



OFFICE OF INSPECTOR GENERAL

U.S. ENVIRONMENTAL PROTECTION AGENCY

CUSTOMER SERVICE ★ INTEGRITY ★ ACCOUNTABILITY

Operating efficiently and effectively

EPA's Emergency Response Systems at Risk of Having Inadequate Security Controls

Report No. 21-E-0226

September 13, 2021



Report Contributors: LaSharn Barnes
Rudolph M. Brevard
Nii-Lantei Lamptey
lantha Maness
Christina Nelson
Teresa L. Richardson
Albert E. Schmidt

Abbreviations:

CISO	Chief Information Security Officer
EPA	U.S. Environmental Protection Agency
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OLEM	Office of Land and Emergency Management
OMS	Office of Mission Support
ORD	Office of Research and Development
SP	Special Publication
SSP	System Security Plan

Key Definition: System Security Plan Provides an overview of the security requirements of an information system by documenting the system’s security categorization and the controls in place to protect the system and its data, as well as the system’s confidentiality, integrity, and availability.

Cover Image: The EPA’s information systems did not have proper security controls because the Agency did not adhere to federal guidance when determining security categorizations. (EPA OIG image)

Are you aware of fraud, waste, or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, D.C. 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our [OIG Hotline](#).

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, D.C. 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our [Email Updates](#)
Follow us on Twitter [@EPAoig](#)
Send us your [Project Suggestions](#)



Office of Inspector General U.S. Environmental Protection Agency **At a Glance**

21-E-0226
September 13, 2021

Why We Did This Evaluation

We performed this evaluation to determine whether the system security plans in the Office of the Chief Financial Officer, the Office of Land and Emergency Management, and the Office of Research and Development are developed and updated in accordance with National Institute of Standards and Technology guidance.

System security plans are required for all information systems. The National Institute of Standards and Technology states that major applications require “special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.” The plans should document an information system’s security categorization and include an inventory of the system’s minor applications, which are similar to major applications but do not require “special attention.”

This evaluation supports an U.S. Environmental Protection Agency mission-related effort:

- *Operating efficiently and effectively.*

This evaluation addresses top EPA [management challenges](#):

- *Complying with key internal control requirements (data quality).*
- *Enhancing information technology security.*

Address inquiries to our public affairs office at (202) 566-2391 or OIG_WEBCOMMENTS@epa.gov.

[List of OIG reports.](#)

EPA’s Emergency Response Systems at Risk of Having Inadequate Security Controls

What We Found

The EPA did not follow the National Institute of Standards and Technology guidance in determining and documenting the justification for the security categorizations of five emergency response systems. Further, the EPA’s security categorization process did not include key participants, as recommended by NIST. In addition, security documentation for some of the EPA’s minor applications did not exist.

If the availability and integrity of emergency response system data are jeopardized, it could harm the EPA’s ability to coordinate response efforts to protect the public from environmental disasters.

NIST requires that agencies develop system security plans for all information systems, including major applications and general support systems, and tailor the systems’ security controls based on the systems’ security categorization. A system with a high-security categorization would require greater security controls than a system with a moderate- or low-security categorization. NIST guidance provides that security controls specific to minor applications should be documented in a system security plan as an appendix or in a paragraph. NIST also provides that all applications be secure and free of vulnerabilities.

The EPA’s staff and managers may not fully understand NIST requirements because the Agency’s security training does not cover the NIST security categorization process. The EPA’s security categorization guidance referenced NIST but did not describe the steps EPA personnel should take to implement NIST guidance. Additionally, the EPA has not implemented controls or oversight to assure that NIST guidance was followed. EPA systems are more vulnerable to security threats if the Agency does not follow NIST guidance when categorizing security levels for systems or documenting system security. Such threats could compromise a system’s data and negatively impact the EPA’s ability to respond to emergencies.

Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Land and Emergency Management implement controls to follow NIST guidance when conducting system categorizations. We recommend that the assistant administrator for Research and Development implement a process to list and describe all minor applications in the appropriate system security plan. We also recommend that the assistant administrator for Mission Support provide role-based training that covers system security categorizations and implement a process to document that tools and models are secure. The Agency concurred with five of the seven recommendations and provided acceptable corrective actions and estimated milestone dates. Two recommendations remain unresolved with resolution efforts in progress.



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

THE INSPECTOR GENERAL

September 13, 2021

MEMORANDUM

SUBJECT: EPA's Emergency Response Systems at Risk of Having Inadequate Security Controls
Report No. 21-E-0226

FROM: Sean W. O' Donnell

A handwritten signature in blue ink that reads "Sean W O'Donnell".

TO: Lynnann Hitchens, Acting Principal Deputy Assistant Administrator
Office of Mission Support

Barry Breen, Acting Assistant Administrator
Office of Land and Emergency Management

Wayne E. Cascio, MD, Acting Principal Deputy Assistant Administrator for Science
Performing Delegated Duties of Assistant Administrator
Office of Research and Development

This is our report on the subject evaluation conducted by the U.S. Environmental Protection Agency's Office of Inspector General. The project number for this evaluation was [OA&E-FY20-0176](#). This report contains findings that describe the problems the OIG has identified and the corrective actions the OIG recommends. Final determinations on the matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The Office of Land and Emergency Management, the Office of Research and Development, and the Office of Mission Support are responsible for the issues described in the report. In accordance with EPA Manual 2750, your offices provided corrective actions for Recommendations 1, 2, 3, 6, and 7. These recommendations are resolved.

Action Required

Recommendations 4 and 5 are unresolved. The resolution process, as described in the EPA's Audit Management Procedures, begins immediately with the issuance of this report. Furthermore, we request a written response to the final report within 60 days of this memorandum. Your response will be posted on the OIG's website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

This report will be posted to our website at www.epa.gov/oig.

Table of Contents

Chapters

1	Introduction.....	1
	Purpose.....	1
	Background.....	1
	Responsible Offices	4
	Scope and Methodology.....	4
	Prior Report	5
2	Not Following NIST Guidelines Created a Risk that Emergency Response Systems Are Not Fully Secured	6
	NIST and EPA Provide Guidance for Determining and Documenting Security Categorizations for Information Systems	6
	EPA Did Not Fully Adhere to NIST Guidance When Assigning Security Categories.....	7
	OLEM Did Not Include CISO and Mission Owners in Categorization Process	8
	OLEM Did Not Document Its Determinations and Decisions or Select Applicable Information Types.....	8
	EPA Did Not Fully Implement NIST Categorization Process Due to Lack of Training and Oversight Controls	9
	EPA Systems, Including Those Used for Emergency Response, Are at Risk of Not Having Sufficient Security Controls.....	10
	Conclusions.....	10
	Recommendations.....	11
	Agency Response and OIG Assessment.....	11
3	Security Needs to be Documented for EPA’s Minor Applications, Tools, and Models.....	13
	NIST and EPA Provide Guidance for Documenting Security for Minor Applications Within SSPs	13
	ORD and OLEM Did Not Document Security Controls for Nonmajor Applications.....	14
	ORD and OLEM Do Not Have Process to Verify that Security Is Documented for Nonmajor Applications	15
	Security Breaches of Nonmajor Applications Could Impact EPA’s Ability to Complete Mission-Related Activities.....	15
	Conclusions.....	15
	Recommendations.....	16
	Agency Response and OIG Assessment.....	16
	Status of Recommendations.....	17

Appendixes

A	Federal Information Processing Standards Publication 199 Defined Impact Levels.....	18
B	Description of Information Technology Officials’ Roles.....	19
C	Description of Major Applications	20
D	OMS’s Response to Draft Report	21
E	OLEM’s Response to Draft Report	24
F	ORD’s Response to Draft Report.....	27
G	Distribution	29

Chapter 1

Introduction

Purpose

The Office of Inspector General of the U.S. Environmental Protection Agency [initiated](#) this evaluation to determine whether the system security plans, or SSPs, in the Office of the Chief Financial Officer; the Office of Land and Emergency Management, or OLEM; and the Office of Research and Development, or ORD, are developed and updated in accordance with the standards published by the National Institute of Standards and Technology, or NIST.

Top Management Challenges Addressed

This evaluation addresses the following top management challenge for the Agency, as identified in OIG Report No. [20-N-0231](#), *EPA's FYs 2020–2021 Top Management Challenges*, issued July 21, 2020:

- Complying with key internal control requirements (data quality).
- Enhancing information technology security.

Background

In accordance with the Federal Information Security Management Act of 2002, each federal agency is required to develop, document, and implement an information security program for the information and information systems that support the operations and assets of the agency. An SSP provides an overview of the security requirements of the information system by documenting the system's security categorization and the controls in place to protect the system and its data, as well as the system's confidentiality, integrity, and availability. Per NIST, the "authorizing official," such as a senior federal official or executive, needs to approve the SSP and formally authorize the operation of the information system. The SSP also provides a summary of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. These plans need to be updated regularly to accurately reflect the current state of the system. All information systems must be covered by an SSP and labeled as either a major application or a general support system. Systems include both major and minor applications.

An *authorization to operate* documents management's explicit acceptance of the risk of the loss of a system's confidentiality, integrity, or availability, as well as impacts to organizational operations, organizational assets, individuals, other organizations, and the United States based on the implementation of an agreed-upon set of security controls.

NIST states that both major and minor applications require:

[A]ttention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

The primary difference between major and minor applications are that major applications, because of the information they contain,

NIST defines an application as a "software program hosted by an information system." NIST defines a general support system as an "interconnected set of information resources under the same direct management control that shares common functionality."

require special (or extra) management oversight and an SSP. While SSPs are required for major applications, a minor application does not need its own SSP because minor applications are normally a part of a general support system or can be interconnected to a major application. A major application's and a general support system's SSP should include an inventory of all connected minor applications and document the controls in place to protect the data in those minor applications.

Tools and models are a group of applications that are not required to have an SSP; however, NIST provides that all applications—including tools and models—require protection.

System Categorization

Prior to developing an SSP, the information and information system must be categorized. All federal agencies are required to categorize their information and information systems using NIST's Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*. This requires categorizing the security objectives—confidentiality, integrity, and availability—of information and information systems as low, moderate, or high. These provisional impact levels are based on the potential impact of loss if there is a security breach. Appendix A describes the potential impact for each security level. A single, overall security categorization is then selected for the entire system.

The NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Revision 1, Volume I, provides an overview of the security categorization process (Table 1). Identifying the type of the information processed within an information system is essential for selecting the proper security controls the system should have and for ensuring the confidentiality, integrity, and availability of the system and its information.

Information types are specific categories of information. Examples of information types include budget formulation, emergency management, and pollution prevention and control information.

A federal agency's information system security officer assigns information systems a provisional security categorization—low, moderate, or high—based on the types of information the system contains. This provisional security categorization is then reviewed and adjusted, as appropriate, by senior management based on the system's organization, environment, mission, use, and data sharing using special factors provided by NIST. Security categorization is instrumental in determining the system's security impact level. The rationale or justification for these adjustments must be documented if the security categorization selected is lower than what is recommended by NIST. The overall security categorization of an information system will dictate which security controls should be included in the control tailoring process, wherein the Agency determines the security controls that will be used to protect the system.

Table 1: NIST SP 800-60 Volume I Security Categorization Process Roadmap

Process step	Activities	Participants*
Identify information types	Agencies must identify and document all of the information types (as defined within NIST SP 800-60 Volume II) based on the data or function of the system.	Mission owners and information owners
Select provisional impact levels	Agencies should use the information types identified in Step 1 to establish the system's provisional impact levels. The provisional impact levels (high, medium, or low) are the original impact levels assigned to each security objective (confidentiality, integrity, and availability) as provided within NIST SP 800-60 Volume II, without any adjustments. Also, the initial security categorization for the information type is established and documented.	Information system security officer
Review provisional impact levels and adjust and finalize information impact levels	Agencies should (1) review the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing; (2) adjust the security objective impact levels as necessary using the "special factors" found in NIST SP 800-60 Volume II, Appendixes C and D; and (3) document the rational or justification for all adjustments to the impact levels.	Information system security officer, senior agency information security officer,** mission owners, and information owners
Assign system security category	Agencies should: <ul style="list-style-type: none"> Review the identified security categorizations for each information type identified in Step 1. Determine the system security categorization by identifying the high-water mark for each of the security objectives (confidentiality, integrity, and availability) based on the aggregate of the information types. For example, if confidentiality is listed as low for one information type and high for the other information type in the same system, the high-water mark would be high for confidentiality. Adjust the high-water mark for each system security objective, as necessary. Assign the overall information system impact level based on the highest impact level for the system security objectives. Document all security categorization determinations and decisions. 	Chief information officer, information system security officer, senior agency information security officer, mission owners, and information owners

Source: OIG analysis of NIST SP 800-60. (EPA OIG table)

* Appendix B contains the description of the roles of the participants.

** The EPA's chief information security officer is equivalent to the senior agency information security officer, the term used in NIST SP 800-60 Volume I, Table 3.

Tailoring Security Controls

Agencies use the system security level identified during the security categorization process described above to determine the baseline security controls that are necessary to protect the information and the information system. The baseline security controls are identified during the control tailoring process, as set forth in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. After selecting the appropriate security control baseline, the agency should align the system's security controls to meet the security categorization's requirements. This is accomplished by using the NIST process for tailoring baseline security controls that includes leveraging compensating security controls.

A compensating security control is a control employed by an organization in lieu of a NIST-required security control that provides the same or comparable protection.

NIST SP 800-53, Revision 4, states:

The set of security controls in the security plan must be sufficient to adequately mitigate risks to organizational operations and assets, individuals, other organizations, and the Nation based on the organizational risk tolerance.

Per NIST, “all federal applications require some level of protection,” including tools and models. For example, NIST SP 800-163, Revision 1, *Vetting the Security of Mobile Applications*, states:

[Mobile applications] can pose serious security risks to an organization and its users due to vulnerabilities that may exist within their software. Such vulnerabilities may be exploited to steal information, control a user’s device, deplete hardware resources, or result in unexpected app or device behavior.

A vulnerability is a weakness that can be accidentally triggered or intentionally exploited, resulting in a negative impact to confidentiality, integrity, or availability.

Responsible Offices

The Office of Mission Support leads the EPA’s information management and information technology programs, which provide services to support the Agency’s mission to protect human health and the environment. Within the OMS, the chief information officer is responsible for establishing minimum mandatory risk-based technical, operational, and management information security control requirements for the Agency’s information and information systems.

The Office of the Chief Financial Officer is responsible for information technology planning, developing, and deploying financial systems for the Agency. OLEM provides policy, guidance, direction, and oversight for the Agency’s hazardous waste management, underground storage tanks, brownfields, and accidental oil and chemical release programs. The ORD provides the data, tools, and information that form the scientific foundation that the Agency relies on to fulfill its mission to protect the environment and safeguard public health.

As owners of the information systems that we reviewed, the Office of the Chief Financial Officer, OLEM, and the ORD are responsible for developing SSPs, categorizing their respective information systems properly within the respective SSPs, revising the security control assessments within the respective SSPs, and reviewing SSPs annually.

Scope and Methodology

We conducted this evaluation from April 2020 to June 2021 in accordance with the *Quality Standards for Inspection and Evaluation* published in January 2012 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we perform the evaluation to obtain sufficient, competent, and relevant evidence to provide a reasonable basis for our findings, conclusions, and recommendations based on our objective. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations.

We reviewed special publications and federal information processing standards issued by NIST. We also reviewed federal and EPA criteria related to system security planning. We requested a comprehensive list of all ORD, OLEM, and Office of the Chief Financial Officer systems and their SSPs. These offices own 22 major applications and general support systems that require SSPs. This includes three ORD systems, 11 OLEM systems, and eight Office of the Chief Financial Officer systems.

We reviewed the 22 SSPs to evaluate whether they contained:

- A security categorization level consistent with the function of the system.
- Consideration of 11 security controls and control enhancements related to remote access based on the security categorization listed in the SSP. These 11 controls were judgmentally selected due to the impact of agencywide telework resulting from the coronavirus pandemic.

We interviewed system owners and other Agency personnel responsible for developing, maintaining, reviewing, and approving the 22 SSPs. We performed substantive test work to determine whether the EPA followed NIST procedures for determining a system’s security categorization for six OLEM systems whose categorization we determined to be questionable based on the function of the systems. Specifically, five of these systems were related to emergency response functions, but all six received a moderate- or low-security categorization instead of a high-security categorization.

While verifying that the Office of the Chief Financial Officer, the ORD, and OLEM provided a comprehensive list of all systems, we determined that the ORD and OLEM had additional applications that were listed in the EPA’s system inventory. We determined that the ORD and OLEM had 83 minor applications and 41 tools and models (Table 2).

Table 2: Number of ORD and OLEM minor applications, tools, and models

Type of application	ORD	OLEM	Total
Minor applications	70	13	83
EPA tools and models	38	3	41
Total	108	16	124

Source: OIG analysis of OLEM and ORD information. (EPA OIG table)

Prior Report

In Report No. [18-P-0217](#), *Management Alert: To Minimize Risk of Environmental Harm, the Security Categorization of Electronic Manifest System Data Needs to Be Re-Evaluated*, issued June 21, 2018, we identified problems with the categorization of the e-Manifest system. Specifically, the EPA categorized the sensitivity of the information within its e-Manifest system at such a low level that the required security controls would not protect the information within the system to minimize the risk of environmental harm. The e-Manifest system was designed to track the shipment of hazardous waste from a generator’s site to another site for disposition, and a breach of the system may facilitate terrorist or other criminal activities. Personnel responsible for categorizing the sensitivity of the system and its information did not sufficiently consider homeland security implications as they relate to chemicals of interest. Also, the EPA did not consider further uses of the system, such as by first responders in the event of an incident involving transport of waste. In June 2020, we concluded that the EPA completed corrective actions for all recommendations in this report.

Chemicals of interest are hazardous chemicals that the U.S. Department of Homeland Security wants to keep out of the hands of those who would misuse them.

Chapter 2

Not Following NIST Guidelines Created a Risk that Emergency Response Systems Are Not Fully Secured

The EPA did not follow federal requirements, used to establish the level of system security controls, when assigning security categories for information systems. Specifically, the EPA did not adhere to the process set forth in the NIST standards and guidelines for determining security categorizations, did not involve key stakeholders in the categorization process, and did not fully document its categorization determinations and decisions. The EPA's security training and guidance did not explain the NIST security categorization process and the EPA had not implemented control measures to help ensure that the system security categorization process complied with federal requirements. As a result, five EPA emergency response systems were at risk of being categorized too low and not having sufficient security controls in place to protect the integrity and availability of the data in those systems during an emergency.

NIST and EPA Provide Guidance for Determining and Documenting Security Categorizations for Information Systems

Federal and EPA guidance requires information and information systems to be categorized according to the level of security controls needed to adequately protect the systems. NIST SP 800-60 Volume I provides an overview of the security categorization process.

The Process Roadmap in NIST SP 800-60 Volume I (Table 1), describes the four major steps in the security categorization process and the roles that key stakeholders have in this process. A system's mission owners should be involved in multiple steps of the categorization process, including helping to identify all the information types stored or produced by a system. Chief information security officers, or CISOs, play key roles throughout the process, including assigning the system security level and documenting the security categorization determinations and decisions. The documentation should address consideration of the risk factors outlined in NIST guidance. Appendix B describes the roles of the various stakeholders who are included in the security categorization process.

Similarly, the EPA's *Information Security – Risk Assessment Procedures*, CIO 2150-P-14.2, dated April 11, 2016, states that information and information systems shall be categorized in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance. This includes adhering to the NIST SP 800-60 requirements for the security categorization process. Additionally, the results and rationale for the categorization should be documented in the SSP.

We reviewed OLEM's 11 SSPs for compliance with the NIST security categorization requirements. We found that six of the SSPs had inconsistencies per the systems' descriptions, information types contained in the system, and the system's security categorization. The following section provides the results of our analysis of these six systems, which are described in Appendix C.

EPA Did Not Fully Adhere to NIST Guidance When Assigning Security Categories

We found that the EPA did not adhere to the NIST SP 800-60 Process Roadmap when assigning security categories for six of OLEM’s information systems (Table 3). Specifically, the EPA did not:

- Include the CISO and mission owners in the security categorization process. The CISO indicated that the CISO’s team reviews the authorization to operate packages—which include SSPs that document results of the categorization process—to determine whether everything looks complete and right, but the CISO does not specifically participate in the categorization process, as defined by the NIST Process Roadmap.
- Select and document all applicable information types, per Step 2 of the Process Roadmap (Table 1). Information systems can have multiple information types, and all applicable information types need to be selected.
- Select the appropriate provisional impact levels associated with the applicable information types, per Step 3 of the Process Roadmap (Table 1).
- Document the decisions and justifications for downgrading the selected provisional impact levels, per Step 4 of the Process Roadmap (Table 1).

During a meeting with OLEM to discuss our findings, we asked whether OLEM would be willing to find a third party with the proper expertise to provide oversight of the categorization process, such as the CISO’s office. OLEM agreed to that solution, if the CISO’s office is willing. Further, OLEM added that the CISO does not give an opinion because the CISO does not know the systems’ data like the program office but that it is willing to try to include the CISO in its process. Further, OLEM’s information security officer stated that users of a system do not take part in the system categorization and would not know or be expected to know enough about information security to be able to do that if asked.

Table 3: Steps EPA did not fully adhere to when providing security categorization

System and assigned security level*	Step 1: Were Information types documented in the SSP?	Step 1: Were all applicable information types documented in the SSP?	Step 2: Were the correct provisional levels selected?	Step 3: Were downgrades to selected provisional levels documented?	Were mission owners and the CISO involved during the categorization process?
EPA OSC (low)	Yes	No	No	N/A	No
Scribe.NET (low)	Yes	No	No	N/A	No
WebEOC (low)	Yes	No	No	N/A	No
VIPER (low)	Yes	No	No	N/A	No
EMP (moderate)	Yes	No	No	No	No
Contaminated Site Cleanup IC LAN (low)	Yes	Yes	No	No	No

Source: OIG analysis based on NIST SP 800-60 Process Roadmap. (EPA OIG table)

* System descriptions are in Appendix C.

Note: OSC is On-Scene Coordinator, WebEOC is Web Emergency Operations Center, EMP is Emergency Management Portal, and IC LAN is Information Contractor Local Area Network.

The SSPs for all six information systems stated that their security categorization level was at a level lower than high. As described in NIST SP 800-60 Volume II, emergency response systems should start with a high provisional categorization for the integrity and availability security objectives. If these

provisional categorizations are downgraded during the categorization process, the rationale for these decisions needs to be documented.

Categorization of these systems at a higher level would have required the Agency to use higher-level baseline security controls before the control tailoring process. The implementation of the controls must be sufficient to adequately mitigate risks to organizational operations and assets, individuals, other organizations, and the nation.

OLEM Did Not Include CISO and Mission Owners in Categorization Process

The EPA did not include mission owners and the CISO during the system categorization process, as prescribed by NIST. The CISO told us that the only categorization issue brought to the CISO's attention was when the OIG reported concerns regarding the security controls over the Agency's e-Manifest system.¹ OLEM representatives stated that the mission owner's role is not defined or included within the EPA's policies and procedures. According to the CISO, the OMS's Office of Information Security and Privacy staff review authorization to operate packages that contain SSPs submitted by the EPA's program and regional offices to determine whether the plans look complete and correct.

OLEM Did Not Document Its Determinations and Decisions or Select Applicable Information Types

OLEM did not fully adhere to the NIST security categorization Process Roadmap in a number of ways. First, OLEM determined that the provisional security categorization rating of the Emergency Management Portal would be high, yet the final categorization was reduced to moderate without documenting a justification within the SSP to demonstrate that all information types had been considered. The system owner said that the system was downgraded because OLEM's and the Office of Emergency Management's security personnel did not think it needed a high-security categorization; they did not consider it to be similar to other systems with a high-security categorization like the Office of Enforcement and Compliance Assurance's agent management type systems, the water filtration/purification type systems, or air systems.

Second, five of the six plans failed to select all applicable information types as required in the Process Roadmap. For example, VIPER, Scribe.NET, EPA On-Scene Coordinator, Emergency Management Portal, and Web Emergency Operations Center are used during emergency responses, but the Agency did not select the D.4.4 Emergency Response information type during the security categorization process for those systems.² NIST requires that all applicable information types be selected for the information system. By failing to select all the appropriate

NIST SP 800-60, Revision 1, Volume II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, recommends that systems used for emergency response have a provisional categorization of high for the impact levels of both integrity and availability. That information type is D.4.4-Emergency Response. While emergency response systems have a low provisional categorization for confidentiality, special factors may warrant a confidentiality impact level of moderate or high.

¹ OIG, *Management Alert – To Minimize Risk of Environmental Harm, the Security Categorization of Electronic Manifest System Data Needs to Be Re-Evaluated*, Report No. [18-P-0217](#), June 21, 2018.

² NIST SP 800-60, Revision 1, Volume II defines the D.4.4 Emergency Response information type as involving “the immediate actions taken to respond to a disaster (e.g., wildfire management).”

information types, these SSPs did not fully consider whether a higher security categorization was warranted.

The Contaminated Site Cleanup Information Contractor Local Area Network SSP listed information types, such as research and development and environmental remediation, as low even though NIST recommends that those information types have a provisional rating of moderate. The SSP did not explain why these information types were assigned a low rating instead of a moderate rating. The Agency either selected the wrong security categorization or failed to document the reasoning for downgrading the system to a lower security level than what NIST recommends.

EPA Did Not Fully Implement NIST Categorization Process Due to Lack of Training and Oversight Controls

Training on the security categorization process could improve compliance with NIST requirements. We reviewed the training materials provided by the CISO and determined that the training materials did not make any reference to security categorization instructions. The CISO indicated that the CISO's office plans to include security categorization in future role-based training, further confirming that it is not included in the training. If this training is updated to include the security categorization process, individuals responsible for security categorization would learn how the security categorization process works.

Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, states that management is "responsible for establishing and maintaining internal controls to achieve specific internal control objectives related to operations, reporting, and compliance."

OLEM said that using compensating security controls could reduce the security categorization of a system. For example, OLEM categorized the Web Emergency Operations Center as low because OLEM receives the same information from the U.S. Coast Guard via telephone, a compensating security control. However, compensating security controls are not to be applied and considered until after the categorization process is completed. While receiving information via telephone could be considered a compensating security control, it should not change the system's security categorization. Lack of training prevented OLEM from understanding that compensating security controls do not impact the security categorization and caused OLEM to not justify implementing required controls.

As previously discussed and set forth in NIST SP 800-53, compensating security controls are used during the control tailoring process and not the security categorization process. Without reviewing all applicable baseline controls, the Agency cannot be sure that the compensating security controls address all the higher-level controls that need to be considered during control tailoring.

Further, OLEM was unaware of how to include all participants in the categorization process. OLEM management stated that the CISO reviews the system categorization findings of the system owner, who is solely responsible for the system categorization determination. However, the CISO reviews authorization to operate packages that contain an SPP.

In addition, the EPA lacked internal controls to oversee the security categorization process to help program offices follow NIST standards and guidelines during the categorization process. For example, some of the internal controls that were lacking include:

- Developing and implementing policies and procedures requiring:
 - Responsible parties to adhere to the activity steps as outlined in the NIST SP 800-60 Process Roadmap.
 - Responsible parties to adhere to all documentation requirements of the Process Roadmap.
- Documenting that all relevant stakeholders—including mission owners and the CISO—are involved in the security categorization process, as required by the Process Roadmap.
- Defining and documenting who holds the mission owner role.
- Reviewing listings of program missions and determining which systems support the mission, such as emergency response, as well as determining whether the system security categorization is appropriate for the supported mission. The CIO has to conduct this review.

NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, describes *mission owner* as the senior official within an organization with specific mission or line of business responsibilities and that has a security or privacy interest in the organizational systems supporting those missions or lines of business.

The implementation of oversight controls provides assurance that the NIST security categorization is followed and that systems have sufficient controls in place to protect the data in those systems.

EPA Systems, Including Those Used for Emergency Response, Are at Risk of Not Having Sufficient Security Controls

By not adhering to the activity steps and documentation requirements outlined in the NIST SP 800-60 Process Roadmap and by not involving key stakeholders in the decision-making process, the EPA is at risk of categorizing the six systems listed in Table 3 too low. Our review showed that when OLEM performed the control tailoring process for five of its systems, it only documented consideration of the baseline controls for the level the system was assessed—either low or moderate—and not the higher level. If OLEM selected a higher-security categorization, it would have been required to consider additional controls during the control tailoring process.

The availability and integrity of the data in these systems could be jeopardized, impeding the EPA’s ability to respond to emergencies. Not fulfilling emergency management responsibilities and activities in a timely manner could harm individuals and the EPA’s ability to respond to emergencies.

Conclusions

Not adhering to NIST’s applicable standards and guidelines when assigning security categories used to establish system security controls for its emergency response systems could impact the accuracy of the security categorizations for some of the EPA’s emergency response systems and result in selecting weak security controls to protect the systems. Information and information systems should be categorized according to the level of security controls needed to adequately protect the systems, according to federal requirements and EPA directives.

Recommendations

We recommend that the assistant administrator for Land and Emergency Management:

1. Implement controls to follow National Institute of Standards and Technology guidance when conducting systems categorizations by:
 - a. Involving the appropriate key stakeholders, including mission owners and the chief information security officer, during the system security categorization process as prescribed in the National Institute for Standards and Technology Special Publication 800-60 Volume I, Table 3, Process Roadmap.
 - b. Having responsible parties adhere to all activity steps as outlined in the National Institute for Standards and Technology Process Roadmap, including selecting all application information types applicable to information systems.
 - c. Having responsible parties document the security categorization determinations and decisions within system security plans as provided in the National Institute for Standards and Technology Process Roadmap, including documenting all downward adjustments to provisional security levels.
2. Reevaluate the system security categorizations for the EPA On-Scene Coordinator, Scribe.NET, Web Emergency Operations Center, VIPER, Contaminated Site Cleanup Information Contractor Local Area Network, and Emergency Management Portal systems in accordance with National Institute of Standards and Technology guidelines. Adjust security categorizations as appropriate based on those evaluations.

We recommend that the assistant administrator for Mission Support:

3. Follow Agency guidance and implement controls to update the EPA's security categorization guidance to include the chief information security officer when adjusting the provisional security categorization and determining the final security categorization, as prescribed in the National Institute for Standards and Technology Process Roadmap.
4. Update the EPA's security categorization guidance to define and include the role of the mission owner.
5. Develop and provide role-based training to individuals who have security responsibilities for National Institute of Standards and Technology system security categorization.

Agency Response and OIG Assessment

OLEM and the OMS concurred with Recommendations 1, 2, and 3. Both of the offices provided acceptable planned corrective actions with estimated milestone dates. We consider these recommendations resolved with corrective actions pending.

The OMS did not concur with Recommendations 4 and 5 and stated that in accordance with NIST guidance, the senior information officials are assigned to the mission owner role and that the OMS had

created security training to comply with federal role-based training requirements. We requested support to show that the senior information officials are assigned to the mission owner role and that the role-based security training covers requirements for system security categorization. The OMS was unable to provide the support. We consider Recommendations 4 and 5 unresolved with resolution efforts in progress. The OMS's response to the draft report is in Appendix D, and OLEM's response to the draft report is in Appendix E.

Chapter 3

Security Needs to be Documented for EPA's Minor Applications, Tools, and Models

Not all of the ORD's and OLEM's minor applications were documented in their associated major applications' or general support systems' SSPs. Minor applications are not required to have their own SSPs, but NIST standards and guidelines provide that security controls specific to minor applications should be documented in the SSP of a major application or general support system. Security for smaller applications, such as tools and models, does not need to be documented within an SSP, but NIST provides that all applications should be secure and free of vulnerabilities. Neither NIST nor the EPA expressly addresses security documentation for tools and models, and EPA policies and procedures do not provide a mechanism to document security controls for tools and models. Without specific internal controls on security documentation, the Agency cannot verify that tools and models are protected against vulnerabilities in systems, hardware, or software.³

Factors contributing to a lack of security documentation for minor applications, tools, and models—referred to collectively as nonmajor applications—included:

- The ORD and OLEM not having a process for verifying that security was documented for all minor applications, as well as for tools and models.
- The application inventory listings not identifying the major applications or general support system that the minor applications were connected to or supported.
- The EPA's system development life cycle excluding tools and models.

These nonmajor applications help the EPA carry out its missions. Without proper documentation for nonmajor applications, the EPA would be unaware of whether systems are properly secure and can carry out the EPA's missions, such as remediating disaster sites.

NIST and EPA Provide Guidance for Documenting Security for Minor Applications Within SSPs

NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, dated February 2006, states:

Agencies are expected to exercise management judgment in determining which of their applications are minor applications and to ensure that the security requirements of minor applications are addressed as part of the system security plan for the applicable general support systems or, in some cases, the applicable major application.

³ Office of Management and Budget Circular A-123 and U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government* (September 2014) provide that it is incumbent upon management to have policies in place to effectively monitor whether internal controls are operating effectively, as well as addressing and reducing risks.

The EPA’s *Information Security – Interim Planning Procedures*, Version 3.6, CIO 2150.3-P-12.1, dated July 17, 2012, also provides that SSPs must identify all minor applications that the information system supports and address the security requirements for those minor applications.

ORD and OLEM Did Not Document Security Controls for Nonmajor Applications

The ORD did not document security controls for 70 of its 108 nonmajor applications (Table 4). Specifically:

- 70 of the ORD’s nonmajor applications were not documented within an SSP. These nonmajor applications included 24 hosted in the National Computer Center’s Hosting Environment, seven hosted in the ORD General Support System, and one hosted in the vendor’s cloud environment.
- Of the 70 nonmajor applications without security control documentation, 38 were EPA-developed tools and models. Tools and models must be protected even if they do not have to be included in an SSP.

NIST SP 800-18 states that security controls are “The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.”

Table 4: ORD’s nonmajor (minor) application security documentation

Application	Does not have security control documentation	Has security documentation	Total
Minor application in the National Computer Center’s hosting environment	24	7	31
Minor application in the ORD General Support System	7	27	34
Minor application in a vendor’s cloud environment	1	4	5
ORD’s tools and models	38	0	38
TOTAL	70	38	108

Source: OIG analysis of ORD information. (EPA OIG table)

OLEM did not document the existence of security controls for five of its 16 nonmajor applications (Table 5). Specifically:

- Three of OLEM’s minor applications were not documented within an SSP. These minor applications included two hosted in the National Computer Center’s Hosting Environment and one hosted in the vendor’s cloud environment.
- Three of OLEM’s tools and models (minor applications) hosted in a vendor’s cloud environment were not documented within the SSP.

Table 5: OLEM nonmajor security applications’ security control documentation

Application	Does not have security control documentation	Has security documentation	Total
Minor application in the National Computer Center’s hosting environment	2	7	9
Minor application in a vendor’s cloud environment	1	3	4
EPA tools and models	3	0	3
TOTAL	6	10	16

Source: OIG analysis of OLEM and OMS information. (EPA OIG table)

ORD and OLEM Do Not Have Process to Verify that Security Is Documented for Nonmajor Applications

Minor Applications

The ORD and OLEM do not have a process—such as validating a comprehensive inventory—to verify that minor applications are documented or described within associated SSPs. Three of OLEM’s minor applications without security documentation were hosted in a vendor’s cloud environment. The SSP for the vendor’s cloud environment only addresses the environment and not the security of the hosted applications. While OLEM may not be able to modify the vendor’s SSP, it can create its own appendix to the vendor’s SSP.

For each minor application, the ORD did not follow best practices by recording the corresponding major application or general support system in an internal application inventory database. Listing the hosting environment in an internal application inventory database would allow the EPA to easily identify where it should document the applications’ controls. In response to the discussion documents we issued to the Agency, the ORD updated its internal application inventory database to list each minor application’s associated major application or general support system.

Tools and Models

The EPA’s *System Life Cycle Management Procedure*, CIO 2121-P-03.1, dated July 7, 2005, establishes the Agency’s approach for planning, developing, and managing information technology systems, applications, and solutions. This procedure is intended to assure that the Agency’s System Life Cycle Management approach is consistent with EPA and federal information technology planning, management, and acquisition requirements, including those related to security. Small applications, including tools and models, are not covered by the life cycle management procedure. The OMS developed and documented a process, dated March 6, 2020, for securing small applications during their development, but this process has not been incorporated into the EPA’s *Life Cycle Management Procedure*.

Security Breaches of Nonmajor Applications Could Impact EPA’s Ability to Complete Mission-Related Activities

By not documenting the security controls established for nonmajor applications, the EPA does not have reasonable assurance that these items are protected from threats that could compromise the availability or integrity of data. Compromises to the data could hamper the EPA’s ability to complete its missions. For example, the EPA’s Incident Waste Decision Support Tool, an ORD minor application, does not have security documentation. This application is used to manage waste resulting from natural disasters, like hurricanes or tornados, or following a terrorist attack. If this application does not have the proper security controls, remediation efforts could be hampered because of waste removal delays.

Conclusions

The ORD and OLEM do not document security controls for all nonmajor applications. NIST SP 800-18 provides that security controls specific to minor applications should be documented in an SSP. The ORD and OLEM do not have a process for verifying that minor applications were documented within their

associated SSPs. Further, since the OMS does not implement procedures for reviewing and documenting security for nonmajor applications, the EPA would be unaware of whether those systems are secure or able to carry out the Agency's missions, such as the remediation of disaster sites.

Recommendations

We recommend that the assistant administrator for Research and Development:

6. Develop and implement a process to list and describe all minor applications in the appropriate system security plan.

We recommend that the assistant administrator for Mission Support:

7. Implement a process to document that tools and models are secure.

Agency Response and OIG Assessment

The ORD concurred with Recommendation 6, and the OMS concurred with Recommendation 7. Both offices provided acceptable corrective actions with planned completion dates. We consider the recommendations resolved with corrective actions pending. The OMS's response to the draft report is in Appendix D, and the ORD's response to the draft report is in Appendix F.

Status of Recommendations

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status ¹	Action Official	Planned Completion Date
1	11	<p>Implement controls to follow National Institute of Standards and Technology guidance when conducting systems categorizations by:</p> <p>a. Involving the appropriate key stakeholders, including mission owners and the chief information security officer, during the system security categorization process as prescribed in the National Institute for Standards and Technology Special Publication 800-60 Volume I, Table 3, Process Roadmap.</p> <p>b. Having responsible parties adhere to all activity steps as outlined in the National Institute for Standards and Technology Process Roadmap, including selecting all application information types applicable to information systems.</p> <p>c. Having responsible parties document the security categorization determinations and decisions within system security plans as provided in the National Institute for Standards and Technology Process Roadmap, including documenting all downward adjustments to provisional security levels.</p>	R	Assistant Administrator for Land and Emergency Management	6/30/22
2	11	Reevaluate the system security categorizations for the EPA On-Scene Coordinator, Scribe.NET, Web Emergency Operations Center, VIPER, Contaminated Site Cleanup Information Contractor Local Area Network, and Emergency Management Portal systems in accordance with National Institute of Standards and Technology guidelines. Adjust security categorizations as appropriate based on those evaluations.	R	Assistant Administrator for Land and Emergency Management	6/30/22
3	11	Follow Agency guidance and implement controls to update the EPA's security categorization guidance to include the chief information security officer when adjusting the provisional security categorization and determining the final security categorization, as prescribed in the National Institute for Standards and Technology Process Roadmap.	R	Assistant Administrator for Mission Support	4/15/22
4	11	Update the EPA's security categorization guidance to define and include the role of the mission owner.	U	Assistant Administrator for Mission Support	
5	11	Develop and provide role-based training to individuals who have security responsibilities for National Institute of Standards and Technology system security categorization.	U	Assistant Administrator for Mission Support	
6	16	Develop and implement a process to list and describe all minor applications in the appropriate system security plan.	R	Assistant Administrator for Research and Development	5/31/22
7	16	Implement a process to document that tools and models are secure.	R	Assistant Administrator for Mission Support	10/15/21

¹ C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

Federal Information Processing Standards Publication 199 Defined Impact Levels

Level	Definition	Description
Low	“The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.”	“A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.”
Moderate	“The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.”	“A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.”
High	“The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.”	“A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.”

Source: Extractions from Federal Information Processing Standards Publication 199. (EPA OIG table)

Description of Information Technology Officials' Roles

Information technology role	NIST position description
Senior agency information security officer (referred to as the EPA's chief information security officer)	Responsible for the requirements under the Federal Information Security Management Act of 2002 and serves as the liaison to the agency's authorizing officials, information system owners, and information system security officers (NIST 800-18).
Information system security officer	Responsible for maintaining security for an information system or program (NIST 800-18).
Mission owners	Senior officials with specific mission responsibilities. Have a security or privacy interest in the organizational systems supporting those missions (NIST 800-37).
Information owners	Have authority for specified information and "responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal" (NIST 800-18).

Source: OIG analysis of NIST 800-18 and NIST 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*. (EPA OIG table)

Description of Major Applications

System name	Description
EPA On-Scene Coordinator	Website that provides links to resources and site profiles to support on-scene coordinators for emergency responses and time-critical removal and remedial site activities.
Scribe.NET	Web-based system used by EPA emergency response and removal personnel and contractors to create labels and Chain of Custody Reports for air, water, soil, and biota samples during emergency response and remediation activities.
Web Emergency Operations Center	System that manages the collection and dissemination of response information to authorized EPA Emergency Operations Center users. It is used to keep all members of an Emergency Operations Center updated with real-time information. It can also be used for day-to-day activities to manage routine, nonemergency-related operations. The real-time nature of information in the system allows for timely, informed decisions.
VIPER	A wireless network-based communications system designed to enable real-time transmission of the levels of hazardous materials in the air and water from field sensors to a local computer, remote computer, or enterprise server for data management, analysis, and visualization. It has been used in emergencies, such as hurricanes, and for national events, including the Super Bowl.
Contaminated Site Cleanup Information Contractor Local Area Network	A series of websites that provide information about treatment and site characterization technologies to the hazardous waste remediation community.
Emergency Management Portal	Portal that provides the EPA's emergency management staff access to the information they need to respond to emergencies. It provides a single access point to increase coordination while responding to emergencies. For example, it provides responders access to its "Sampling-Monitoring & Analysis" module to collate regional sampling and monitor information, as well as to present information to subject matter experts for review during incidents of national significance, such as chemical and oil spills.

Source: OIG analysis of documentation from the different systems. (EPA OIG table)

OMS's Response to Draft Report



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

July 15, 2021

OFFICE OF MISSION SUPPORT

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report Project No. OA&E-FY20-0176
"EPA's Emergency Response Systems at Risk of Having Inadequate Security Controls,"
dated June 17, 2021

FROM: Vaughn Noga, Deputy Assistant Administrator for Environmental Information and Chief Information Officer
Noga,
Vaughn

Digitally signed by Noga,
Vaughn
Date: 2021.07.15
09:42:27 -04'00'

TO: LaSharn Barnes, Director
Information Resources Management
Office of Inspector General

Thank you for the opportunity to respond to the subject audit report. The following summarizes the OMS's overall position, along with its position on each of the report recommendations. We have provided high-level intended corrective actions for each recommendation with completion dates.

OMS POSITION

The Office of Mission Support's Office of Information Security and Privacy (OMS/OISP) concurs with recommendations #3 and #7 as outlined in the Office of Inspector General's Draft Report and has developed corrective actions to address them. They are listed below. OMS/OISP disagrees with recommendations #4 and #5 and have provided our justification below.

OMS RESPONSE TO REPORT RECOMMENDATIONS

Agreements

No.	Recommendation	High-Level Intended Corrective Actions	Estimated Completion
3	Follow Agency guidance and implement controls to update the EPA's security categorization guidance to include the chief information security officer when adjusting the provisional security categorization and determining the final security categorization as prescribed in the National Institute	OMS/OISP is in the process of updating the "Information Security - Risk Assessment Procedure" from NIST SP 800-53, Revision 4 to Revision 5 and will ensure that security control RA-2, <i>Security Categorization</i> , is updated to reflect required approvals for adjusted security categorizations by the Program/Regional Office Senior Information Official (SIO),	April 15, 2022

Internet Address (URL) • <http://www.epa.gov>

No.	Recommendation	High-Level Intended Corrective Actions	Estimated Completion
	for Standards and Technology categorization Process Roadmap.	serving as the Authorizing Official and the mission owner, and the Chief Information Security Officer.	
7	Implement a process to document that tools and models are secure.	<p>OMS/OISP is in the process of updating the "Information Security - Planning Procedure" from NIST SP 800-53, Revision 4 to Revision 5 and will ensure that security control PL-2, <i>System Security and Privacy Plans</i>, is updated to reflect the requirement to document all nonmajor applications, including all minor applications, tools, and models. Additionally, the agency will take the following corrective actions:</p> <p>1.1 Ensure the EPA's Registry of EPA Applications, Models and Data Warehouses (READ) - or other applicable agency master inventory tool - is updated by all system owners to capture all major and nonmajor applications and systems.</p>	October 15, 2021

Disagreements

No.	Recommendation	High-Level Intended Corrective Actions	Estimated Completion
4	Update the EPA’s security categorization guidance to assign the role of the mission owner.	<p>The role of mission owner has been assigned to the Senior Information Official (SIO).</p> <p>The draft report (Appendix B – Description of Information Technology Officials) quotes NIST SP 800-37 in that a ‘mission owner’ is “Senior officials with specific mission responsibilities and has a security or privacy interest in the organizational systems supporting those missions.”</p> <p>NIST SP 800-37, revision 2 (December 2018) lists this role as part of the Authorizing Official (Appendix D – Roles and Responsibilities). “Authorizing officials typically have budgetary oversight for the system or are responsible for the mission and/or business operations supported by the system.”</p>	N/A
No.	Recommendation	High-Level Intended Corrective Actions	Estimated Completion
		<p>The EPA Roles and Responsibilities Procedure Document (https://www.epa.gov/sites/production/files/2013-11/documents/cio-2150-3-p-19-1.pdf) specifically states that the Senior Information Official (SIO) carries out the duties of Authorizing Official.</p>	
5	Develop and provide role-based training to individuals who have security responsibilities for National Institute of Standards and Technology system security categorization.	OISP created a Security Training Program in FedTalent to ensure compliance with Federal role-based training requirements. Included in this program is a course entitled, Security Controls, which covers requirements for system security categorization.	N/A

OLEM's Response to Draft Report



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

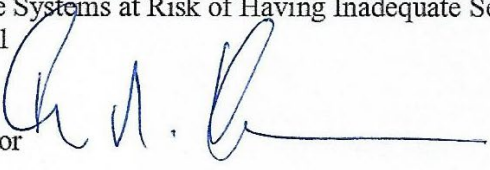
WASHINGTON, D.C. 20460

July 16, 2021

OFFICE OF
LAND AND EMERGENCY
MANAGEMENT

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OA&E-FY20-0176
"EPA's Emergency Response Systems at Risk of Having Inadequate Security
Controls" dated June 17, 2021

FROM: Barry N. Breen
Acting Assistant Administrator 

TO: Sean W. O'Donnell
Inspector General
Office of Inspector General

Thank you for the opportunity to respond to the issues and recommendations in the subject audit report. Following is a summary of the Office of Land and Emergency Management's (OLEM) overall position, along with its position on each of the OLEM-assigned report recommendations. For your consideration, we have included a technical comment to supplement this response.

OLEM'S OVERALL POSITION

OLEM does not concur with the Office of Inspector General's (OIG) view that the OLEM systems listed in the report are miscategorized. OLEM believes we have selected a Federal Information Security Modernization Act classification appropriate for the level of impact to the organization and its employees. National Institute of Standards and Technology (NIST) Special Publication 800-60 Section 4.3 indicates that information types only provide "provisional security impact levels, the agency should review the appropriateness of the provisional impact levels in the context of the organization, environment, mission, use, and data sharing associated with the information system under review".

OLEM observes that the documentation included in the system security plan developed by the system owner may not sufficiently explain the role of the system as it relates to EPA's primary mission and fully describe the rationale for the Low categorization. OLEM will be reviewing the security classification assessments, following the NIST SP 800-60 process, document all

adjustments to the impact levels and provide the rationale or justification for the adjustments. These actions are captured in the corrective actions below.

AGENCY’S RESPONSE TO REPORT RECOMMENDATIONS

Agreements

No.	Recommendation	High-Level Intended Corrective Action(s)	Estimated Completion by Quarter and FY
1	<p>1. Implement controls to follow National Institute of Standards and Technology guidance when conducting systems categorizations by:</p> <p>a. Involving the appropriate key stakeholders, including mission owners and the chief information security officer, during the system security categorization process as prescribed in the National Institute for Standards and Technology Special Publication 800-60, Volume I, Table 3, “Process Roadmap.”</p> <p>b. Having responsible parties adhere to all activity steps as outlined in the National Institute for Standards and Technology Process Roadmap, including selecting all application information types applicable to information systems.</p> <p>c. Having responsible parties document the security categorization determinations and decisions within system security plans as provided in the National Institute for Standards and Technology Process Roadmap, including documenting all</p>	<p>During the annual system categorization review, OLEM system owners will expand the participation to include mission owners (if the agency process includes this new role), key stakeholders, and OLEM system security officers following the process as prescribed in the National Institute for Standards and Technology Special Publication 800-60, Volume I, Table 3, “Process Roadmap.”</p> <p>The group will document all security categorization determinations including all downward adjustments to provisional security levels. The Chief Information Security Officer (CISO) will review this documentation as part of the Authority to Operate (ATO) approval process.</p>	3 rd Quarter FY 2022

	downward adjustments to provisional security levels.		
2	Re-evaluate the system security categorizations for the EPA On-Scene Coordinator, Scribe.NET, Web Emergency Operations Center, VIPER, Contaminated Site Cleanup Information Contractor Local Area Network, and Emergency Management Portal systems in accordance with National Institute of Standards and Technology guidelines. Adjust security categorizations as appropriate based on those evaluations.	OLEM will direct the system owners for these systems to convene system categorization re-evaluations and include mission owners, key stakeholders, and OLEM system security officers in the review. The review will follow the process as prescribed in the National Institute for Standards and Technology Special Publication 800-60, Volume I, Table 3, "Process Roadmap." The group will document all security categorization determinations including all downward adjustments to provisional security levels. The CISO will review this documentation as part of the ATO approval process.	3 rd Quarter FY 2022
6	Develop and implement a process to list and describe all minor applications in the appropriate system security plan.	OLEM currently follows and will continue to follow, the agency's process to list and describe minor applications, which are hosted by the agency's General Support Systems (GSS.) OLEM does not have its own GSS that hosts its minor applications.	N/A

ORD's Response to Draft Report

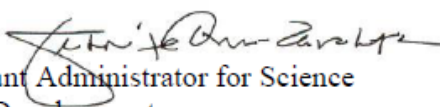


UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

July 8, 2021

MEMORANDUM

SUBJECT: Response to Office of Inspector General (OIG) Draft Report No. OA&E-FY20-0176 "EPA's Emergency Response Systems at Risk of Having Inadequate Security Controls" dated June 17, 2021

FROM: Jennifer Orme-Zavaleta 
Principal Deputy Assistant Administrator for Science
Office of Research and Development

TO: Sean W. O'Donnell
Inspector General
Office of Inspector General

The EPA's Office of Research and Development (ORD) appreciates the opportunity to review and comment on the OIG's Draft Report titled "*EPA's Emergency Response Systems at Risk of Having Inadequate Security Controls*" (Project No. OA&E-FY20-0176). We thank the OIG for recognizing ORD's commitment to following Agency best practices by considering a recommendation resolved in the draft report. ORD requests that some statements in the report are further clarified to avoid inadvertently misleading the reader. For example, revising the report title and differentiating between the evaluation's participating offices would enhance the audit's purpose to improve EPA's business practices and accountability. Further, ORD requests additional details concerning the survey, scope and methodology that OIG used to develop the overarching conclusions. The attachment provides additional detailed comments, including specific language suggestions and recommendations to improve accuracy. Immediately below is ORD's response to the OIG's recommendation.

Recommendation 6: Develop and implement a process to list and describe all minor applications in the appropriate system security plan.

Response 6: ORD concurs with this recommendation and proposes the following corrective action and completion date.

Corrective Action 6: The hosting location field in ORD's Application Inventory will be made required/mandatory. In addition, ORD will investigate and adjust current ORD processes (i.e. system's categorization form) to ensure the applicable ORD maintained System Security Plan is updated with newly added dependent National Institute of Standards and Technology Minor applications.

Planned Completion Date: May 31, 2022

Distribution

The Administrator
Deputy Administrator
Chief of Staff, Office of the Administrator
Deputy Chief of Staff, Office of the Administrator
Agency Follow-Up Official (the CFO)
Assistant Administrator for Mission Support
Assistant Administrator for Land and Emergency Management
Assistant Administrator and EPA Science Advisor, Office of Research and Development
Principal Deputy Assistant Administrator for Mission Support
Principal Deputy Assistant Administrator for Land and Emergency Management
Principal Deputy Assistant Administrator for Science, Office of Research and Development
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Associate Deputy Assistant Administrator for Mission Support
Deputy Assistant Administrator for Administration and Resources Management, Office of Mission Support
Deputy Assistant Administrator for Environmental Information and Chief Information Officer, Office of Mission Support
Deputy Assistant Administrator for Land and Emergency Management
Deputy Assistant Administrator for Management, Office of Research and Development
Deputy Assistant Administrator for Science Policy, Office of Research and Development
Director, Office of Continuous Improvement, Office of the Chief Financial Officer
Director, Office of Resources and Business Operations, Office of Mission Support
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of Mission Support
Audit Follow-Up Coordinator, Office of Land and Emergency Management
Audit Follow-Up Coordinator, Office of Research and Development