Office of Inspector General

OFFICE OF TECHNOLOGY, FINANCIAL, AND ANALYTICS

AUDIT REPORT -

THE OFFICE OF ENVIRONMENTAL MANAGEMENT'S

MISSION INFORMATION PROTECTION PROGRAM

Department of Energy
Washington, DC 20585

July 21, 2021

Memorandum for the Acting Assistant Secretary for Environmental Management

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

Subject: Audit Report on "The Office of Environmental Management's Mission Information Protection Program"

What We Reviewed and Why

The Department of Energy's Office of Environmental Management (Environmental Management) was created to prepare for and manage the cleanup efforts resulting from decades of the Department's nuclear weapons development and nuclear energy research. Information technology systems have become vital to the successful execution of its cleanup mission and operations. To enhance Environmental Management's information assurance and cybersecurity posture, the Mission Information Protection Program (MIPP) was formed to conduct a variety of activities including, but not limited to, independent cybersecurity assessments of Environmental Management field sites through testing and validation of security controls; procuring enterprise cybersecurity tools; providing mission support cybersecurity services; and providing Information System Security Officer support for Environmental Management Headquarters. MIPP's cybersecurity professionals are divided into the Headquarters Security System (HQSS) and Information Security Continuous Monitoring (ISCM) teams. The HQSS team assists sites in sharing and mitigating vulnerabilities and detecting malicious activity through the Environmental Management Continuous Monitoring Center. The ISCM team serves as an independent evaluator conducting cybersecurity site assessments and assistance visits within Environmental Management. During our audit, we conducted a full review of the ISCM team and a limited review of the HQSS team. No immediate issues came to our attention related to the HQSS function; therefore, we focused our review on the ISCM team.

Environmental Management sites relied on the ISCM team to assist with their annual tests of security controls. From fiscal year (FY) 2017 through FY 2019, the ISCM team was tasked to conduct cybersecurity reviews at seven sites. The ISCM process was designed to ensure that all security controls are tested over a 3-year period and that Environmental Management

Headquarters and its sites remained informed of potential cybersecurity issues at the locations reviewed by the ISCM team. During recent audit work performed at two Environmental Management field sites, the Office of Inspector General identified cybersecurity program weaknesses in numerous security control areas. Although the ISCM team previously assessed the two locations' cybersecurity programs, we identified additional weaknesses and noted that the issues previously identified by the ISCM team continued to exist. The weaknesses identified at those sites indicated potentially systemic problems related to the adequacy of Environmental Management's MIPP ISCM evaluations and the program's response to the results of the evaluations.

We initiated this audit to determine whether MIPP provided effective and efficient services while meeting its goals and objectives.

What We Found

We did not identify any issues with the MIPP HQSS component during our limited testing. However, we determined that the ISCM function had not always provided effective and efficient services or fully met its goals and objectives. Specifically, the ISCM team had not always ensured that issues identified through its assessments were appropriately carried forward for evaluation and followup testing in subsequent years. Furthermore, we found that over 400 weaknesses documented within ISCM assessment reports had not been recorded in Environmental Management's central tracking system to ensure that key program officials had an accurate picture of the organization's overall cybersecurity and risk posture.

Followup of Assessment Report Issues

MIPP ISCM personnel had not always ensured that cybersecurity weaknesses identified within assessment reports were included in subsequent site reviews to determine whether they were adequately addressed by site management. Specifically, at the time of our review, we found that 181 of 1,592 (11 percent) weaknesses identified at 7 Environmental Management locations in FY 2017 and FY 2018 had not been included in followup testing during the subsequent site evaluations. For example, ISCM cybersecurity assessments conducted at the Hanford Site in FY 2017 identified one security requirement and/or control related to contingency planning that had not been implemented for a national security system boundary. However, subsequent reviews of the same boundary performed by the ISCM team did not include any information related to the previous test and evaluation results of the control or the implementation status of the previously identified weakness. Similarly, an assessment performed in FY 2018 on 1 of the Portsmouth/Paducah Project Office's general support systems found 19 security weaknesses during the period under review related to areas such as system security plans and developer security testing and evaluation; however, these controls were not reassessed in the subsequent year to determine if corrective actions had been taken.

Environmental Management officials disputed our analysis and indicated that reported "Areas for Improvement" (AFIs) should not have been included in subsequent assessments.

Specifically, officials noted that AFIs were only issued for the Authorizing Official[1] to make an implementation decision and did not require followup by the ISCM team. Contrary to Environmental Management's assertion, we noted that followup of AFIs was inconsistent. Specifically, except for where included in the 181 instances noted above, we found that the ISCM team generally followed up on AFIs from year to year. In addition, Environmental Management policy did not provide any distinction between "Not Implemented Controls" and AFIs related to any differences in treatment as weaknesses. In fact, Environmental Management's Risk Management Approach Implementation Plan stated that continuous monitoring assessment-discovered weaknesses that recommend further corrective action must be tracked. As AFIs provided recommendations to site management, we conclude that they should have been consistently included for followup in subsequent years. To their credit, Environmental Management officials stated that they recently changed how the ISCM team issued reports and how weaknesses were identified.

The issues related to the followup of assessment report weaknesses occurred, in part, because Environmental Management officials had not fully developed program documentation necessary to support the MIPP ISCM mission or ensure its effective operations. In particular, Environmental Management officials had not established well-defined documentation related to MIPP's objectives, scope, or testing and monitoring activities. For instance, the Risk Management Approach Implementation Plan briefly described MIPP's high-level support of the Environmental Management enterprise. In addition, the contract deliverables required the MIPP contractor to develop a Standard Operating Procedure. However, the documents delivered under the contract were limited to data collection and teleconferencing procedures, were not specific to MIPP cybersecurity assessments, and did not document procedures for followup activities. Notably, the task for MIPP support was recently moved to leverage the Department's Office of the Chief Information Officer's Business Operations Support Services contract vehicle. At that time, the list of deliverables was updated to include more detail and contained specific mechanisms through which the deliverables would be managed and reviewed. The enhancements made by Environmental Management related to contract deliverables, coupled with remediation of the issues identified during our review, should ensure effective contract execution related to MIPP ISCM operations.

Corrective Actions

Although MIPP ISCM assessment results were provided to certain Headquarters and site officials, weaknesses were not always formally tracked to ensure progress toward the completion of corrective actions. Specifically, we determined that 426 weaknesses that required corrective action and were older than 90 days had not been recorded in Environmental Management's central tracking system by site officials, as required. Headquarters officials utilized the tracking system to gain visibility into deficiencies discovered through audits and continuous monitoring activities and to monitor the progress in correcting those deficiencies through a plan of action and milestones (POA&M). Environmental Management sites were responsible for establishing a POA&M entry in the central tracking system for any assessment-discovered weaknesses that

---

[1] The Authorizing Official is a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations, assets, and individuals.

required more than 90 days to correct. Because sites had not tracked the 426 reported weaknesses noted above, it was unlikely that stakeholders had an accurate view of the overall cybersecurity and risk posture for Environmental Management's systems and data and may have been unable to effectively ensure that weaknesses at various locations were addressed.

The issues related to corrective actions were due, in part, to the lack of a formalized process to ensure that the assessment reports' results were adequately shared and communicated, as well as to ensure the full implementation of the Risk Management Approach Implementation Plan. Specifically, Environmental Management Headquarters officials had not established a monitoring process to ensure that weaknesses identified and documented within MIPP ISCM assessment reports were entered into the central POA&M tracking system by site officials. Without this information, senior management officials may have been unaware of security deficiencies existing within Environmental Management authorization boundaries and unable to monitor the progress of corrective efforts.

Notably, Environmental Management officials took significant actions subsequent to the period covered by our review to improve the organization's cybersecurity posture, including enhancing communication. For instance, officials stated that as part of their maturing risk management process, they began to provide Headquarters Field Operations officials with a copy of the final ISCM reports in March 2020 for each site reviewed. In addition, they established quarterly POA&M meetings with the sites and developed cybersecurity scorecards to help improve communication related to cybersecurity weaknesses. Furthermore, in a prior report, we recommended that Environmental Management develop and implement a process to ensure that ISCM assessment findings were entered into the POA&M tracking system. Environmental Management officials agreed and noted that implementation of process improvements had been taken. These actions, if effectively implemented, should address the communication issues identified during our review.

Impact to the Department

Without improvements, Environmental Management's information systems and data may be exposed to a higher-than-necessary risk of compromise, loss, modification, and/or non-availability. For example, weaknesses identified during MIPP ISCM assessments could continue to exist if followup activities are not completed to ensure that vulnerabilities were remediated. Similarly, future planning and prioritization of limited resources to ensure adequate protection of systems and information could be adversely affected if identified weaknesses and related corrective actions are not appropriately tracked. In addition, officials throughout the organization may be unaware of Environmental Management boundaries' security posture, the program-level risk, proposed mitigations, and/or planned corrective actions to address identified weaknesses.

What We Recommend

In a prior report, we recommended that Environmental Management develop and implement a process to ensure that weaknesses identified and documented within ISCM assessment reports were entered into the central POA&M tracking system and communicated. Environmental Management officials indicated during our current review that corrective actions had been taken.

To help further improve the management of MIPP and enhance Environmental Management's cybersecurity posture, we recommend that the Acting Assistant Secretary for Environmental Management:

1. Ensure that documentation, such as a standard operating procedure, is developed to fully define the MIPP ISCM team's objectives, scope, and day-to-day operating expectations, including the need to follow up on weaknesses previously identified during its assessments.

Management Comments

Management concurred with the report's recommendation and indicated that corrective actions were taken to address the issues identified in the report. However, management questioned the accuracy of several numbers in our report related to tracking and followup of AFIs.

Office of Inspector General Response

Management's corrective actions were responsive to the report's recommendation. In response to management's assertion that our analysis was inaccurate, we validated our results using additional information provided by Environmental Management officials and updated the report's numbers accordingly. As noted in the report, we found that the MIPP ISCM team generally followed up on AFIs annually and determined that they should have been consistently included for follow up in subsequent years. Management's comments are included in Appendix 4.

Attachments

cc: Deputy Secretary
    Chief of Staff

Appendix 1

Commonly Used Terms

Areas for Improvement	AFIs
Department of Energy	Department or DOE
Fiscal Year	FY
Headquarters Security System	HQSS
Information Security Continuous Monitoring	ISCM
Mission Information Protection Program	MIPP
Office of Environmental Management	Environmental Management
Plan of Action and Milestones	POA&M

Objective, Scope, and Methodology

Objective

We conducted this audit to determine whether the Office of Environmental Management's Mission Information Protection Program (MIPP) provided effective and efficient services while meeting its goals and objectives.

Scope

The audit was performed from December 2019 through April 2021 at the Office of Environmental Management's Headquarters in Washington, DC. The scope of the audit included Department of Energy and the Office of Environmental Management contractor activities related to MIPP project management, program cost and budget, and cybersecurity technical and compliance reviews. This assessment was conducted under Office of Inspector General project number A20TG004.

Methodology

To accomplish our objective, we:

- Reviewed laws, regulations, and program guidance applicable to MIPP and cybersecurity;

- Held discussions with Department officials, including various Federal and contractor personnel regarding the goals, objectives, and resources of MIPP;

- Reviewed documentation pertaining to MIPP contracts, including contract requirements, deliverables, and status reports related to technical support services, cyber analysis, and information technology system cyber monitoring;

- Reviewed relevant reports issued by the Office of Inspector General related to MIPP and cybersecurity; and

- Evaluated Information Security Continuous Monitoring Assessment Reviews developed by the MIPP Information Security Continuous Monitoring team.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed whether control activities and the underlying principles of control activities design and implementation had been implemented. However, because our review was limited to this

internal control component and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit. We did not rely on computer-processed data to satisfy our audit objective.

An exit conference was held with Department management on June 29, 2021.

Prior Reports

- Audit Report on *Management of a Department of Energy Site Cybersecurity Program* (DOE-OIG-21-07, December 2020). The site had not implemented an effective cybersecurity program in accordance with Federal and Department of Energy requirements. Our review identified control weaknesses in each of the 14 control families tested as described in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Due to the sensitive nature of the vulnerabilities identified during our audit, the report issued to the Department was for Official Use Only. We provided site and program officials with detailed information regarding vulnerabilities that we identified.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2019* (DOE-OIG-20-12, November 2019). The Department, including the National Nuclear Security Administration, had made progress remediating weaknesses identified in our fiscal year 2018 evaluation, which resulted in the closure of 21 of 25 (84 percent) prior year recommendations. Although these actions were positive, our evaluation identified weaknesses that were consistent with our prior reports related to vulnerability management, configuration management, system integrity of web applications, access controls and segregation of duties, cybersecurity and privacy training, and security control testing and continuous monitoring.

- Management Alert on *Management of Cybersecurity Activities at a Department of Energy Site* (DOE-OIG-19-44, August 2019). Results of test work conducted at the site revealed potentially significant cybersecurity vulnerabilities on the site's general support system, including major financial management and safety applications. Eleven recommendations have been made to the site's manager to help improve its cybersecurity program. Due to the sensitive nature of the vulnerabilities identified, the management alert issued to the Department was for Official Use Only.

- Audit Report on *Management of a Department of Energy Site Cybersecurity Program* (DOE-OIG-19-42, July 2019). The site had not fully implemented its cybersecurity program in accordance with Federal and Department requirements. Weaknesses existed related to vulnerability and configuration management, logical and physical access controls, contingency planning, and continuous monitoring. Due to the sensitive nature of the vulnerabilities identified during our audit, the report issued to the Department was for Official Use Only. We provided site and program officials with detailed information regarding vulnerabilities that we identified.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2018* (DOE-OIG-19-01, October 2018). The Office of Inspector General found weaknesses that were mostly consistent with our prior reports related to vulnerability and configuration management, system integrity of web applications, access controls, security awareness and

training, and security control testing. Test work uncovered access control weaknesses at four locations related to the disablement of user accounts, inadequate use of least privilege and/or segregation of duties, and a lack of adequate enforcement of access controls on web applications. The weaknesses identified occurred, in part, because Department officials had not fully developed and/or implemented policies and procedures related to cybersecurity training and vulnerability and configuration management programs.

Management Comments

EM-2020-001167

Department of Energy
Washington, DC 20585
June 14, 2021

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

FROM: WILLIAM I. WHITE
       ACTING ASSISTANT SECRETARY
        FOR ENVIRONMENTAL MANAGEMENT

SUBJECT: Response to the Office of the Inspector General Draft Audit
       Report entitled: *Office of Environmental Management's Mission*
       Information Protection Program (A20TG004)

The Office of Environmental Management (EM) appreciates the opportunity to provide a
management response to the Office of the Inspector General's (IG) Draft Audit Report
titled, *"Office of Environmental Management's Mission Information Protection
Program" (A20TG004)*.

The IG has issued one recommendation for the Acting Assistant Secretary for
Environmental Management in this audit. EM concurs with the IG's recommendation
and has established the attached formal Standing Operating Policy and Procedures on
Information System Continuous Monitoring and on Quarterly Plan of Action and
Milestone Reviews. These actions close the recommendation. EM has outlined several
factual inaccuracies within the draft report in the attachment provided. Please consider
updating the Report consistent with this feedback.

The IG should direct any questions to Ms. Jeanne Beard, Director, Office of Information
Systems, Office of Environmental Management, at (202) 586-0200 or at
jeanne.beard@em.doe.gov.

Attachments

2

MANAGEMENT RESPONSE
IG Draft Audit Report
Office of Environmental Management's Mission Information Protection Program
(A20TG004)

Recommendation 1:

Ensure that documentation, such as standard operating procedures, is developed to fully define the Mission Information Protection Program (MIPP) Information System Continuous Monitoring (ISCM) team's objectives, scope, and day-to-day operating expectations, including the need to follow up on weaknesses previously identified during its assessments.

Management Response: Concur

EM has created formal EM Headquarters (HQ) Standing Operating Policy and Procedures (SOPPs) to address the IG's recommendation, including:

- EM MIPP ISCM SOPP to define the ISCM team's objectives, scope, and day-to-day operating expectations.
- Quarterly Plan of Action & Milestone (POA&M) Review SOPP for scheduling and conducting Quarterly Plan of Action & Milestone (POA&M) Reviews at the boundary level, including reviewing all active POA&Ms and following up on weaknesses identified during previous assessments.

Estimated Completion Date: Completed

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.