OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

AUDIT REPORT

DOE-OIG-19-34

June 2019

SECURITY OVER INDUSTRIAL CONTROL SYSTEMS AT SELECT DEPARTMENT OF ENERGY LOCATIONS

Department of Energy
Washington, DC 20585

June 7, 2019

MEMORANDUM FOR THE SECRETARY

FROM: Teri L. Donaldson
Inspector General

SUBJECT: INFORMATION: Audit Report on "Security over Industrial Control Systems at Select Department of Energy Locations"

BACKGROUND

Successful cyber or physical attacks on industrial control systems can have significant impacts to operations and safety and result in costly recovery. The Federal Government has increased efforts to ensure agencies identify and protect these types of systems. For example, agencies are required to identify, prioritize, and coordinate the protection of critical infrastructure and key resources to prevent, deter, and mitigate the effects of compromise. Office of Management and Budget Memorandum M-17-09, *Management of Federal High Value Assets*, also highlighted the importance of managing high impact Federal information systems and provided requirements for identifying, categorizing, prioritizing, reporting, and assessing such assets. The Department of Energy utilizes industrial control systems and/or high value assets to support its missions related to energy, scientific research, environmental cleanup, and national security. For example, industrial control systems used at field sites can include operational technology systems related to physical security, heating, ventilation, cooling, electrical, and water systems, as well as supervisory control and data acquisition systems.

While prior reviews have identified physical and cybersecurity weaknesses on various types of information systems, the Office of Inspector General has conducted limited testing related to the industrial control systems that manage critical operations. Our annual evaluation report related to the Department's implementation of the *Federal Information Security Modernization Act of 2014* continues to identify weaknesses related to the Department's business systems but does not typically include the review of industrial control systems. We initiated this audit to determine whether the Department implemented security controls over selected industrial control systems in accordance with established requirements.

RESULTS OF AUDIT

The Department had not always implemented security controls over selected industrial control systems in accordance with established requirements. The Department continues to make

improvements related to its cybersecurity program; however, we noted that additional efforts were needed to ensure that security controls were implemented to protect industrial control systems. Specifically, we found:

- Although required, locations reviewed had not always developed complete inventories of industrial control systems. For instance, we found that the four locations reviewed excluded industrial control systems, some of which were designated as high value assets[1] and/or components of those systems, from their system inventories.

- Two locations had not appropriately categorized the impact of industrial control systems to external systems and the Department's mission in accordance with Federal requirements. For instance, one location determined that a system was only moderate impact even though the system could have significant negative impacts if no longer operational. At another site, a system was categorized as low impact even though interviews and detailed test work identified that the system should have potentially been categorized at a higher level due to its significance. Although one site agreed that a review of the categorization should occur, the other site expressed concern regarding unintended consequences of raising its system categorization.

- Improvements were needed related to documentation of security controls for industrial control systems. In particular, specific security policies and procedures and system security plans were not always developed in accordance with Federal requirements.

- Weaknesses related to vulnerability management existed at three locations. Generally, we found that six of the industrial control and/or related support systems tested did not always have the most recent software patches installed or used outdated and/or unsupported software.

- Physical and/or logical access control weaknesses existed at each of the four locations reviewed. For instance, we found that physical security controls did not always provide sufficient restrictions over information systems. In addition, we noted that improvements were needed to restrict user privileges.

Based on our test work and discussions with site officials, we determined that the weaknesses identified existed, in part, because the Department experienced challenges balancing mission needs with ensuring adequate system security. Specifically, Federal requirements indicated that information security was just one aspect to consider when operating systems. However, we found that conflicting priorities between information technology officials and those responsible for operating industrial control systems was a common challenge during our review. In addition, the Department's cybersecurity directives and related program-specific requirements did not clearly articulate what constituted an information technology system versus an operational technology system; due to this ambiguity, it was unclear whether the *Federal Information*

[1] High value assets include Federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the Nation's security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health.

Security Modernization Act of 2014 must be applied to operational technology systems. Also, the locations reviewed had not always appropriately categorized systems and documented the selection, implementation, and effectiveness of selected security controls because site officials had not fully developed and implemented the required risk management strategy. Specifically, locations reviewed had not always completed business impact analyses, defined risk tolerance levels, developed continuous monitoring programs, and implemented the most recent minimum Federal cybersecurity requirements.

Without improvements to the cybersecurity programs at the locations reviewed, information systems and data may be exposed to a higher than necessary level of risk of compromise, loss, modification, or non-availability. For example, inappropriate system categorization can result in less stringent application of cybersecurity requirements, leaving the information system and its data at a higher risk of negative operational impact, including potentially impairing mission accomplishment. Furthermore, the Department's operations could be negatively affected without sufficient security measures, such as effective continuous monitoring processes, in place. As such, we have made recommendations that, if fully implemented, could improve security controls over industrial control systems.

Due to the sensitive nature of the vulnerabilities identified during our audit, we have omitted certain information from this report. We have provided site officials with detailed information regarding vulnerabilities that we identified at their locations and, in some cases, officials have initiated corrective actions to address the identified vulnerabilities.

MANAGEMENT RESPONSE

Management concurred with the report's recommendations and indicated that it had initiated or planned corrective actions to address issues identified in the report. Management's comments and our responses are summarized in the body of the report. Management's formal comments are included in Appendix 3. Due to the sensitive nature, including site or system specific information, of Management's responses to the recommendations, these comments have been omitted from the report.

Attachment

cc: Deputy Secretary
Chief of Staff
Administrator, National Nuclear Security Administration
Under Secretary of Energy
Under Secretary for Science
Chief Information Officer
Acting Chief Financial Officer
Assistant Secretary for Electricity

SECURITY OVER INDUSTRIAL CONTROL SYSTEMS AT SELECT DEPARTMENT OF ENERGY LOCATIONS

TABLE OF CONTENTS

Audit Report

Appendices

SECURITY OVER INDUSTRIAL CONTROL SYSTEMS AT SELECT DEPARTMENT OF ENERGY LOCATIONS

BACKGROUND

The Department of Energy utilizes industrial control systems and/or high value assets[1] to support its missions related to energy, scientific research, environmental cleanup, and national security. For the purposes of our review, industrial control systems included non-financial operational technology systems supporting location-specific operations such as physical security, heating, ventilation, cooling, electrical, and water systems, as well as supervisory control and data acquisition systems. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides overarching cybersecurity requirements for Federal information systems. In addition, NIST SP 800-82, Revision 2, *Guide to Industrial Control Systems* (*ICS*) *Security*, provides specific requirements related to industrial control systems. The Office of the Chief Information Officer established that the Department and its facility management contractors comply with NIST publications. As such, we evaluated cybersecurity controls over eight industrial control systems at four locations, including Site 1, Site 2, Site 3, and Site 4. Our review included testing more than 40 NIST cybersecurity controls in areas such as access controls, security assessment and authorization, configuration management, physical and environmental protection, and risk assessment.

DETAILS OF FINDINGS

We determined that the Department had not always implemented security controls over selected industrial control systems in accordance with established requirements. Specifically, additional efforts were needed to implement required security controls to protect industrial control systems at the locations reviewed. In particular, locations had not always developed complete inventories of industrial control systems in accordance with Federal requirements. In addition, the risk to information systems reviewed was not always appropriately categorized. Our test work also identified that improvements were needed related to documentation of security controls. Also, technical vulnerability testing identified unique vulnerabilities, including critical or high-risk weaknesses. Furthermore, we found that physical and logical access security controls did not always provide sufficient restrictions over information technology (IT) resources.

High Value Assets and System Inventories

Although Department elements had developed inventories of high value assets, our review identified that the approach was not consistently applied. Specifically, some locations identified systems as high value assets, while at other locations, systems performing the same type of functions were not included in the Department's high value asset inventory. For example, one industrial control system reviewed at Site 1 was not identified by the site as a high value asset even though other locations included similar systems in their high value asset inventories. Site 1

[1] High value assets include Federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the Nation's security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health.

officials explained that although the system was previously considered a high value asset in November 2015, its designation was modified based on their interpretation of the high value asset definition. In addition, site officials stated during the site visit that the system had not been categorized as high risk under NIST Federal Information Processing Standard Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, and, therefore, was not identified as a high value asset. However, according to an official from the Department's Office of the Chief Information Officer and the requirements of Office of Management and Budget (OMB) Memorandum M-17-09, *Management of High Value Assets*, there was no minimum NIST Federal Information Processing Standard Publication 199 risk categorization for a system to be considered a high value asset. Rather, NIST Federal Information Processing Standard Publication 199 ratings were only one factor to consider in the identification and prioritization process of high value assets. The audit team noted that the recently issued OMB Memorandum M-19-08 on *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program* also did not include such requirements related to minimum categorizations. In addition, we found that some locations included business-related systems in their inventory of high value assets while other locations did not. We are concerned that without a complete inventory of high value assets, including industrial control systems, oversight and authorizing officials may not have a thorough understanding of the operating environment necessary to effectively manage risk and ensure proper allocation of resources for protecting information systems.

In addition, and contrary to Federal requirements, the Department had not always developed complete system inventories to include all systems and related components. For instance, although Site 3 officials developed a corrective action plan to establish a complete inventory of information systems, the efforts were not completed as of October 2018, nearly a year past their initial estimate for completion. In addition, while NIST required all components within the system's authorization boundary to be identified, the locations reviewed had not always included underlying databases or tracked virtual servers within component inventories. Instead, inventories primarily consisted of physical equipment that could be tagged. We have continuously reported on system inventory weaknesses across the Department during our *Federal Information Security Modernization Act of 2014* evaluations and other audits.

Furthermore, we determined that Site 1 continued to operate an industrial control system without formal approval by the authorizing official even though the Department's Office of Enterprise Assessments identified the same concern in September 2013. Site 1 officials also had not included this system in the site's inventory or as a high value asset. Specifically, as of October 2018, Site 1 was still in the process of developing an authorization package for one of its systems, but officials stated that competing priorities continued to delay efforts. Until an authorization package that identifies risks and describes the implementation of necessary controls is completed, the system continues to operate without officials understanding the true risk of operating the system.

System Categorization

Locations reviewed may not have always appropriately categorized the impact of industrial control systems to external systems and the Department's mission. System categorization[1] is an initial step necessary for determining which security controls to implement and for ensuring effective management and oversight of information security programs. Specifically, NIST noted that information systems supporting the most critical and/or sensitive operations and assets within the organization, as indicated by the security categorization, demand the greatest level of attention and effort to ensure that appropriate information security and risk mitigation is achieved. Federal requirements also indicate that the potential for a catastrophic loss, including costs to replace the system and the aggregated effect such loss could have on the mission, should result in a higher categorization level with more robust controls. However, we determined that the industrial control system categorization process used at two locations reviewed was not consistent with Federal requirements. Specifically, we found:

- One Site 1 system reviewed was categorized as moderate even though a compromise of the system could potentially result in significant negative impacts to external systems if no longer operational. In addition, Site 1 officials noted significant replacement costs related to the system. According to NIST guidance, this type of system should be categorized as high and include commensurate protections based on the need for system availability. We found that the system security plan identified NIST system categorization requirements but did not provide explanations for a lower categorization. Site 1 officials agreed that additional review was warranted based on the Office of Inspector General and the Office of Enterprise Assessments questioning this system's categorization.

- One Site 2 system reviewed was categorized as low even though interviews and detailed test work identified that the system should have potentially been categorized at a higher level. Specifically, Site 2 officials indicated that a catastrophic loss of the system could result in loss of use and scientific reputation. During our testing, we determined that the site had scheduled out the next decade of planned experiments, and officials stated that, aside from scheduled maintenance, only in the event of a potential catastrophe would the system shut down to avoid potential research errors and excessive costs. In addition, Site 2 officials had implemented additional physical security controls for personnel safety when operating the system that were not within the security plan. Similar to the Site 1 system, Site 2 officials explained the importance of availability, given the strict limits for downtime due to research needs. Furthermore, the system security plan did not provide a detailed explanation for the categorization level selected. Although Site 2 officials did not agree or disagree with our assessment, an official explained that the site was attempting to prevent possible unintended consequences, such as limiting research, associated with raising the categorization of its system.

[1] Categorization guidance was provided under NIST Federal Information Processing Standard Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*; NIST SP 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*; NIST SP 800-60, Volume I, *Guide for Mapping Types of Information and Information Systems to Security Categories*; and NIST SP 800-60, Volume II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*.

Security Control Documentation

Our test work identified that improvements were needed related to documentation of security controls for industrial control systems. Given the unique nature of these types of systems, NIST SP 800-82 tailored Federal cybersecurity requirements for industrial control systems. However, we found that specific security policies and procedures, and system security plans were not always developed in accordance with NIST. For example, one system security plan reviewed at Site 2 indicated that the system heavily relied upon the site's enterprise-level controls instead of controls tailored to the industrial control system. Specifically, the system's security plan indicated reliance on enterprise-level controls for 11 areas, such as awareness and training, security assessment and authorization, configuration management, incident response, physical and environmental protection, and risk assessment. However, the plan did not discuss supplemental controls related to these areas that would have been required of an industrial control system. Although Site 2 implemented additional physical and environmental protection controls for the system reviewed, it did not identify these controls in the system security plan. Developing and maintaining an accurate security plan is critical for ensuring the effectiveness of ongoing system testing.

In addition, we found that Site 4 had not ensured that system security plans were developed according to current Federal requirements. Specifically, officials were still using NIST SP 800-53, Revision 3, even though the current version of the standards provided an additional 52 controls or control enhancements for moderate-risk systems that were to be implemented by April 2014.

Vulnerability Management

Technical vulnerability testing conducted on the selected industrial control systems at three locations identified various unique vulnerabilities, including a number that were considered critical or high risk. We found that systems did not always have the most recent software patches installed or used outdated or unsupported software. Site officials noted these systems often required specialized software that was no longer supported by the vendor due to their unique capabilities and often were not connected to networks where these potential vulnerabilities could be exploited by external parties. However, a number of the weaknesses included valid vulnerabilities that could be exploited by malicious insiders based on existing system configurations or through external attacks for systems connected to the network. For example, contrary to NIST requirements related to access controls and system integrity, one major system was running an unencrypted remote access service and outdated software that could negatively impact the confidentiality, integrity, and availability of the system by allowing an attacker to execute malicious code on the host. We found that although compensating controls existed to help alleviate the impact of the weaknesses identified, officials at the locations reviewed agree that the vulnerabilities were valid and should be addressed. While only some of the systems tested were connected to other networks or systems, officials should consider these conditions as control systems trend toward becoming more connected to site networks or otherwise evolve.

Physical Security

Physical security controls did not always provide sufficient restrictions over IT resources. While emphasis was placed on accountability, improvements to physical security controls were needed to assist in security over industrial control systems. In particular, we found that although many of the areas at the locations reviewed required badged access, improvements were necessary. Although Site 2 officials commented that access was based on functional roles, we found that more than one-third of individuals with access to each of the three data centers reviewed had not badged into the server room facilities in at least 6 months and, in some cases, for more than a year. For instance, we identified that 78 of 205 (38 percent) individuals with access to one data center had not accessed the facility in at least 6 months. We also identified that facility access records included a Headquarters official even though the individual was not an employee of or located at the facility. In addition, one of the areas at Site 4 did not utilize badge readers for controlling a system's data center access but instead relied on a door lock. NIST SP 800-53, Revision 4 indicated that it was critical to locate servers in secure physical environments, using protections such as server rack locks, badge reader access, security guards, or physical intrusion detection systems. Furthermore, best practices indicated that access should be restricted to those who need to maintain the servers or infrastructure of the room. Also, at Site 4, anyone with access to the site could have potentially gained access to the critical monitors and sensors of one of the systems reviewed, potentially increasing the risk of insider threat.

At Site 2, we found that network asset records identified assets by the room associated with their connection point to the network (i.e., the room associated with the wall jack or a switch port). This limited the effectiveness of identifying assets that physically resided in an adjacent room and analyzing potential vulnerabilities during technical testing. This could increase the risk to systems if not sufficiently secured. The Industrial Control Systems Cyber Emergency Response Team noted that gaining physical access to a control room or control system components often implies gaining logical access to the process control system as well. As a result, assets may not receive the appropriate level of physical protection necessary for securing the system.

User Privileges and Authentication

We found that improvements were necessary related to restricting logical access privileges for information system users and improving authentication at select locations reviewed. Our testing noted that although locations established timeframes for changing passwords, we found:

- Passwords for 22 of 372 accounts (6 percent) for one system at Site 1 were set to never expire. We also determined that 3 of 10 accounts on a development system at the site had not been changed within timeframes established by the site. Weaknesses in access controls could potentially result in unauthorized changes to the information systems.

- Approximately 40 percent (884 of 2,218) of Site 2's account passwords had not been changed within timeframes required by site policy. This included 20 passwords that had never been changed. Site 2 officials commented that password problems were the result of complying with the Department's multi-factor authentication process and indicated that corrective actions had been taken.

Furthermore, we identified eight authentication-specific vulnerabilities at two locations reviewed pertaining to the use of strong authentication techniques. Specifically, the vulnerabilities included the ability for an attacker to eavesdrop and potentially alter communications and, in one case, there was no security over communications. The Office of Enterprise Assessments also reported on authentication deficiencies at another site included in our review.

Cybersecurity Program Management

Based on our test work and discussions with site officials, we determined that the weaknesses identified existed, in part, because of challenges in balancing mission needs while also ensuring system security. In addition, the weaknesses related to developing a system's inventory and identifying high value assets occurred due to a lack of clarity within the Department's cybersecurity directive and related program-specific cybersecurity requirements. Furthermore, we found that the locations reviewed had not fully developed and implemented a risk management strategy designed to meet Federal requirements.

Operational and Information Technology

During our test work and discussions with Department officials, we determined that a contributing factor to a number of weaknesses identified was balancing the need for industrial control systems to function reliably with the need to secure those systems. Specifically, operational technology officials were responsible for ensuring that systems operated as intended, while IT officials were responsible for ensuring system security. Operational technology supports physical resources and manufacturing processes comprised of devices, sensors, and software necessary to control and monitor plants and equipment. IT combines all necessary technologies for processing information. However, contrary to Federal requirements, operations systems, such as industrial control systems, were not always considered IT systems and, therefore, according to officials, were not always included in system inventories, properly certified and accredited for operation, or subjected to Federal cybersecurity controls. Rather, industrial control systems had been considered operational in nature but, as time progressed, additional networking and communications capabilities blurred the lines of infrastructure and IT systems. According to OMB M-15-14, *Management and Oversight of Federal Information Technology*, IT includes any services or equipment, or interconnected systems or subsystems of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

We also determined that functionality over cybersecurity was a key mission difference among the infrastructure and IT functions. For example, although NIST required that access controls include separate system logins, automatic system locks for inactivity, or password changes when individuals left employment, one site had not implemented these controls to accommodate the functionality of the system. In addition, Site 4 officials indicated that resources were project-driven and that costs associated with cybersecurity were dependent on each of the site's project budgets rather than the site's IT budget. As such, funding had not always been prioritized for the site to implement the most current cybersecurity requirements, such as those identified by NIST.

The systems reviewed provided significant capabilities to help the Department meet its mission. However, system security plans, control testing and results, and plans to mitigate any potential weaknesses discovered during control testing were not always developed for industrial control systems because the systems had not historically been identified and secured at the same level as other types of information systems. Although NIST had provided control requirements for industrial control systems for years, Department officials indicated that differences between infrastructure and IT functions continued to exist. While sufficient resources are necessary to ensure that systems perform tasks as designed, it is also necessary to balance competing priorities to ensure that they do so in a secure manner. As previously reported in our review of *The Department of Energy's July 2013 Cyber Security Breach*, (DOE/IG-0900, December 2013), the inability to effectively balance system functionality with security can leave information systems vulnerable and negatively impact the Department's operations.

Defining Systems and Identifying High Value Assets

The weaknesses related to developing a system's inventory and identifying high value assets occurred, in part, due to a lack of clarity within the Department's cybersecurity directive and related program-specific cybersecurity requirements. In particular, we found that the directive and related guidance did not adequately define what constituted an information system or major application, leaving this determination at the discretion of each site. In one instance, we determined that this resulted in Site 1 not identifying an information system or implementing the requisite security controls. In addition, OMB's guidance on *Management of High Value Assets* required that agencies take an enterprise-wide perspective of risks posed by their high value assets and develop a risk-based matrix of threats, vulnerabilities, impacts, and likelihood of compromise. However, according to Office of the Chief Information Officer officials, individual Department elements were initially responsible for identifying their own high value assets. The Department reported this combined high value asset list without completing an enterprise-wide assessment to ensure that an enterprise-wide perspective was achieved. Subsequent to this reporting and after we expressed our concerns with inconsistencies in reported systems to the Office of the Chief Information Officer, the list was updated to remove 77 of 101 (76 percent) systems but still contained the same types of inconsistencies. For example, some locations continued to report general support systems such as networks or financial systems as high value assets while other locations did not. Without an accurate inventory, the Department may not identify all systems that should be considered high value assets for assisting in the Federal Government's effort to strengthen its cybersecurity posture.

Risk Management

The locations reviewed had not always appropriately categorized systems and documented the selection, implementation, and effectiveness of selected security controls because they had not fully developed and implemented an adequate risk management strategy. Specifically, locations reviewed had not always completed business impact analyses, defined risk tolerance levels, developed continuous monitoring programs, and implemented the most recent NIST cybersecurity requirements. NIST requires an authorizing official to explicitly accept risk after considering factors such as organizational operations and assets, as well as the resulting impact on individuals, other organizations, and the Nation. The risk-based determination to authorize

operations follows a process of categorizing information systems, including selecting, implementing, testing, and monitoring those controls based on the system categorization. In addition, NIST requires that risk management strategies provide guidance and relevant information to authorizing officials who approve systems to operate and assume the resulting operational risk.

We found that Site 2's system categorization process was based on site assist visits performed approximately a decade ago by former Headquarters officials. However, Site 2 officials indicated that the process was not documented. In addition, the categorization process had not been updated despite significant changes to Federal cybersecurity requirements and the system since the time the assessment was completed.

Our test work determined that one of Site 1's industrial control systems may have been categorized higher if a business impact analysis had been completed. A business impact analysis assists the authorizing official in making risk-based system authorization decisions. Such an analysis should include potential impacts that the system would have on entities dependent on its information systems. Therefore, this determination could have increased the availability assessment of the system. As of October 2018, a draft business impact analysis was still being developed.

Also, even though previously recommended by the Office of Inspector General, we found that the locations reviewed had not developed risk tolerance levels for their information systems – a key component of the risk management framework that provides constraints on risk-based decisions, affects the nature and extent of risk management oversight, the rigor of risk assessments, and the content of strategies for responding to risk. We noted that the development of risk tolerance levels could have assisted in determining what risk categorization and associated controls were appropriate.

In addition, we determined that the lack of effective continuous monitoring programs also contributed to some of the weaknesses identified. For instance, Site 1 was still in the process of developing a continuous monitoring program even though NIST published requirements for continuous monitoring in September 2011. An effective continuous monitoring program can ensure that relevant risks are identified and considered so that changes to a system's risk categorization can be made, if necessary. Continuous monitoring also necessitates proper identification of how controls are designed and implemented to ensure that potential vulnerabilities are identified for a risk-based system authorization decision. However, we found that system security plans at Site 1 did not always identify how security controls were designed or implemented. Implementation of a fully effective continuous monitoring process at Site 1 may have identified many of the weaknesses noted during our review and helped ensure that current Federal requirements were implemented, including those related to access controls. Similarly, the lack of a fully effective risk management process at Site 2 and Site 4 resulted in system security plans that did not provide full details about how specific NIST requirements were designed and implemented. In the case of Site 4, the continuous monitoring process was impacted because the site was still negotiating the contract terms for adding the most up-to-date Federal requirements. For example, the site had not always implemented all NIST SP 800-53, Revision 4 controls, which prescribe the need for organizations to enforce physical access logs,

provide lockable casings to protect information systems from unauthorized physical access, and enforce physical access authorizations to the information system. Although NIST SP 800-53, Revision 4 should have been implemented several years prior to our review, site officials stated that the Department and contractor have not agreed about the level of funding necessary for implementing these controls.

Path Forward

Without improvements to cybersecurity programs at the locations reviewed, information and systems may be exposed to a higher than necessary level of risk of compromise, loss, modification, or non-availability. For example, inaccurate system risk categorization can result in the less stringent application of cybersecurity requirements, leaving the information system and its data at a higher risk of negative operational impact, including potentially impairing mission accomplishment. The Department's multi-faceted mission related to energy, scientific research, environmental cleanup, and national security could also be negatively affected without sufficient security measures in place.

RECOMMENDATIONS

To improve security controls over industrial control systems, we recommend that the Department's Chief Information Officer:

1. Determine what types of operational technology and IT systems should be defined as an information system to ensure consistency with Federal requirements and codify the decision within the Department's cybersecurity order.

Using information provided by the Department's Chief Information Officer, we recommend that the Administrator for the National Nuclear Security Administration, Under Secretary of Energy, Under Secretary for Science, and Assistant Secretary for Electricity:

2. Identify, inventory, and assess the allocation of resources for the protection of industrial control systems, including high value assets, and ensure sites exercise appropriate security authorization processes for industrial control system assets.

We also recommend that the Management of Site 1, Site 2, Site 3, and Site 4:

3. Resolve or mitigate specific weaknesses identified within this report and during technical vulnerability scanning and penetration testing performed at selected locations; and

4. Ensure the appropriate risk management processes are implemented, including developing adequate documentation to support security processes, implementing effective continuous monitoring processes, and developing/evaluating risk tolerance levels related to system operations.

We also recommend that the Management of Site 4, direct the Contracting Officer to:

5. Ensure current Federal cybersecurity requirements are included in site-level contracts in a timely manner.

MANAGEMENT RESPONSE

Management concurred with the report's recommendations and indicated that it had initiated or completed corrective actions to address issues identified during our review. For example, management stated that it is updating the Department's cybersecurity directive and planned to more fully define operational and technology systems by the end of the calendar year. Management also indicated that it would leverage ongoing efforts to update its cybersecurity order and undertake various initiatives from a recent Office of Enterprise Assessments report to identify, inventory, and assess resource allocation. In addition, management resolved or agreed to mitigate specific weaknesses identified during our review. With regards to ensuring that appropriate risk management processes are implemented, management noted that it plans to develop risk tolerance levels and formalize an authority to operate the system noted during our review. Furthermore, management commented that the most recent Federal cybersecurity requirements were added to Site 4's contracts since of the time of our review.

AUDITOR COMMENTS

Management's comments and planned corrective actions were responsive to our recommendations. Management's comments are included in Appendix 3. Due to the sensitive nature, including site or system specific information, of Management's responses to the recommendations, these comments have been omitted from the report.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

We conducted this audit to determine whether the Department of Energy implemented security controls over selected industrial control systems in accordance with established requirements.

Scope

The audit was performed between January 2017 and February 2019 at Site 1, Site 2, Site 3, and Site 4. In addition, discussions were held with Headquarters and other Department location officials. The audit was conducted under Office of Inspector General Project Number A17TG017.

Methodology

To accomplish our objective, we:

- Reviewed applicable laws, regulations, directives, and best practices related to information and cybersecurity;
- Reviewed applicable standards and guidance issued by the Department;
- Reviewed applicable standards and guidance issued by the Office of Management and Budget and the National Institute of Standards and Technology for the planning and management of system and information security, such as Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, and National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;
- Selected 46 Federal cybersecurity requirements from each of the National Institute of Standards and Technology Special Publication 800-53, Revision 4 control families and compared them, as necessary, to additional interpretations of these controls for industrial control systems within National Institute of Standards and Technology Special Publication 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*;
- Requested information system inventories from the Department's programs and locations to identify industrial control systems and tested two systems from each of the four locations selected;
- Reviewed relevant reports issued by the Office of Inspector General and the Government Accountability Office;
- Reviewed both physical and cybersecurity plans and supporting documents to determine whether potential opportunities existed for improving the Department's security posture;

- Contracted with KPMG LLP to perform, at three of the locations reviewed, external penetration testing and vulnerability scanning of selected systems or the associated test/development system, when necessary, to minimize risks associated with such testing on production systems;

- Held discussions with Federal and contractor officials from various Department elements; and

- Assessed controls over network operations and systems to determine the effectiveness related to safeguarding information resources from unauthorized internal and external sources.

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 objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. We assessed the Department's implementation of the *GPRA Modernization Act of 2010* and determined that the Department had not established performance measures related to the cybersecurity management of industrial control 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 did not solely rely on computer-processed data to satisfy our audit objective. However, we used computer-assisted audit tools to perform scans of various networks and drives. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel. In addition, we obtained data in electronic format and used data analysis software to evaluate physical and logical access controls. We confirmed the validity of this data by cross-referencing supporting source documents and discussing potential discrepancies with site personnel.

Management waived an exit conference on May 14, 2019.

PRIOR REPORTS

- Audit Report on the *Followup on Bonneville Power Administration's Cybersecurity Program* (DOE-OIG-17-06, August 2017). Bonneville Power Administration (Bonneville) made efforts to improve its cybersecurity program since our prior review, such as elevating the Chief Information Officer position for greater visibility, accountability, and oversight. However, we found that Bonneville had not implemented a fully effective cybersecurity program and continued to identify weaknesses in the areas of access controls, vulnerability and configuration management, and contingency planning. Furthermore, we noted that officials had not ensured that all systems contained up-to-date security controls. We also noted weaknesses related to risk management. The issues identified occurred, at least in part, because officials had not ensured that Federal and Bonneville requirements were updated and/or fully implemented. For example, contrary to Federal requirements, Bonneville had not implemented an effective continuous monitoring program. Specifically, Bonneville lacked separation of duties related to the individuals that designed security controls and tested those controls. Moreover, Bonneville did not effectively utilize plans of action and milestones, a critical component of an effective continuous monitoring program.

- Audit Report on *The Department of Energy's Cybersecurity Risk Management Framework* (DOE-OIG-16-02, November 2015). Our review found that although progress had been made toward implementing an unclassified cybersecurity risk management framework designed to reduce the likelihood of compromise to its information systems and data, additional effort was needed to ensure that operating system risks were identified, and systems and information were adequately secured. Although certain controls had been established, officials had not always thoroughly and independently assessed or monitored such controls to ensure that they were effective. Furthermore, programs and sites had not ensured that authorizing officials responsible for accepting system risk were fully aware of the risks, weaknesses, and vulnerabilities to the information systems under their purview. The weaknesses identified existed, in part, because Federal requirements for securing information systems had not been fully implemented, and the Department of Energy had not established sufficient oversight and communication to support its cybersecurity risk management program. In addition, Federal officials had not provided adequate oversight to ensure that effective risk management practices had been implemented, and Department management had not always ensured that risk tolerances were established and communicated to field elements as required to help ensure the implementation of an effective risk management program.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program - 2014* (DOE/IG-0925, October 2014). While the Department and the National Nuclear Security Administration had taken positive actions to correct deficiencies identified in prior years, additional effort was needed to ensure that the risks to operating systems were identified and that systems and information were adequately secured. For example, we noted issues pertaining to reporting contractor system performance metrics, patch management, system integrity, logical access controls, configuration management, and security management to include not having developed a complete system inventory. The

issues identified occurred, at least in part, because the Department's programs and sites had not ensured that cybersecurity policies and procedures were developed and properly implemented. The weaknesses identified in this report should be thoroughly considered as the Department transitions its cybersecurity program from the traditional compliance-based process to one that supports the National Institute of Standards and Technology's Risk Management Framework and continuous system authorizations.

- Special Report on *The Department of Energy's July 2013 Cyber Security Breach* (DOE/IG-0900, December 2013). The July 2013 incident resulted in the exfiltration of a variety of personally identifiable information on over 104,000 individuals. Our review identified a number of technical and management issues that contributed to an environment in which this breach was possible. Compliance and technical problems included the frequent use of complete social security numbers as identifiers, permitting direct internet access to a highly sensitive system without adequate security controls, lack of assurance that required security planning and testing activities were conducted, and failure to assign the appropriate level of urgency to replace end-of-life systems. We also identified numerous contributing factors related to inadequate management processes. These issues created an environment in which the cybersecurity weaknesses we observed could go undetected and/or uncorrected. While we did not identify a single point of failure that led to the breach, the combination of the technical and managerial problems we observed set the stage for individuals with malicious intent to access the system with what appeared to be relative ease.

- Audit Report on *Management of Los Alamos National Laboratory's Cyber Security Program* (DOE/IG-0880, February 2013). The Los Alamos National Laboratory had not fully implemented its risk management, system security testing, and vulnerability management practices. The issues identified occurred, in part, because of a lack of effective monitoring and oversight of Los Alamos National Laboratory's cybersecurity program by the Los Alamos Field Office (formerly known as the Los Alamos Site Office), including approval of practices that were less rigorous than those required by Federal directives. In addition, we found that Los Alamos National Laboratory's Information Technology Directorate had not followed National Nuclear Security Administration policies and guidance for assessing system risk and had not fully implemented the Laboratory's own policy related to ensuring that scanning was conducted to identify and mitigate security vulnerabilities in a timely manner.

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

April 25, 2019

MEMORANDUM FOR TERI L. DONALDSON
INSPECTOR GENERAL

FROM: STEPHEN (MAX) EVERETT
CHIEF INFORMATION OFFICER

SUBJECT: Inspector General's Draft Report on "Security over Industrial Control Systems at Select Department of Energy Locations" (Job Code A17TG017)"

Thank you for the opportunity to comment on the Draft Evaluation Report, "Security over Industrial Control Systems at Select Department of Energy Locations." The Department of Energy (DOE) understands the Office of Inspector General (IG) conducted this audit to determine whether DOE implemented security controls over selected industrial control systems in accordance with established requirements.

DOE concurs with recommendations 1, 2, and 5 and concurs in principle with recommendations 3 and 4. Details are in the attached enclosure.

If you have any questions or need additional information, please contact Mr. Emery Csulak, Deputy Chief Information Officer for Cybersecurity, at 202-586-0166.

Enclosure

Printed with soy ink on recycled paper

Due to the sensitive nature, including site or system specific information, of Management's responses to the recommendations, these comments have been omitted from the 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) 586-1818. For media-related inquiries, please call (202) 586-7406.