OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

SPECIAL REPORT

OIG-SR-17-05 June 2017

THE OFFICE OF ENTERPRISE ASSESSMENTS TESTING INCIDENT AT THE 2016 DEPARTMENT OF ENERGY CYBER CONFERENCE

Department of Energy
Washington, DC 20585

June 15, 2017

MEMORANDUM FOR THE SECRETARY

FROM: April G. Stephenson
Acting Inspector General

SUBJECT: INFORMATION: Special Report on "The Office of Enterprise Assessments Testing Incident at the 2016 Department of Energy Cyber Conference"

BACKGROUND

The Department of Energy's Office of Enterprise Assessments is responsible for conducting independent assessments on behalf of the Secretary and Deputy Secretary in the areas of nuclear and industrial safety and cyber and physical security. Within the Office of Enterprise Assessments, the Office of Cyber Assessments evaluates the effectiveness of cybersecurity policy throughout the Department, as well as program and site office performance as it relates to implementation of cybersecurity programs. Assessments can be announced or unannounced and typically include a programmatic cybersecurity policy review in conjunction with technical performance testing. Announced testing is coordinated with the organization being tested and conducted as part of a scheduled appraisal activity. Unannounced tests, also known as red team exercises, are conducted without informing the site but are required to include coordination with a trusted agent. Due to the potential operational impacts, assessments must be carefully and thoroughly conducted and coordinated.

The Office of the Chief Information Officer (OCIO) recently sponsored the Department's 2016 Cyber Conference, held at a non-Federal facility located in Atlanta, Georgia. During the conference, the Office of Cyber Assessments conducted an unannounced assessment related to the use of mobile device charging stations. Officials indicated that the purpose was to determine whether conference participants would connect government and/or personal devices to a charging station. Due to concerns raised by various Department officials related to the Office of Cyber Assessments' lack of coordination with the OCIO prior to the assessment, the Office of Inspector General initiated a special inquiry to determine the facts and circumstances surrounding the assessment.

RESULTS OF INQUIRY

Our review of the cyber conference testing incident substantiated concerns that the assessment had not been appropriately coordinated with the OCIO. We also identified issues related to the

resulting response by OCIO officials. Although they participated in planning the conference, we found that the Office of Cyber Assessments had not taken appropriate planning and coordination steps when conducting its security assessment during the Department's 2016 Cyber Conference. Specifically, we found that Office of Cyber Assessments officials placed two data collection devices disguised as charging stations outside the conference exhibit hall just prior to commencement of the conference, without coordination with any individual responsible for planning or hosting the conference. In addition, once discovered, OCIO officials may not have taken the appropriate steps in responding to the identification of the uncoordinated devices. While it was ultimately determined that the devices were not malicious, did not pose a risk to the conference attendees, and no data was collected during the conference, we are concerned about the lack of coordination among Department elements and the related OCIO response to the potential threat that such devices could have posed. While not specifically addressing the operations related to the Department's 2016 Cyber Conference, a review conducted in November 2016 by the Associate Deputy Secretary found that the Office of Enterprise Assessments acted within its authorities.

Placement of Data Collection Devices

We found that as part of an unannounced assessment, the Office of Cyber Assessments had used data collection devices that were disguised as mobile device charging stations and intended to collect specific, non-sensitive information from devices (such as cell phones) connected to them. In particular, the assessment included the placement of two white acrylic boxes with Department stickers and DOE Cyber Conference "Charging Station" labels outside the conference exhibit hall prior to the start of the conference. Inside each charging station was a computer that was programmed by Office of Cyber Assessments personnel to collect limited data from any connected devices. To avoid the collection of personally identifiable information, the data collected, as verified in an Integrated Joint Cybersecurity Coordination Center (iJC3) report, was limited to device name, serial number, manufacturer, and model number. Officials stated that the intent was to compile statistics, such as the number of unique connections, for presentation during a conference session to raise awareness about potential threats. Although Office of Enterprise Assessments officials noted that contact information was included inside of the devices, in light of the potential for physical threats, we are concerned that an individual would have had to tamper with the suspicious devices to learn of their origin.

Figure 1: "Charging Station"

Contrary to the Office of Enterprise Assessments' internal procedures, we found that the assessment was not coordinated with OCIO or conference planning personnel prior to the

conference. Although Office of Enterprise Assessments officials indicated that the assessment was discussed with the Department's Chief Information Security Officer prior to the conference, the Chief Information Security Officer commented that he was not made aware that testing would occur. The Office of Cyber Assessments indicated that it did not consider this activity to be an unannounced assessment and did not follow established procedures. However, our review of documentation provided by the program indicated that the effort was a red team exercise, which should have been considered an unannounced assessment. The devices were discovered by a conference planning representative, hired by the OCIO, within hours of being placed in the conference area. Once notified, OCIO management directed the removal of the devices from the publicly accessible conference space. At the direction of OCIO officials, the devices were stored in the facility's conference planning office until they were transferred to an alternate storage location by facility staff the next morning. Following their transfer, Office of Cyber Assessment personnel contacted the conference planner to reclaim the devices. Shortly thereafter, OCIO management and Office of Cyber Assessments personnel met to discuss the incident and the devices were returned to the Office of Cyber Assessments.

In preliminary comments on our report, OCIO management indicated that there was no discussion or agreement with the Office of Cyber Assessments regarding further testing. Although Office of Cyber Assessments personnel believed they were authorized to resume testing, OCIO personnel stated the devices were returned only for use in a private conference session. However, that evening assessment officials placed the devices back into the same public conference space from which they had been removed. Within approximately 30 minutes, a conference planning representative once again identified the devices in the area and notified management. OCIO management directed the removal of the devices and initiated an incident response process. While we were not present during the conversations between management officials and could not fully substantiate either party's assertions, our discussions with Department and contractor officials made it clear to us that a lack of effective communication and coordination existed between the OCIO and the Office of Cyber Assessments.

Incident Response

Based on our discussions with Department officials, we determined that the OCIO had not appropriately responded to the discovery of the charging stations at the conference. Specifically, after a conference planning representative hired by the OCIO discovered the charging stations, she contacted OCIO personnel in an attempt to identify the source of the devices. However, when OCIO personnel were unable to determine the source of the charging stations after a brief inquiry, the devices were removed from the publicly accessible conference space by conference planning staff and placed into a conference room. We noted that OCIO officials had not immediately reported the discovery of the devices to appropriate security and/or law enforcement to determine whether the devices posed a threat, either physical or logical, to conference attendees, or the general public. Considering the charging stations were of unknown origin and appeared to target conference attendees, notification that the devices had been discovered to security personnel may have been a prudent action to ensure there was no threat to public safety.

The following day, after Office of Cyber Assessments personnel retrieved the devices from the OCIO and placed them back into operation, the devices were quickly detected by an OCIO conference planning representative and once again removed from the publicly accessible

conference space. At that time, management believed that further research into the devices was warranted. As such, officials disassembled one of the devices to evaluate the contents and check for possible physical threats, including what an OCIO official termed as "booby traps." After the first charging station was dismantled and it was determined that it contained a computer, an iJC3 team was assembled to perform forensic analysis of the computers. An OCIO official informed the audit team that it had assembled the iJC3 team to perform the analysis to determine whether any personally identifiable information had been collected. The iJC3 team determined that there was no evidence that any device had been plugged into either charging station after being deployed at the conference. While it was ultimately determined that the devices did not pose a risk to the conference attendees or the public, we are concerned about the lack of coordination among Department elements and the related response by the OCIO to the potential threat that such devices could have posed.

Contributing Factors to the Cyber Conference Incident

We found that a number of factors contributed, at least in part, to the testing incident that occurred at the Department's Cyber Conference. In particular, we noted that the Office of Cyber Assessments procedures were not always followed by personnel during this unannounced assessment. Similarly, the response by the OCIO did not adhere to Department incident response guidance, leaving conference attendees and other facility patrons vulnerable to potential unmitigated threats. Furthermore, we determined that the Office of Enterprise Assessments should have been more diligent in monitoring the execution of the assessment.

Implementation of Procedures

We found that Office of Enterprise Assessments officials had not fully followed existing procedures, which contributed to the testing incident at the conference. Although processes and procedures were in place related to planning and execution of cyber assessments, the Office of Cyber Assessments official responsible for the assessment did not believe they were applicable and commented that he did not incorporate the procedures into this exercise that would have been followed had this been a "typical" unannounced assessment. The *Assessment Process Guide* indicated that assessments are intended to evaluate a site's cybersecurity posture and that unannounced penetration testing, or red teaming, is primarily used to evaluate a site's ability to withstand focused attacks from Internet sources. Although Office of Cyber Assessments support personnel identified the testing as a red team activity, an Office of Enterprise Assessments official stated that because the testing did not consist of the active exploitation of a Department system, it was not a typical red teaming engagement. Therefore, Office of Cyber Assessments personnel had not fully followed the red team procedures established in the Guide. Specifically, although the Guide required that a plan be developed and approved by the Director, Office of Cyber and Security Assessments, for each assessment, we found that an assessment plan had not been finalized or approved for the conference testing. During the course of our review, a senior Office of Enterprise Assessments official commented that the Guide should have been followed, which would have required senior official review and approval of the testing plan.

In addition, the divergence from the established processes and procedures resulted in the uncoordinated execution of testing and the lack of notification of the details of the operation to OCIO management. In particular, the Guide required that the Office of Cyber Assessments work

with a trusted agent to coordinate activities which ensures the assessment remains within specified operational parameters. However, as noted during our review, a trusted agent was not established within the Department for this exercise by the Office of Cyber Assessments. An Office of Enterprise Assessments management official informed the audit team that adherence to current procedures, to include coordinating with trusted agents, would have prevented the issues that occurred as a result of the testing at the conference. Although we agree with that assertion, we believe additional consideration of risk is warranted prior to conducting future operations at an offsite facility to prevent an unforeseen escalation of events. To its credit, an Office of Enterprise Assessments official noted that they were already in the process of evaluating and updating the Guide as a result of the lessons learned at the conference.

We also found that the incident response by the OCIO was not adequate and did not adhere to Department procedures and best practices. For example, OCIO officials did not consider the devices to be potential threats when first discovered, impacting the type and focus of the resulting response. Upon first identifying the devices in the area, the devices were removed and stored in the local conference planning room instead of being assessed as possible threats. In our opinion, the unknown origin of the boxes and the fact that the devices were designed to target conference attendees should have resulted in an initial evaluation by appropriate security personnel for possible physical or logical threats. In light of the current threat environment and the need for vigilance, additional action may have been prudent. For instance, the Department of Homeland Security warned in its June 2016 bulletin that it was especially concerned that terrorist-inspired individuals and homegrown violent extremist may be encouraged or inspired to target public events or places. The bulletin also advised to report suspicious activity to local law enforcement. However, as previously noted, OCIO management did not immediately report the existence of the suspicious devices to appropriate security and/or law enforcement to determine whether they posed a threat to conference attendees or the general public. In addition, we noted that although the iJC3 incident reporting procedures require complete incident notification within 1 hour of detection, OCIO officials did not complete a notification in a timely fashion. In fact, an iJC3 team was not even assembled until the devices were discovered the second time - nearly 24 hours after the initial placement and subsequent detection and removal of the devices. Further, the devices were not reported when the origin was unknown, instead reporting occurred after identifying them as Office of Cyber Assessments testing resources.

Management Oversight

We determined that, in this instance, senior Office of Enterprise Assessments management provided minimal oversight of Office of Cyber Assessments operations. For example, although Office of Cyber Assessments officials had not followed processes for typical red team activities, including coordination with trusted agents, no additional scrutiny or review was considered by senior Office of Enterprise Assessments management even though they were aware of the unique nature of the assessment. We also found that Office of Enterprise Assessments officials did not effectively implement a system of checks and balances in its processes for conducting operations, resulting in Office of Cyber Assessments personnel operating independently and with minimal oversight. In this situation, the Director, Office of Cyber Assessments, was able to conduct the full scope of planning, managing, and executing the assessment. This included assigning work to contractor personnel without corroboration from any other Office of Cyber Assessments personnel and, as noted above, without providing formal notification and obtaining

approval from his immediate supervisors as required by the Guide. Although a senior Office of Enterprise Assessments official commented that he was aware of the assessment prior to the conference, he considered the testing benign and did not require additional controls.

Potential Impact

This incident illustrates shortcomings in the planning and operations of the Office of Enterprise Assessments and operations of the OCIO. The lack of adequate management and oversight of the unannounced assessment illustrated weaknesses in the performance of assessment operations that, if left uncorrected, could have the potential for negative repercussions on future operations. In addition, although we did not find evidence of malicious intent by the Office of Cyber Assessments when performing the assessment, the lack of adequate controls created an environment in which it was possible to subvert established processes. This incident could also have negative implications on the Office of Cyber Assessments' ongoing mission effectiveness and the perception of work completed by the office going forward. Furthermore, although not involved in the planning and performance of the assessment, the response to the incident by the OCIO illustrated the need to reinforce incident response procedures and the consideration of security threats, both cyber and physical, in various types of environments.

RECOMMENDATIONS

To help improve the Department's processes related to planning and executing cybersecurity assessments, we recommend that the Director, Office of Enterprise Assessments:

1. Ensure that policies and procedures governing the cyber assessment process be reviewed and updated for accuracy and effectiveness, as appropriate, including consideration of testing at a non-Federal offsite facility and adequate system of checks and balances governing cybersecurity assessments; and

2. Ensure that procedures for management oversight and approval are effectively implemented.

To help improve the incident response process within the Department, we recommend that the Acting Chief Information Officer:

3. Ensure that Department policies and procedures governing physical and logical security threats and incidents are appropriately addressed through training and awareness programs; and

4. Ensure that OCIO personnel are aware of all requirements related to identifying and responding to security threats.

MANAGEMENT RESPONSE

Management concurred with each of the report's recommendations and indicated that corrective actions had been taken, or were being planned, to address the identified issues. Specifically,

although Office of Enterprise Assessments management disagreed with the description of the testing conducted at the 2016 Cyber Conference as an "unannounced assessment" or a "red team exercise," it recognized that the activity exposed a gap in procedures and protocols relative to activities that did not meet normal assessment criteria. As a result, management indicated that the *Assessment Process Guide* was being revised to address multiple types of cyber testing activities performed under any potential condition. When finalized, management noted that the guide will be posted to the Office of Enterprise Assessments website and reviewed annually. In addition, although Office of Enterprise Assessments officials concurred that the coordination of testing with the OCIO was not adequate and could have been improved, they added that they had made some effort to advise the OCIO of the testing activity. OCIO management concurred with our recommendations concerning security threats and incidents and noted that personnel would be instructed to attend training related to observing, identifying, and reporting unusual behavior. The OCIO also planned to have its Headquarters Security Officer provide a briefing to both Federal and contractor staff related to identifying and responding to security threats.

AUDITOR COMMENTS

Management's comments and planned corrective actions were responsive to our recommendations. While the Office of Enterprise Assessments disagreed with our identification of the testing as an unannounced assessment or a red team exercise, documentation provided during our review and interviews with Office of Enterprise Assessments contractors and staff identified the assessment as an unannounced assessment or red team review. Furthermore, although the Office of Enterprise Assessments responded that it had made an effort to advise the OCIO of the testing activity, as noted in our report, the referenced notification by the Office of Enterprise Assessments to an OCIO official occurred during a separate testing activity prior to the cyber conference. We were told by the OCIO official that this discussion included neither the necessary testing details nor the acknowledged engagement by the OCIO to be considered coordination. Therefore, we continue to conclude that the notification by the Office of Enterprise Assessments was not adequate. Management's comments are included in Attachment 3.

Attachment

cc: Deputy Secretary
Chief of Staff
Director, Office of Enterprise Assessments
Acting Chief Information Officer

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

To determine the facts and circumstances surrounding the Office of Enterprise Assessments security assessment at the Department of Energy's 2016 Cyber Conference.

SCOPE

This inquiry was performed between September 2016 and June 2017 at Department Headquarters in Washington, DC, and Germantown, Maryland. The inquiry was limited to evaluating the circumstances surrounding the cybersecurity testing incident at the Department's 2016 Cyber Conference. The inquiry was conducted under Office of Inspector General project number A17TG007.

METHODOLOGY

To accomplish the objective, we:

- Reviewed applicable laws and regulations;
- Reviewed applicable standards and guidance issued by the Department, including the Department's Office of Enterprise Assessments;
- Reviewed prior reports issued by the Office of Inspector General and the Government Accountability Office;
- Reviewed the Associate Deputy Secretary's analysis of the activities of the Office of Enterprise Assessments;
- Reviewed the forensics reports on the devices conducted by the Office of Inspector General Technology Crimes Section and the Integrated Joint Cybersecurity Coordination Center;
- Held discussions with officials and personnel from Department Headquarters, including representatives from the Office of the Chief Information Officer and the Office of Enterprise Assessments; and
- Interviewed personnel responsible for performing cybersecurity assessments.

We conducted an allegation-based inquiry 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 objective. We believe the evidence obtained provided a reasonable basis for our conclusions and observations based on our objective. Accordingly, the inquiry included tests of controls and

compliance with laws and regulations to the extent necessary to satisfy the objective. Because our inquiry was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our work. Finally, we did not rely on computer-processed data to satisfy our objective.

An exit conference was held with Department management on June 12, 2017.

PRIOR REPORTS

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2016* (DOE-OIG-17-01, October 2016). The Department of Energy, including the National Nuclear Security Administration, had taken a number of actions over the past year to address previously identified weaknesses related to its cybersecurity program. In particular, the Department made progress remediating weaknesses identified in our fiscal year 2015 evaluation, which resulted in the closure of 10 of 12 prior year deficiencies. The Department also improved the completeness of its reporting of contractor system security information to the Department of Homeland Security and the Office of Management and Budget, an issue we had reported on for several years. While these actions were positive, our current evaluation found that the types of deficiencies identified in prior years, including issues related to vulnerability management, system integrity of Web applications, access controls and segregation of duties, and configuration management, continue to exist. The weaknesses identified occurred, in part, because the Department had not fully developed and/or implemented policies and procedures related to the weaknesses identified in our report. For instance, we found that the implementation of configuration and security patch management processes had not ensured that software remained secure.

- Audit Report on *Follow-up Audit of the Department's Cyber Security Incident Management Program* (DOE/IG-0878, December 2012). Although certain actions had been taken in response to our prior report, we identified several issues that limited the efficiency and effectiveness of the Department's cybersecurity incident management program and adversely impacted the ability of law enforcement to investigate incidents. The issues identified were due, in part, to the lack of a unified, Department-wide cybersecurity incident management strategy. In addition, changes to the Department's incident management policy and guidance may have adversely impacted overall incident management and response by law enforcement and counterintelligence officials. Also, we found that incident reporting to law enforcement was not always timely or complete, which hindered investigations into events.

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

May 5, 2017

MEMORANDUM FOR APRIL STEPHENSON
ACTING INSPECTOR GENERAL
OFFICE OF INSPECTOR GENERAL

FROM: GLENN S. PODONSKY
DIRECTOR
OFFICE OF ENTERPRISE ASSESSMENTS

SUBJECT: The Office of Enterprise Assessments Testing Incident at the 2016 Department of Energy Cyber Conference (A17TG007)

The Office of Enterprise Assessments (EA) and the Office of the Chief Information Officer (OCIO) have reviewed the Office of the Inspector General (OIG) draft report, "*The Office of Enterprise Assessments Testing Incident at the 2016 Department of Energy Cyber Conference*" (the Draft Report). While EA accepts and concurs with the OIG's underlying intent and recommendations, as set forth below, we recommend a change to the Draft Report which we believe enhances the recommendations and response to this incident. Indeed, in light of this incident, EA has already conducted a thorough review of its cyber assessment protocols, had them reviewed by the Department's Office of General Counsel for programmatic risks, and has updated them to cover any situations where EA's cyber assessment program is conducting testing of any type.

With regard to the Draft Report, however, we wish to point out our disagreement with the Draft Report's description of the testing conducted at the Cyber Conference as an "unannounced assessment related to the use of mobile device charging stations" and a "red team exercise." *See* Draft Report at 1-1, 1-3. While this incident shared some traits of assessments and red team exercises, we respectfully disagree with this conclusion. The testing done at the Cyber Conference was not, in our view, an "assessment." Rather, EA considered the testing to be part of an educational exercise related to the presentation topic to be presented at the Cyber Conference, specifically on the potential risks posed by connecting devices to charging stations. As such, it was not considered to be an assessment, announced or unannounced, and, consequently, the assessment protocols did not apply. EA also did not consider this to be a "red team" exercise, as it was conducted simply to test whether people would connect to the charging station and then use that data in a presentation at the conference. A "red team" exercise would be more traditionally designed to defeat cyber defenses and protocols. As stated, EA considered this to be an educational testing effort designed to collect a discrete data set, specifically, the number of devices which connected to the charging station.

Even though EA did not consider this test to be an "unannounced assessment" or "red team exercise," as found in the Draft Report, EA did take steps in engineering the testing equipment and software to ensure that it was non-intrusive and did not collect any personally identifiable information or other unauthorized information from any devices. Additionally, EA personnel were also present to monitor the testing equipment and environment. Finally, while we concur that the coordination in this incident was inadequate and should have been better, EA did make some effort to advise OCIO of this activity.

As a result of this incident and the reviews which followed, EA recognizes that this activity exposed a gap in its procedures and protocols relating to incidents that did not specifically meet the criteria for an assessment. As noted below in the specific responses to the Draft Report's recommendations, EA has carefully considered the OIG's concerns and contributing factors identified in the Draft Report and has undertaken a complete and thorough review of its cyber assessment procedures. Accordingly, EA has drafted modifications to the EA-21 Assessment Process Guide to include procedures for any activities that include cyber testing, which would include testing of the kind done at the Cyber Conference. Further, EA has strengthened its management processes for coordination and communication of such testing to ensure that such activities do not detract from the beneficial partnerships EA has with OCIO and others in DOE and the important role EA plays in assessing the performance of DOE line management, sites, contractors and the OCIO in protecting DOE cyber systems complex-wide. It is in this regard that we recommend that the Draft Report focus instead on the gap EA has identified and is mitigating, rather than a conclusion that EA failed to follow the assessment procedures and protocols. *See* Draft Report at 4.

EA has coordinated this response with the OCIO, and the OCIO concurs with the findings associated with the OCIO in the Draft Report and has already undertaken actions responsive to the OIG's recommendations to the OCIO. OCIO makes no representation as to the factual accuracy of statements referring to events and procedures internal to EA and for which it has no knowledge. OCIO and EA have also increased communication and collaboration in response to this incident.

If you have any questions, please contact Barbara Pruitt of my staff, who may be reached at (301) 903-5981.

Attachment: Management Responses to Draft IG Report: *The Office of Enterprise Assessments Testing Incident at the 2016 Department of Energy Cyber Conference (A17TG007)*

Attachment

Management Responses to Draft IG Report:
The Office of Enterprise Assessments Testing Incident at the 2016 Department of Energy Cyber Conference (A17TG007)

Recommendation 1: *Ensure that policies and procedures governing the cyber assessment process be reviewed and updated for accuracy and effectiveness, as appropriate, including consideration of testing at a non-Federal offsite facility and adequate system of checks and balances governing cybersecurity assessments.*

Management Response: Concur with comment

As stated above, EA agrees with the underlying intent of the recommendation that the policies and procedures guiding its cyber activities should be improved. The recommendation would be more complete and useful if it was broadened to suggest that policy and procedure revision be made to address cyber testing conducted by EA under any circumstances, including activities conducted outside formal assessment activities at DOE facilities and offsite locations.

Expectations for EA management oversight of cyber security assessment activities are well defined and consistently followed for all announced and unannounced assessments as defined in EA's policies and procedures. The Recommendation would be further improved if it suggested that EA enhance its management oversight of cyber security testing activities conducted outside of formal assessment activities.

Action Plan: As described above, the EA-21Assessment Process Guide has been revised to address cyber testing activities performed under any potential condition and is undergoing internal management review. When finalized, this guide will be posted to the EA website and reviewed annually.

Estimated Completion Date: August 1, 2017

Recommendation 2: *Ensure that procedures for management oversight and approval are effectively implemented.*

Management Response: Concur with comment

With the suggested expansion of the first recommendation, this recommendation is unnecessary. If it is retained, we suggest that it be refocused to address improvements to EA management approval and oversight of cyber testing activities conducted outside formal announced and unannounced assessments.

Action Plan: As described above, the EA-21Assessment Process Guide has been revised to address cyber testing activities performed under any potential condition and is undergoing internal management review. When finalized, this guide will be posted to the EA website and reviewed annually.

Estimated Completion Date: August 1, 2017

Recommendation 3: *Ensure that Department policies and procedures governing physical and logical security threats and incidents are appropriately addressed through training and awareness programs.*

Management Response: Concur
Action Plan: The OCIO concurs with the recommendations and understands the need for OCIO personnel to be reminded of all requirements related to identifying and responding to security threats. The OCIO currently conducts annual security training as required by the Department. In addition to security programs already in place, the OCIO will instruct all OCIO employees to complete course number PER-140DE, "Unusual Behavior" by September 1, 2017. This is EA/NTC's beginner-level eLearning course which provides the basic foundation for knowledge and skill training needed to observe, identify, and report unusual behavior. Additionally, the OCIO's Headquarters Security Officer will provide a briefing to the OCIO's contractor and Federal staff related to identifying and responding to security threats during an OCIO All Hands at a date to be determined prior to September 1st 2017.

Estimated Completion Date: September 1, 2017

Recommendation 4: *Ensure that OCIO personnel are aware of all requirements related to identifying and responding to security threats.*

Management Response: Concur

Action Plan: The OCIO concurs with the recommendations and understands the need for OCIO personnel to be reminded of all requirements related to identifying and responding to security threats. The OCIO currently conducts annual security training as required by the Department. In addition to security programs already in place, the OCIO will instruct all OCIO employees to complete course number PER-140DE, "Unusual Behavior" by September 1, 2017. This is EA/NTC's beginner-level eLearning course which provides the basic foundation for knowledge and skill training needed to observe, identify, and report unusual behavior. Additionally, the OCIO's Headquarters Security Officer will provide a briefing to the OCIO's contractor and Federal staff related to identifying and responding to security threats during an OCIO All Hands at a date to be determined prior to September 1st 2017.

Estimated Completion Date: September 1, 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 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.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu