Office of Inspector General

OFFICE OF TECHNOLOGY, FINANCIAL, AND ANALYTICS

AUDIT REPORT - CONTINGENCY PLANNING EFFORTS FOR INFORMATION TECHNOLOGY MISSION SUPPORT SYSTEMS AT SELECTED DEPARTMENT OF ENERGY LOCATIONS

DOE-OIG-21-08
DECEMBER 2020

Department of Energy
Washington, DC 20585

December 14, 2020

Memorandum for the Under Secretary for Science
Acting Administrator, National Nuclear Security Administration

Sarah B. Nelson

From: Sarah B. Nelson
Assistant Inspector General
for Technology, Financial, and Analytics
Office of Inspector General

Subject: Audit Report on "Contingency Planning Efforts for Information Technology Mission Support Systems at Selected Department of Energy Locations"

What We Reviewed and Why

Information technology (IT) mission support systems and their related functions play a paramount role in the Department of Energy's ability to accomplish its day-to-day missions. However, information systems are vulnerable to a variety of disruptions ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Ensuring that IT support systems are available at critical moments can impact the Department's ability to withstand or recover from disruptions. Contingency planning supports this requirement through the establishment of thorough plans, procedures, and technical measures that enable a system to be recovered as quickly and effectively as possible following a service disruption. To prepare for a contingency, system owners should evaluate the organization's business processes and related support systems to identify the necessary steps to ensure availability or restoration of systems. Planning should also include an evaluation of system infrastructure requirements, security configurations, and backup information systems.

Because of the importance of the Department's missions, it is imperative that the Department understands the impact of potential disruptions on its computing environment and be able to maintain or restore its information systems and maintain operations, as appropriate. As such, we initiated this audit to determine whether the Department had adequately planned for the restoration of IT mission support systems and functions in accordance with established requirements to ensure functionality in the event of a disruption.

What We Found

The Department had not always adequately planned for the restoration of information systems in accordance with established requirements to ensure availability and functionality in the event of a disruption. Specifically, we found that three of the four sites reviewed had not fully implemented contingency planning requirements related to development of a Business Impact Analysis (BIA) as identified in Federal requirements. In addition, sites had not fully developed Information System Contingency Plans (ISCP) in accordance with Federal guidance for 10 of the 17 systems reviewed. Even when ISCPs were developed, some were missing key information pertaining to specific information systems. In light of the weaknesses identified, we made recommendations that, if fully implemented, should help the Department ensure its ability to maintain and/or recover information systems as quickly and effectively as possible.

Planning for Information System Disruptions

Contingency planning is designed to mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability. According to National Institute of Standards and Technology (NIST) Special Publication 800-34, Revision. 1, *Contingency Planning Guide for Federal Information Systems*, information system contingency planning applies to all information systems in Federal organizations. NIST details a seven-step process for effective contingency planning. Essential to the development of organization contingency planning is to conduct a BIA for each information system. This facilitates prioritizing the systems and processes based on impact level and develops priority recovery strategies for minimizing loss. The BIA also helps in the development of the other steps in the contingency planning process of identifying preventive controls, developing the ISCP, and developing effective testing, training, and exercises.

Contrary to NIST direction, we found that the locations reviewed had not always incorporated requirements into maintenance and restoration processes for IT mission support systems and related functions. In particular, we noted that in most cases BIAs were not fully developed in accordance with NIST. We also determined that a number of weaknesses existed related to the development of ISCPs.

Business Impact Analysis

The sites reviewed had not fully applied the risk-based process identified by NIST related to development of BIAs. A BIA determines how critical an information system or process is to the supported mission or business objectives and what impact the loss of the information system or process could have on the organization. In short, a BIA is a primary source for determining resiliency and contingency planning strategies. However, our test work identified that only 7 of 17 information systems reviewed at 4 sites contained system-specific BIAs. In particular, we found that system-level BIAs had not been developed for national security or unclassified systems at the Hanford Site and Oak Ridge National Laboratory (ORNL). Additionally, while the Pacific Northwest National Laboratory (PNNL) had developed BIAs for the two national security systems reviewed, it had not established BIAs for its unclassified systems. The systems

lacking BIAs at the sites reviewed served a variety of purposes including industrial control, core information technology infrastructure, and enterprise services.
Hanford had developed a BIA for the mission-essential support system identified in the site's Continuity of Operations Plan. However, site officials noted that BIAs for Hanford's non-essential systems were under development and had not yet been completed. Similarly, while PNNL's *Information System Contingency Plan* required development of BIAs, the site did not identify maximum system downtime or recovery priority for the two unclassified systems we reviewed.

Notably, four systems reviewed at Los Alamos National Laboratory and two systems reviewed at PNNL each had BIAs that included detailed descriptions of the computing environments, information for key individuals, detailed software and hardware listings, estimated cost of restoration, accumulated loss, and impact to site operations if systems/data were lost or disabled. Through the use of BIAs, an analysis of risk and related dependencies of information systems can help in the identification of non-obvious risks, gaps in an organization's operational processes and procedures, and resource requirements.

Information System Contingency Plans

We found that three of the four sites reviewed had not fully developed ISCPs in accordance with NIST Special Publication 800-34. According to NIST, if a contingency event causes a disruption to an information system, the ISCP will be utilized to coordinate and restore the affected system or service. The ISCP outlines system-specific recovery procedures, roles and responsibilities, inventory information, assessment procedures, and testing of the information systems. Based on our review, we determined a lack of progress related to development, implementation, and testing of contingency plans. In particular:

- ORNL was unable to provide system-specific ISCPs for two of the five systems reviewed, including its industrial control systems. For example, site officials had not developed an ISCP for industrial control systems which consisted of systems that operate and monitor utilities, emergency management, supervisory control and data acquisition, lighting, heating, ventilation, and air conditioning. While ORNL had a disaster recovery plan for the computing center, the plan did not include sufficient details for recovery procedures. Specifically, while the disaster recovery plan noted that several of the major infrastructure components had automatic failover, we noted that there were several applications that required manual failover. However, those processes and procedures were not fully detailed within the disaster recovery plan. Similarly, ORNL's national security systems ISCP did not include detailed recovery procedures or hardware components. Overall, we noted that system-specific activation and recovery procedures, and training requirements were not sufficiently detailed for four of the systems reviewed. Notably, ORNL provided ISCPs for its core financial system that adequately established procedures for backup and recovery.

- PNNL had not developed system-specific ISCPs for two of the four systems reviewed. While officials provided a single ISCP to cover all of the unclassified information systems reviewed, we determined that the document lacked critical elements necessary to meet Federal requirements. Specifically, the ISCP lacked system-specific details, including hardware and software inventories, names and contact information of technical team members, specific training requirements, cost recovery analysis, and equipment replacement strategies. To its credit, PNNL provided an ISCP for its national security systems that generally met Federal requirements.

- Although the Hanford Site had developed an ISCP for its business management system, the plan did not provide enough system-specific information to meet NIST requirements. In particular, our review found that the plan lacked details regarding system-specific hardware and training requirements.

To its credit, Los Alamos National Laboratory provided ISCPs for each of the four systems reviewed that included system-specific information, contact information for key individuals, recovery priorities and sequences, detailed inventories, site layout, and system-specific recovery procedures. As such, we concluded that overall the Los Alamos National Laboratory ISCPs reviewed were developed in accordance with Federal requirements.

Interpretation and Implementation of Requirements

The issues we identified related to the Department's IT mission support systems and functions were due primarily to inappropriate interpretations of contingency planning requirements by Federal and contractor officials. For instance, officials at two of the locations reviewed indicated that they had not developed BIAs or ISCPs because their locations did not maintain any mission-critical or mission-essential systems. At ORNL, for example, officials commented that the site had no mission-critical systems and that system continuity and continuity of operations is the best effort to restore operations. Contrary to this, NIST Special Publication 800-34 notes that "ISCPs apply to all information systems in Federal organizations" and that the BIA is a key step in implementing the contingency planning controls and in the overall contingency planning process.

In summary, contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level. However, as noted in our report, we identified shortcomings with three of the four sites' approaches to contingency planning. Because contingency planning is not an optional part of the business model and should be factored into the day-to-day operations within the Department, we believe that additional emphasis should be placed on ensuring that Federal requirements are met related to this area.

Impact to the Department

The weaknesses identified may negatively impact the availability of the Department's IT mission support systems in the event of a disruption. Without ensuring that current Federal requirements are met, the sites reviewed will maintain a less than fully effective information system contingency program. In addition, without thoroughly implementing and documenting the contingency planning process, Department officials may not be fully aware of current risks, threats, and impacts associated with the IT environment. As such, until the Department fully addresses the weaknesses identified within our report, its ability to maintain and/or recover information systems and functions in the event of a significant disruption may be negatively impacted.

What We Recommend

To improve contingency planning related to IT mission support systems and functions at the locations reviewed, we recommend that the Director, Office of Science, and Senior Advisor for Environmental Management to the Under Secretary for Science:

1. Ensure that BIAs are completed at PNNL, ORNL, and the Hanford Site in accordance with Federal requirements; and

2. Ensure that ISCPs for all systems at PNNL, ORNL, and the Hanford Site, including industrial control systems, are thoroughly completed in accordance with Federal requirements such as NIST Special Publication 800-34 and NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*.

Management Comments

Management concurred with the recommendations and indicated that corrective actions were planned to address the issues identified in the report. Management's formal comments are included in Appendix 3.

Office of Inspector General Response

Management's comments and planned corrective actions were responsive to the report's recommendations.

cc: Deputy Secretary
Chief of Staff

Appendix 1

Commonly Used Terms

Business Impact Analysis	BIA
Department of Energy	Department
Information System Contingency Plan	ISCP
Information Technology	IT
National Institute of Standards and Technology	NIST
Oak Ridge National Laboratory	ORNL
Pacific Northwest National Laboratory	PNNL

Objective, Scope, and Methodology

Objective

We conducted this audit to determine whether the Department of Energy had planned the maintenance and restoration process for information technology mission support systems and functions in accordance with established requirements to ensure functionality in the event of a disruption.

Scope

The audit was performed from September 2018 through September 2020. We conducted work at Department Headquarters in Washington, DC and Germantown, Maryland; the Hanford Site and Pacific Northwest National Laboratory in Richland, Washington; Los Alamos National Laboratory in Los Alamos, New Mexico; and Oak Ridge National Laboratory in Oak Ridge, Tennessee. The review was limited to evaluating the contingency planning process for information technology mission support systems and functions in accordance with Federal requirements. The audit was conducted under Office of Inspector General project number A18TG046.

Methodology

To accomplish our objective, we:

- Reviewed prior audits and related recommendations to determine what corrective actions had been taken, if applicable.

- Reviewed applicable laws, regulations, policies, and procedures, including those issued by the National Institute of Standards and Technology.

- Interviewed relevant Department program and site officials.

- Reviewed applicable documentation related to the planning and implementation of the Department's sustainment of information technology mission support functions.

- Assessed Headquarters' direction to programs and site offices related to implementation and oversight of the Department's process for sustaining information technology mission support functions.

- Determined how the assurance of information technology mission support functions are implemented at the field sites.

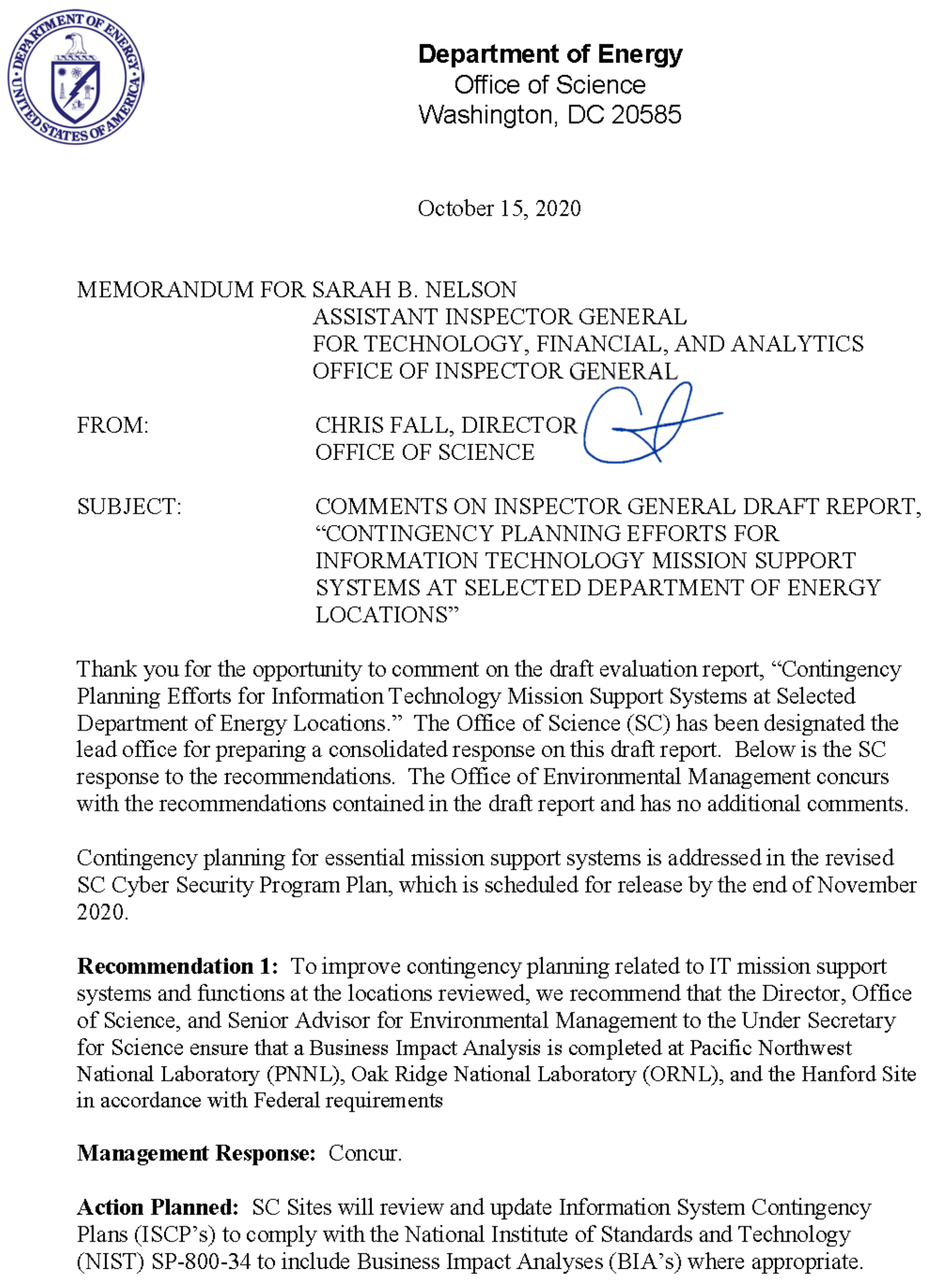
- Assessed a judgmental sample of information systems at the sites reviewed to determine the effectiveness related to contingency planning efforts. Because our sample was judgmental our results are limited to the items tested and results cannot be projected to the entire population.

We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusion based on our objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We used computer-processed data to satisfy our objective, and, overall, we determined that the computer-processed data used could be relied upon to support our decisions and recommendations.

Management waived an exit conference on November 5, 2020.

Appendix 3

Management Comments



Department of Energy
Office of Science
Washington, DC 20585

October 15, 2020

MEMORANDUM FOR SARAH B. NELSON
ASSISTANT INSPECTOR GENERAL
FOR TECHNOLOGY, FINANCIAL, AND ANALYTICS
OFFICE OF INSPECTOR GENERAL

FROM: CHRIS FALL, DIRECTOR
OFFICE OF SCIENCE

SUBJECT: COMMENTS ON INSPECTOR GENERAL DRAFT REPORT, "CONTINGENCY PLANNING EFFORTS FOR INFORMATION TECHNOLOGY MISSION SUPPORT SYSTEMS AT SELECTED DEPARTMENT OF ENERGY LOCATIONS"

Thank you for the opportunity to comment on the draft evaluation report, "Contingency Planning Efforts for Information Technology Mission Support Systems at Selected Department of Energy Locations." The Office of Science (SC) has been designated the lead office for preparing a consolidated response on this draft report. Below is the SC response to the recommendations. The Office of Environmental Management concurs with the recommendations contained in the draft report and has no additional comments.

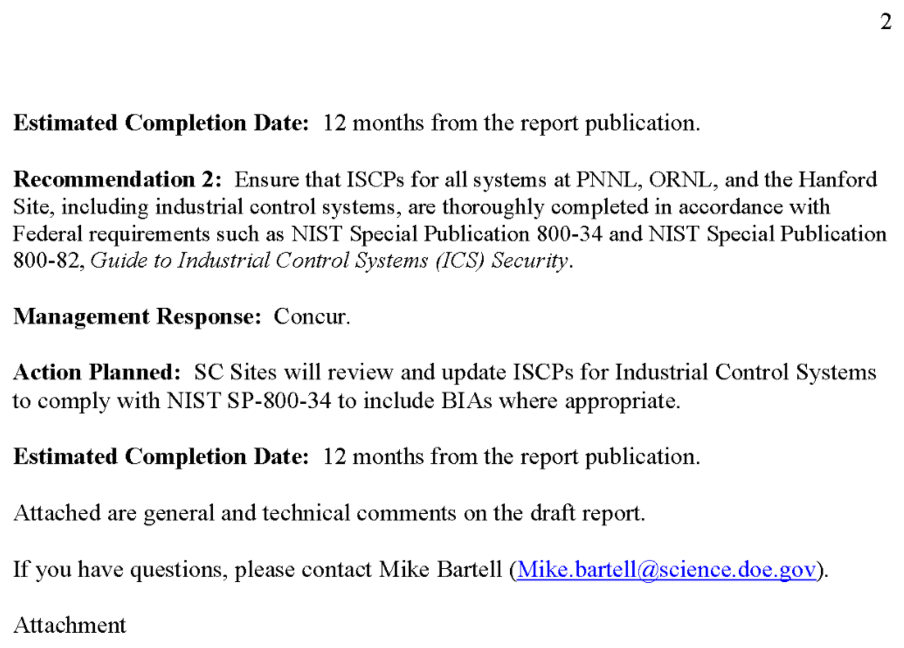
Contingency planning for essential mission support systems is addressed in the revised SC Cyber Security Program Plan, which is scheduled for release by the end of November 2020.

Recommendation 1: To improve contingency planning related to IT mission support systems and functions at the locations reviewed, we recommend that the Director, Office of Science, and Senior Advisor for Environmental Management to the Under Secretary for Science ensure that a Business Impact Analysis is completed at Pacific Northwest National Laboratory (PNNL), Oak Ridge National Laboratory (ORNL), and the Hanford Site in accordance with Federal requirements

Management Response: Concur.

Action Planned: SC Sites will review and update Information System Contingency Plans (ISCP's) to comply with the National Institute of Standards and Technology (NIST) SP-800-34 to include Business Impact Analyses (BIA's) where appropriate.

Appendix 3



Estimated Completion Date: 12 months from the report publication.

Recommendation 2: Ensure that ISCPs for all systems at PNNL, ORNL, and the Hanford Site, including industrial control systems, are thoroughly completed in accordance with Federal requirements such as NIST Special Publication 800-34 and NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*.

Management Response: Concur.

Action Planned: SC Sites will review and update ISCPs for Industrial Control Systems to comply with NIST SP-800-34 to include BIAs where appropriate.

Estimated Completion Date: 12 months from the report publication.

Attached are general and technical comments on the draft report.

If you have questions, please contact Mike Bartell (Mike.bartell@science.doe.gov).

Attachment

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.