUBJECT: INFORMATION: Inspection Report on "Alleged Tesa Access Issues at Lawrence Livermore National Laboratory"

BACKGROUND

The National Nuclear Security Administration's Lawrence Livermore National Laboratory (Livermore) is managed and operated by Lawrence Livermore National Security, LLC (LLNS). The Livermore Field Office administers the National Nuclear Security Administration's management and operating contract with LLNS. As a national security laboratory, Livermore has an extensive security infrastructure in place. Livermore's Locks, Keys, and Tesa Group (LKTG) manages the Tesa locks at the site. Tesa locks are electro-mechanical locks that are accessed by inserting a Tesa-encoded card into the lock. Tesa locks can be attached to internal and external doors, or lockboxes to a classified network. A personalized pin may also be required to access certain Tesa locks. LKTG also maintains a Tesa database that is required to contain information on all Tesa locks to which individuals have access at Livermore.

The Office of Inspector General received an allegation that Livermore's Tesa database contained outdated and incorrect data and that this constituted a serious security issue. This incorrect data surfaced after an employee lost his/her Tesa-encoded Livermore Site identification (ID) card in 2014. Specifically, it was alleged that the employee's Tesa locking plan included numerous Tesa locks for which the employee did not have a current need, could not access, or could not locate. We initiated this inspection to examine the facts and circumstances surrounding the allegation.

RESULTS OF INSPECTION

We substantiated the allegation that Livermore's Tesa database contained incorrect data. Of the 63 locks on the employee's locking plan we found:

- 44 Tesa locks for which the employee had no current mission-related need, 5 Tesa locks that the employee was erroneously given access to, and 1 Tesa lock that had been removed from service; and

- 13 locks on the employee's locking plan for Tesa lockbox's related to a classified network account.

A Livermore official told us that any individual that has access to a Tesa lockbox must have an established account to access Livermore's classified network. The employee had an established account to access Livermore's classified network, so he/she had a need for the 13 Tesa lockboxes on his/her locking plan. However, since the employee did not fully complete the lost badge recovery process, LKTG took action to remove the employee's access to 6 of the 13 Tesa lockboxes related to a classified network account. When we discussed this issue with Livermore management, a senior official indicated that this individual's circumstances posed no risk to Livermore's classified network.

Additionally, we found that for 23 of the 85 Livermore employees included in a judgmental sample, information stored in the Tesa database had not been updated in a timely manner or in accordance with Livermore's *Locks, Keys, and Tesa Policy and Procedures* (Tesa Policy).

Livermore's Locks, Keys, and Tesa Process

Livermore's Tesa Policy, which was developed in accordance with Department Order 473.3, *Protection Program Operations*, specified requirements for Livermore's security locks. This policy also establishes the respective responsibilities of LKTG and Tesa custodians, and requires that Livermore's Locks and Keys Program be conducted in a manner that ensures the protection of sensitive information and other valuable assets. Livermore utilizes a graded defense-in-depth protection approach, with multiple layers of security, such as the optional use of a PIN with a Tesa-encoded Site ID card, and the requisite use of a user name and password to access the site's classified network. In addition, a second level of authentication (PIN entry) is required for access to all but the lowest (administrative) level areas within the Livermore Property Protection Areas. We did not test the effectiveness of these additional controls, as it was beyond the scope of our review. However, we determined that when the Tesa-encoded Site ID card was lost by the employee, this may have created a minimal risk to exist for access to low level administrative areas with the Livermore Property Protection Areas during the time required to fully disable access afforded by the lost Tesa card. The time duration for full Tesa card disablement was lengthened by delays in executing the lost badge recovery process.

LKTG is responsible for managing the Tesa database and locking plan components. Tesa locking plans are generated from data in the Tesa database and list all Tesa locks to which an individual has access at Livermore. Each of Livermore's directorates[1] is responsible for adhering to the requirements set forth in the Tesa Policy. To accomplish this, the directorates appoint Tesa custodians responsible for the creation and maintenance of the respective directorate's Tesa locking plans.

[1] Livermore is composed of multiple program offices known as "directorates" (i.e. Weapons & Complex Integration, Computation, Operations & Business, etc.)

Employee's Locking Plan

We found that the employee's locking plan contained 44 Tesa locks for which Livermore could not provide support for a current mission-related need, 5 Tesa locks for which the employee was erroneously provided access, and 1 Tesa lock that had been removed from service.

There were 44 Tesa locks at 3 different directorates for which Livermore could not support a current mission-related need. According to a Livermore official at one directorate, the two previous Tesa custodians at that directorate were no longer employed at Livermore and no previous records were available to support a current mission need to access 41 of the 44 Tesa locks. Additionally, Livermore officials could not provide us a mission-related need for the employee to access these areas at the time the employee's Site ID card was lost. A Livermore official at another directorate stated that the employee had previously worked on a project that required access to 1 of the 44 Tesa locks, but had no current mission-related need to access the lock. For the two remaining Tesa locks located at the third directorate, a Livermore official informed us the employee had not been involved in work there since 2010 and that there was no apparent need for the employee to have access to these Tesa locks. Furthermore, this official stated that the employee's access would likely be removed in the near future.

In addition, the employee was erroneously given access to five Tesa locks located in another directorate. According to the locking plan, four of these Tesa locks belonged to external doors and one to an internal door. The employee informed us that he/she had never required access to this directorate. A Livermore official informed us the employee may have inadvertently been given access to these five Tesa locks because the employee's name was similar to another employee who was supposed to have access. We confirmed that LKTG removed these locks from the employee's locking plan as of August 12, 2014. However, we concluded that the employee unknowingly had unauthorized access to these five Tesa locks for approximately 3 years. We noted that these errors were not identified or corrected as the result of any review process, and that the employee's unauthorized access to these locks was only removed because the employee did not insert his/her replacement Site ID in the locks during the badge recovery process. The badge recovery process consists of inserting a replacement badge into each Tesa lock on an employee's locking plan, which deactivates the employee's lost badge in the Tesa lock. This process helps mitigate the risk of unauthorized use.

Finally, we were told that one Tesa lock on the employee's locking plan was physically removed from service in October 2011. An LKTG official told us that LKTG personnel were again informed that the lock had been physically removed when the lock was belatedly turned into LKTG in October 2014. We noted that the Tesa lock was not actually deleted from the Tesa database until after our fieldwork brought this omission to LKTG's attention. On January 12, 2015, LKTG personnel deleted the lock's file from the Tesa database, more than 3 years after we were told that the Tesa lock was physically removed from the door. At the time of the lock's deletion, the Tesa database listed this lock as being active on the locking plans of over 500 Livermore personnel.

Tesa Database Issues

To determine whether the updating issues experienced by the employee also occurred with other employees, we selected a judgmental sample that included employees who lost a Tesa-encoded Site ID card, had a change in status, or received Access Denial Orders. Similar to losing a Site ID card, the additional events should have triggered an update to the Tesa database and the corresponding locking plans.

For 23 of the 85 Livermore employees included in our judgmental sample, information stored in the Tesa database had not been updated in a timely manner, or in accordance with Livermore's Tesa Policy. According to Livermore's Tesa Policy, Livermore's Protective Force Division must provide copies of its incident reports to LKTG personnel when Tesa-encoded badges are reported lost or stolen. LKTG's badge recovery process includes inserting a replacement badge into all Tesa locks on the employee's locking plan. Also, individuals document completion of the badge recovery process by providing LKTG with a signed and dated copy of the Tesa locking plan indicating that the newly encoded replacement badge has been inserted into all the Tesa lock locations. LKTG officials described this badge recovery process as a risk mitigation measure and explained that inserting a replacement card into the Tesa locks deactivates the lost card, thereby mitigating the risk of unauthorized use. The badge recovery process should be completed within 3 working days of a Tesa-encoded badge being reported lost or stolen. Further, the Tesa Policy states that LKTG is responsible for ensuring prompt notification to affected Tesa custodians of an individual's change in security clearance, lost/stolen locks, keys, or Tesa-encoded badges. In addition, LKTG must complete Tesa database checks for employee separations, transfers, downgrades of security clearance, or Access Denial Orders. Tesa custodians must also ensure removal of an individual's access to Tesa locks when notified by LKTG of Access Denial Orders, separations, transfers, when the need-to-know is no longer valid, or when there is a security clearance downgrade. Individuals with Access Denial Orders are normally not permitted to be badged and are not allowed physical site access.

Based on data obtained from the Livermore Electronic Access Portal[2], we identified a universe of employees that lost their Site ID cards, received an Access Denial Order, or who experienced modifications to their security clearance status during the fiscal years 2011 through 2014. These three high risk subsets from this universe for review consisted of: 29 employees that lost a Site ID card; 23 employees who experienced modification to the security clearance status; and 33 employees that received Access Denial Orders during fiscal years 2011 through 2014. We then compared this data to historical information from the Tesa database, provided by LKTG. Our analysis of this information identified the following issues:

- For 8 of the 29 employees who lost a Tesa-encoded Site ID card, more than 3 working days elapsed between the loss of the Site ID card and the employee's completion of the lost badge recovery process. For those with more than 3 elapsed working days, the average was 14 working days, after adjustment of an outlier of 830 working days.

[2] The Livermore Electronic Access Portal is a software application that provides clearance and badging services to Livermore. The Livermore Electronic Access Portal also provides the ability for programs to submit requests electronically for access (badge) requests, clearance justifications, etc.

- For 8 of the 23 employees subject to the termination, reinstatement, and/or extension of Q-level security clearances, either no action was taken to update the Tesa database or updates were delayed between 6 and 40 days.

- For 7 of the 33 employees who received Access Denial Orders, either the Tesa database was not updated or a significant number of days elapsed between the Access Denial Orders creation date and the disabling/deletion of the employee's Tesa user records in the Tesa database. The average elapsed days was 112 calendar days, after adjustment of an outlier of 1,009 calendar days.

In reviewing a draft of this report, we met with Livermore Security Organization representatives and reached agreement on the specific facts and circumstances for these areas of concern.

Contributing Factors and Impact

The Tesa database contained outdated and incorrect data because Livermore did not always accurately maintain its employee's Tesa locking plans within its areas of responsibility. The non-mission-related Tesa locks on the employee's locking plan, and the additional Tesa database issues from our sample existed because Livermore did not always have adequate controls in place to ensure that Tesa locks were removed from the employee's locking plans when the mission-related need ceased.

The Tesa locking plan reviews required by some directorates' programmatic guidance either were not performed or failed to identify that the employee no longer had a mission-related need for access to multiple Tesa locks. Specifically, one directorate promulgated a directorate-specific Security Plan that required an annual review of Tesa locking plans, but we ascertained that these annual reviews were not performed. Similarly, another directorate established its own Tesa procedure and a related Access Control Policy, both of which required an annual review and update of its Tesa locking plans; however, as previously noted, this review did not identify that the employee no longer had a mission-related need to access these Tesa locks. Although one other directorate had an established Tesa procedure in place, our review of this procedure did not indicate a requirement for an annual review of Tesa locks. However, a Livermore official at this directorate said while Tesa lock reviews are accomplished, the reviews are not documented.

Furthermore, the Livermore Field Office did not provide the level of oversight and review necessary to ensure the accuracy of information in the Tesa database. As the cognizant security authority at Livermore, the Field Office was required by Department Order 470.4B, *Safeguards and Security Program*[3], to conduct surveys to provide assurance that safeguards and security interests and activities were protected at the required levels. Department Order 470.4B also requires that: (1) the Field Office evaluate Livermore's performance assurance programs; (2) Livermore conduct self-assessments of all applicable facility safeguards and security program elements in order to ensure that the objectives are met; and (3) Livermore document the results

[3] DOE O 470.4B stipulates that reports of surveys, self-assessments, and review activities at a Government-owned facility must be maintained in accordance with Department Administrative Records Schedule 18, N1-434-98-2, until 75 years after the discontinuance of the facility.

of performance assurance program testing to provide an audit trail for performance assurance activities and reports. We were informed by a Field Office official that the Field Office had not performed any reviews related to Livermore's Tesa locks, locking plans, or the Tesa database. However, Livermore's self-assessments identified issues with Tesa access at some directorates, but these issues were identified as "observations" rather than "deficiencies," and a Field Office official informed us "observations" were not tracked for follow-up by the Field Office. A Field Office official told us that Livermore's planned self-assessments are factored into the Field Office's overall risk assessment process. We were informed that observations were usually not elevated for further action. In addition, at least one Livermore directorate informed us supporting documentation for the self-assessments was not available. We were informed that the documentation for the self-assessments was supposed to have been provided to the Field Office to satisfy the requirements of Livermore's performance assurance program, and factored into Livermore's performance evaluation reports. Our review of Livermore's performance evaluation reports for fiscal years 2011 through 2014 determined that Livermore received ratings that ranged from *Good* to *Very Good* for all security topical areas.

The existence of incorrect data in the Tesa database could have placed sensitive information and other valuable assets protected by Tesa locks at risk of theft and loss. In addition, according to an email from LKTG, as a result of the employee's failure to complete the lost badge recovery procedure, LKTG removed the employee's access to a number of Tesa door locks and lockboxes. The email stated that the employee had created a vulnerability by failing to complete the required actions. The email also directed Tesa custodians to update these Tesa locks. As previously noted, inserting a replacement card into the Tesa locks deactivates the lost card, thereby mitigating the risk of unauthorized use. The fact that LKTG personnel did not update the Tesa database for nearly 3 years to reflect one particular Tesa lock's removal may have at a minimum demonstrated a non-compliance with policy and procedures. Moreover, due to inadequacies in Livermore's performance assurance activities, management may not have been able to provide assurance that the Department's interests and activities were protected at the required levels.

By not adhering to the Tesa Policy, Livermore may not be able to provide reasonable assurance that sensitive information and other valuable assets are fully protected. Therefore, we made several recommendations to the Manager, Livermore Field Office, designed to address our findings and enhance the protection of Government assets and the security at Livermore.

Other Matters

We observed a number of internal and external doors equipped with Tesa locks that were not associated with areas containing sensitive information or other apparent valuable assets. In fact, we observed that the internal and external doors in these areas were unlocked during business hours so that the use of a Site ID card to gain access through a Tesa lock was not needed at those times. We were told by a Livermore official that the need for the type of lock, and the hours the lock is operational, was at the discretion of each individual directorate; however, all such determinations must remain within the bounds of Department Order requirements and guidance.

Although an assessment of Livermore controls over the deployment of Tesa locks was beyond the scope of our review, we are concerned that the use of Tesa locks in areas without sensitive

information or valuable assets may result in employees being less aware of the importance of the proper use of the locks in areas where they are needed. As stipulated in Department Order 473.3, the lock and key program is to be applied in a manner based on the safeguard and security interests being protected.

RECOMMENDATIONS

We recommend that the Manager, Livermore Field Office, take action to:

1. Implement a policy/procedure with controls to ensure that Livermore's directorates maintain updated and accurate Tesa lock accesses for its responsible area(s);

2. Implement a policy/procedure to ensure that the Field Office incorporates a Federal review of Tesa-related issues into its future surveys, oversight activities, and evaluations of the site's performance assurance programs;

3. Ensure that documentation in support of Livermore's Performance Assurance Program testing is maintained in a manner sufficient to provide an audit trail for performance assurance activities and reports; and

4. Ensure that Tesa locks are deployed in areas with sensitive information or other valuable assets in a manner that is consistent with the safeguard and security interests being protected.

MANAGEMENT RESPONSE

Management concurred with the report's recommendations and indicated that Livermore has already made process and internal control improvements to include more timely notification of badging actions; more frequent and in-depth reviews conducted by the Tesa Database Administrator; and more stringent follow-up on completing the lost badge recovery process. In addition, Livermore has additional actions planned to address the report's recommendations, as well as timelines for completion.

INSPECTOR COMMENTS

Management's comments are responsive to our recommendations. Management stated that Livermore plans to complete a revision to the Locks, Keys, and Tesa Policy and Procedure, the Performance Assurance Program Plan, and conduct an analysis of the deployed Tesa locks to include data on the sensitivity levels of protected assets by December 31, 2017. In addition, Management stated that Livermore will develop a policy/procedure to incorporate a review of Tesa related issues into Livermore's Integrated Assessment Plan and security oversight activities by August 31, 2017. Management's comments are included in Attachment 3.

Attachments

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

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The Office of Inspector General received an allegation that the Lawrence Livermore National Laboratory (Livermore) Tesa database contained outdated and incorrect data and that this constituted a serious security issue. This incorrect information surfaced after an employee lost his/her Tesa-encoded Livermore Site identification card in 2014. Specifically, it was alleged that the employee's Tesa locking plan included numerous Tesa locks for which the employee did not have a current need, could not access, or could not locate. We initiated this inspection to examine the facts and circumstances surrounding the allegation.

SCOPE

This is an allegation-based inspection received by the Office of Inspector General in August 2014. Our inspection was performed from October 2014 through July 2017 at Livermore in Livermore, California. Our fieldwork included a review of Livermore's Locks and Keys Program and pertinent records from Livermore's Tesa database from fiscal years 2011 through 2014. The inspection was conducted under Office of Inspector General project number S15IS002.

METHODOLOGY

In order to accomplish the objective, we performed the following:

- Interviewed the complainant;
- Reviewed previous audits, inspections, and other related reports on this subject area;
- Performed background research on all applicable Department of Energy and National Nuclear Security Administration rules and regulations on the Locks and Keys Program;
- Conducted interviews with Livermore, Livermore Field Office, and contractor officials;
- Reviewed Livermore and Livermore Field Office policies and procedures related to the Locks and Keys Program;
- Reviewed Livermore management and operating contract;
- Obtained briefings and presentations from Livermore officials regarding Livermore's Locks and Keys Program; and
- Analyzed historical data from Livermore's Tesa database, and performed judgmental sampling.

We conducted this allegation-based inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Those standards require that we plan and perform the inspection to obtain sufficient, appropriate evidence to provide a reasonable basis for our conclusions and observations based on our inspection objective. We believe the evidence obtained provided a reasonable basis for our conclusions and observations, based on our inspection objective. Accordingly, the inspection included tests of controls and compliance with laws and regulations to the extent necessary to satisfy the inspection objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our inspection.

We relied on computer-processed data, to some extent, to satisfy our objective related to Tesa lock access. We confirmed the validity of such data, when appropriate, by conducting interviews and reviewing source documents.

Management waived an exit conference on June 12, 2017.

RELATED REPORTS

Office of Inspector General Reports:

- Inspection Report, *Reporting of Security Incidents at the Lawrence Livermore National Laboratory*, (DOE/IG-0625, November 2003). The report concluded that Livermore National Laboratory (Livermore) did not have adequate internal controls to ensure that: (1) security incidents involving missing master keys and Tesa cards were reported within required timeframes, and (2) timely follow-up actions were taken to identify and address any potential security vulnerabilities resulting from the incidents. The report recommended that the National Nuclear Security Administration Administrator ensure that field site security surveys and self-assessments include a review of internal controls relating to the issuance, receipt, and inventory of all keys involving sensitive areas.

- Inspection Report, *Security Clearance Terminations and Badge Retrieval at the Lawrence Livermore National Laboratory*, (DOE/IG-0716, January 2006). The report concluded that Livermore's internal control structure was not adequate to ensure that security badges were retrieved at the time of employee departure or that security clearances of departing employees were terminated in a timely manner. The report recommended that the Livermore Site Office Manager ensure that internal controls are established for the: timely recovery of badges of terminating employees; completion of Security Termination Briefings; completion of Security Termination Statements; and notification to the Department of Energy when security clearances should be terminated. In addition, Livermore officials should improve internal controls such that all security clearances are terminated in the official Livermore database in a timely manner. Several other recommendations were made to the Livermore Field Office Manager designed to address the Office of Inspector General's findings and to enhance security at Livermore.

Government Accountability Office Reports:

- Government Accountability Report, *Better Oversight Needed to Ensure That Security Improvements at Lawrence Livermore National Laboratory Are Fully Implemented and Sustained*, (GAO-09-321, March 2009). The report concluded that weaknesses in Livermore's self-assessment program and Livermore Site Office's[4] oversight contributed to security deficiencies at Livermore. Livermore's security self-assessment program and the Livermore Site Office's annual security survey failed to identify numerous security deficiencies. Livermore Site Office's September 2007 security survey gave Livermore 100 percent satisfactory ratings in its security performance—differing markedly from the security performance the Department observed during its inspection a short time later. The Government Accountability Office recommended (1) the development of a detailed plan and budget for training the National Nuclear Security Administration's Livermore Site Office security staff, and (2) the provision of financial incentives to Livermore's contractor to sustain security improvements.

[4] Subsequent to the issuance of the Government Accounting Office Report, the name of the office changed from the Livermore Site Office to the Livermore Field Office.

MANAGEMENT RESPONSE

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

April 14, 2017

MEMORANDUM FOR APRIL STEPHENSON
ACTING INSPECTOR GENERAL

FROM: FRANK G. KLOTZ FKlotz 4/14/2017

SUBJECT: Comments on the Office of Inspector General Draft Report Titled *Alleged Tesa Access Issues at Lawrence Livermore National Laboratory* (NNSA-2017-000501/S15IS002)

Thank you for the opportunity to review and comment on the subject draft report. NNSA concurs with the findings and recommendations, recognizing that the issues identified were based on records that are now at least three years old, and more recent actions to strengthen controls have not been referenced in the report.

Since the start of the inspection in fiscal year 2014, Livermore has made process and internal control improvements including more timely notification of badging actions; more frequent and in-depth reviews conducted by the Tesa Database Administrator; and more stringent follow-up on completing the lost badge recovery process. The attachment to this report details the additional actions planned to address the report's recommendations, as well as timelines for completion. If you have any questions regarding this response, please contact Mr. Dean Childs, Director, Audits and Internal Affairs, at (301) 903-1341.

Attachment

Attachment

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Response to Report Recommendations

Alleged Tesa Access Issues at Lawrence Livermore National Laboratory (S15IS002)

The Office of Inspector General recommended that the Manager, Livermore Field Office:

Recommendation 1: Develop a policy/procedure with controls to ensure that Livermore directorates maintain updated and accurate Tesa lock accesses for its responsible area(s).

Management Response: Concur

The Lawrence Livermore National Laboratory Security Organization will revise the *Locks, Keys, and Tesa Policy and Procedure*, to include more rigorous processes for ensuring that Directorates maintain updated and accurate Tesa lock accesses for its responsible areas. These updated processes will include periodic reviews of Tesa locking plans and user profiles with follow-on Tesa database alterations. The estimated completion date for this action is December 31, 2017.

Recommendation 2: Develop a policy/procedure to ensure that the Livermore Field Office incorporates a Federal review of Tesa-related issues into its future surveys, oversight activities, and evaluations of the site's performance assurance programs.

Management Response: Concur

The Livermore Field Office will develop a policy/procedure that incorporates a review of Tesa related issues into our Integrated Assessment Plan and security oversight activities. The estimated completion date for this actions is August 31, 2017.

Recommendation 3: Ensure that documentation in support of Livermore's Performance Assurance Program testing is maintained in a manner sufficient to provide an audit trail for performance assurance activities and reports.

Management Response: Concur

The Lawrence Livermore National Laboratory Security Organization will revise the *Performance Assurance Program Plan* to stipulate that all assessments (including those related to the management of Tesa locks) must be executed with the appropriate scope and depth to provide a true measure of the system state, and that all supporting

documentation must be maintained. The estimated completion date for this action is December 31, 2017.

Recommendation 4: Ensure that Tesa locks are deployed in areas with sensitive information or other valuable assets in a manner that is consistent with the safeguard and security interests being protected.

Management Response: Concur

The Lawrence Livermore National Laboratory Security Organization will conduct an analysis of the deployed Tesa locks to include data on the sensitivity levels of protected assets. The analysis will provide conclusions for the appropriateness of currently deployed Tesa locks, with an exploration of the benefits and costs of alternative security mechanisms. The estimated completion date for this action is December 31, 2017.

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.