

**FEMA Should Improve
Controls to Restrict
Unauthorized Access to Its
Systems and Information**





OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

February 15, 2023

MEMORANDUM FOR: The Honorable Deanne Criswell
Administrator
Federal Emergency Management Agency

Randolph D. Alles
Senior Official Performing the Duties of the
Under Secretary for Management

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V. CUFFARI
Date: 2023.02.14
18:38:02 -07'00'

SUBJECT: *FEMA Should Improve Controls to Restrict
Unauthorized Access to Its Systems and
Information*

Attached for your action is our final report, *FEMA Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information*. We incorporated the formal comments provided by your office.

The report contains 10 recommendations aimed at improving the Federal Emergency Management Agency's (FEMA) access controls. Based on information provided in your response to the draft report, we consider recommendations 1 through 9 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov. Recommendation 10 is resolved and closed.

Consistent with our responsibility under the *Inspector General Act of 1978, as amended*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.
Attachment

www.oig.dhs.gov



DHS OIG HIGHLIGHTS

FEMA Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information

February 15, 2023

Why We Did This Audit

FEMA uses IT access controls to help ensure only authorized users have access to its systems and information. When properly implemented, access controls help to prevent individuals from gaining inappropriate access to systems or data. Our audit objective was to determine the extent to which FEMA applied IT access controls to restrict unnecessary access to systems and information.

What We Recommend

We made 10 recommendations to improve FEMA's IT access controls and system security.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

The Federal Emergency Management Agency (FEMA) did not consistently apply the information technology (IT) access controls needed to restrict unnecessary access to its systems and information. Specifically, FEMA did not promptly remove or adjust system and information access when personnel separated or changed positions. For example, 75 percent of the accounts for separated personnel we examined remained active beyond the individual's last workday. Additionally, FEMA did not monitor and configure privileged user access, service accounts, and access to sensitive security functions as required. These deficiencies stemmed from insufficient internal controls and day-to-day oversight to ensure access controls were administered appropriately and effectively to prevent unauthorized access.

Based on our testing, FEMA did not implement all the required security settings and address vulnerabilities timely for its IT systems and workstations. This occurred because FEMA was concerned updates might negatively impact system operations and because it faced operational challenges.

The deficiencies identified during this audit exposed FEMA's network and IT systems to risks of compromise by potential attackers. Additionally, these deficiencies could have limited the Department's overall ability to reduce the risk of unauthorized access to its network, which may disrupt mission operations.

FEMA Response

The Department of Homeland Security and FEMA concurred with all 10 recommendations. We have included a copy of their comments in Appendix B.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Background 1

Results of Audit 3

 FEMA Did Not Effectively Manage Access to Systems and Information ... 4

 FEMA Did Not Implement Required Settings and Address Vulnerabilities
 Timely for IT Infrastructure and Workstations..... 9

Conclusion..... 12

Recommendations..... 12

Appendixes

Appendix A: Objective, Scope, and Methodology 18

Appendix B: DHS Comments to the This Report..... 20

Appendix C: Major Contributors to This Report..... 26

Appendix D: Report Distribution 27

Abbreviations

ALM	Access Lifecycle Management
FEMA	Federal Emergency Management Agency
FECAPS	FEMA Enterprise Cloud Authentication Provisioning Services
FISMA	Federal Information Security Modernization Act
IT	information technology
OCISO	Office of the Chief Information Security Officer
OCSO	Office of the Chief Security Officer
STIG	Security Technical Implementation Guides



OFFICE OF INSPECTOR GENERAL



Department of Homeland Security

Background

The Department of Homeland Security’s critical mission of protecting the country makes its systems and networks high visibility targets for attackers who aim to disrupt essential operations or gain access to sensitive information. For example, Federal officials’ email accounts were compromised during the 2020 SolarWinds incident. During this cyberattack, external attackers breached cyber defenses to gain access to Federal Government networks. Once inside the networks, the attackers successfully set up permissions for themselves to access other programs and applications while being undetected. Attacks can also come from within an organization — insider threats (i.e., employees or contractors who use their authorized access to do harm) pose additional cybersecurity risks.

One effective way to reduce an organization’s overall risk and mitigate the negative impacts of cyberattacks is to enforce well-designed access controls. Access controls ensure that only authorized users have mission-related access to an organization’s networks, systems, and information. All executive branch agencies must implement access controls as part of their security framework to protect their operations and assets from being compromised by bad actors and other unauthorized users. Table 1 lists established access control best practices for DHS personnel based on Federal and Federal Emergency Management Agency (FEMA) criteria.¹



Table 1. Overview of Access Control Phases

Access Control	Control Description
 Initial Approval of Access	Individuals should formally submit requests for network and system access and obtain explicit approval.
 Ongoing Monitoring and Review of Access	Individuals’ access needs are expected to change over time. Access should be reviewed at least annually, or immediately if an individual’s need to know changes (e.g., if they change job functions).

¹ FEMA *Accounts Management Standard Operating Procedure*, Version 4.1, April 3, 2020, and NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Access Control	Control Description
 <p data-bbox="381 384 630 415">Access Removal</p>	<p data-bbox="704 310 1406 604">Individuals who no longer work for an organization should have their access privileges removed immediately. Access privileges should also be immediately terminated if an employee’s job functions have changed such that they no longer require access to the level at which privileges were previously granted.</p>
 <p data-bbox="381 684 605 758">Least Privilege Access</p>	<p data-bbox="704 615 1406 795">Each user in a system should be granted the most restrictive set of privileges (or lowest access) needed to perform authorized tasks. This limits the damage that can result from an accident, error, or unauthorized use.</p>

Source: DHS criteria²

In addition to using access controls, organizations can improve their ability to withstand cyberattacks by promptly addressing vulnerabilities, using appropriate security settings, and keeping management informed about any security challenges. These efforts increase security awareness and minimize risks to systems by identifying, managing, and tracking security risks and threats until they are addressed.

Within DHS, FEMA relies heavily on access controls and vulnerability management to ensure information technology (IT) resources and sensitive information are protected, available, and capable of meeting mission requirements. This sensitive information includes personally identifiable information and financial data that FEMA collects from the public to provide disaster support. Considering FEMA has more than 20,000 personnel nationwide and uses more than 100 IT systems, it is vital that the agency have well-developed processes for controlling access to its systems and information.

FEMA’s Administration of IT Access Controls

FEMA’s Office of the Chief Information Security Officer (OCISO) (within the Office of the Chief Information Officer) oversees and manages the cybersecurity program and protects FEMA networks, systems, and assets. In doing so, FEMA OCISO incorporates access control practices to support and secure



² DHS 4300A *Sensitive Systems Handbook*, Version 12.0, November 15, 2015. On September 20, 2022, DHS rescinded the handbook and replaced it with a new policy directive, DHS 4300A *Information Technology Systems Security Program, Sensitive Systems*, Version 13.2.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

FEMA data and IT systems. FEMA OCISO has established two primary types of IT user accounts for managing access controls: (1) general user and (2) privileged user.

Table 2. Overview of FEMA User Account Types

FEMA Account Type	Description
 General User Account	Used for routine job functions that are not security related.
 Privileged User Account	Authorized to perform security-related functions that ordinary users cannot perform, such as administering system and application changes.

Source: FEMA criteria

FEMA’s general support systems for providing capabilities to accomplish mission critical tasks and meet IT infrastructure requirements include the following:

- FEMA Enterprise Network represents FEMA’s IT infrastructure, including servers, routers, switches, and firewalls.
- FEMA Workstations System consists of approximately 34,000 workstations (laptops, desktops) inside the FEMA Enterprise Network and is used by FEMA personnel to meet daily IT requirements.

We conducted this audit to determine the extent to which FEMA applied IT access controls to restrict unnecessary access to its systems and information.

Results of Audit

FEMA did not consistently apply the IT access controls needed to restrict unnecessary access to its systems and information. Specifically, FEMA did not promptly remove or adjust system and information access when personnel separated or changed positions. For example, 75 percent of the accounts for separated personnel we examined remained active beyond the individual’s last workday. Additionally, FEMA did not monitor and configure privileged user access, service accounts, and access to sensitive security functions as



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

required. These deficiencies stemmed from insufficient internal controls and day-to-day oversight to ensure access controls were administered appropriately and effectively to prevent unauthorized access.

Based on our testing, FEMA did not implement all the required security settings and address vulnerabilities timely for its IT systems and workstations. This occurred because FEMA was concerned that updates might negatively impact system operations and because it faced operational challenges.

The deficiencies identified during this audit exposed FEMA's network and IT systems to risks of compromise by potential attackers. Additionally, these deficiencies could have limited the Department's overall ability to reduce the risk of unauthorized access to its network, which may disrupt mission operations.

FEMA Did Not Effectively Manage Access to Systems and Information

Although FEMA has implemented access control requirements for its systems, it did not consistently manage or remove access for personnel who separated or changed positions. Additionally, FEMA did not meet requirements for monitoring and assigning privileged user access and for monitoring and configuring service accounts. We attribute these deficiencies to insufficient internal controls and day-to-day oversight to ensure access controls were administered appropriately and effectively to prevent unauthorized access.

FEMA Did Not Appropriately Remove or Verify Access for Separated and Transferred Personnel

Removing access for separated and transferred³ personnel is an effective method for preventing individuals who no longer have a mission need from accessing system resources. At the time of our audit, *DHS 4300A Sensitive Systems Handbook*⁴ required that separated and transferred personnel who no longer required access have their IT access terminated immediately. Consistent with DHS' requirement, FEMA's Standard Operating Procedure⁵ requires that the unneeded access be removed on the separating or

³ FEMA uses "internal movement of personnel" to describe personnel that transfer offices within the component.

⁴ *DHS 4300A Sensitive Systems Handbook*, Version 12.0, November 15, 2015, provided the requirements we used for our audit. DHS rescinded the handbook in September 2022 and published a new policy directive, *DHS 4300A Information Technology Systems Security Program, Sensitive Systems*, Version 13.2. on September 20, 2022.

⁵ *FEMA Accounts Management Standard Operating Procedure*, Version 4.1, April 3, 2020.



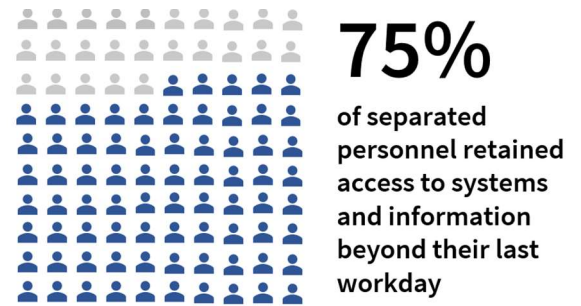
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

transferring individual’s last workday. However, FEMA did not consistently manage or remove access for personnel who separated or changed positions.

Even though access for separated personnel must be disabled immediately, we determined that 263 of 352⁶ (75 percent) separated personnel in our sample population had access to FEMA’s systems and information beyond their last workday, as shown in Figure 1. Of the 263 accounts that were not promptly deactivated, 36 (14 percent) maintained access to FEMA’s network for 30 days or longer.

Figure 1. Separated Personnel Who Retained System Access



Source: DHS OIG

The accounts for separated personnel remained active because FEMA supervisors and contracting officer’s representatives did not correctly follow procedures for disabling the accounts. In 2019, FEMA implemented a process in which supervisors and contracting officer’s representatives must use the Access Lifecycle Management (ALM) system to schedule access removals for separating individuals’ last workday. However, FEMA supervisors and contracting officer’s representatives did not consistently use ALM to schedule timely removals as required. Instead, they often relied on automated backup controls that eventually disable an individual’s account when other personnel actions occur, such as when an employee’s pay status changes in the National Finance Center database or if an individual’s personal identity verification card becomes inactive. FEMA used these backup controls to deactivate most accounts that were not scheduled for disablement through the ALM process. Specifically, 214 of the 263 accounts that were not promptly deactivated were disabled by the backup controls. As a result, 81 percent of those who maintained access beyond their last workday did not have their account disablement scheduled in ALM as required by FEMA.



214 of the 263 accounts that were not promptly deactivated were disabled using backup controls.

⁶ We tested a statistical sample of the 4,205 individuals who separated from FEMA from October 1, 2020, through March 30, 2022.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We identified similar findings in two prior audits of the Department's controls for restricting access to systems and information. Specifically, we reported the U.S. Citizenship Immigration Services did not consistently apply the IT access controls needed to restrict unnecessary access to its systems, information, and network.⁷ Additionally, we reported that DHS did not consistently revoke personal identity verification cards and withdraw security clearances for individuals that no longer worked for the Department, increasing the risk of unauthorized access to systems and facilities.⁸

FEMA also did not have a process to ensure unneeded access privileges were removed when individuals transferred offices within the component. We identified 2,797 individuals who transferred offices within FEMA from October 2020 through January 2022; FEMA could not demonstrate that it had removed access privileges no longer needed for these individuals' new positions. This occurred because FEMA did not have a centralized mechanism to identify and enforce access changes that may be needed when an individual transfers. Instead, each system's application gatekeeper⁹ was expected to proactively identify transferred personnel whose access needed to be reviewed. Moreover, FEMA's policies and procedures did not address DHS' requirements for prompt access removal or define what should qualify as a personnel transfer, causing uncertainty regarding whose access should be reviewed.

FEMA Did Not Adequately Assign and Monitor Privileged User Access

FEMA's privileged users who are trusted to perform critical IT security functions may be granted powerful (i.e., high-level) access to sensitive assets. Attackers often covet privileged accounts because of the broad access typically granted to these accounts. Accordingly, DHS IT security policy¹⁰ requires that privileged access be restricted only to users who have a mission need. Because access needs may change over time, FEMA's Standard Operating Procedure¹¹ requires system owners to monitor privileged user account access semiannually to ensure the access remains appropriate and to disable privileged accounts that are not used at least once every 45 days.

⁷ *USCIS Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information*, OIG-22-65, September 7, 2022.

⁸ *DHS Did Not Always Promptly Revoke PIV Card Access and Withdraw Security Clearances for Separated Individuals*, OIG-23-04, December 20, 2022.

⁹ Application gatekeepers are personnel who help system owners manage access controls.

¹⁰ *DHS Sensitive Systems Policy Directive 4300A*, Version 13.1, July 27, 2017, provided the requirements we used for our audit. DHS published a new policy directive, *DHS 4300A Information Technology Systems Security Program, Sensitive Systems*, Version 13.2. on September 20, 2022.

¹¹ *FEMA Accounts Management Standard Operating Procedure*, April 3, 2020.



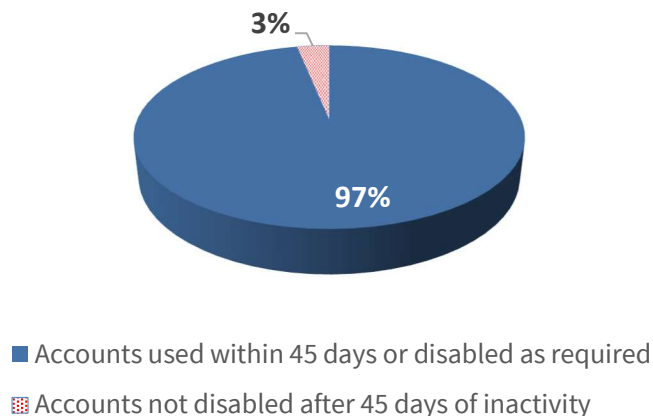
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

FEMA did not monitor privileged user access as required. We found FEMA did not perform semiannual reviews of its 973 privileged accounts because it did not have a formal, component-wide review process. FEMA relied on system owners to develop and perform their own review processes. However, some system owners did not have a review process or assumed that FEMA's Office of the Chief Information Officer was reviewing the accounts for them.

Similarly, FEMA did not consistently disable privileged accounts that had not been used at least once every 45 days. We identified 31 of 973 privileged accounts that remained active without being used in 45 days, including 8 accounts that remained active even though they had not been used in more than 70 days (see Figure 2). This occurred because FEMA did not correctly configure system settings to enforce the requirement.

Figure 2. FEMA Privileged Account Status



Source: DHS OIG, based on Active Directory scans and FEMA documentation

Additionally, FEMA did not limit privileged access to only those users who had a mission need. Specifically, FEMA inappropriately granted 259 users permission to change the password of a powerful and sensitive security account used for access management across the component; these users had no mission need for this access. FEMA officials explained that the 259 users received this access by mistake, as these users inherited the permission to reset the password to the security account indirectly through another permission that was approved for their accounts.



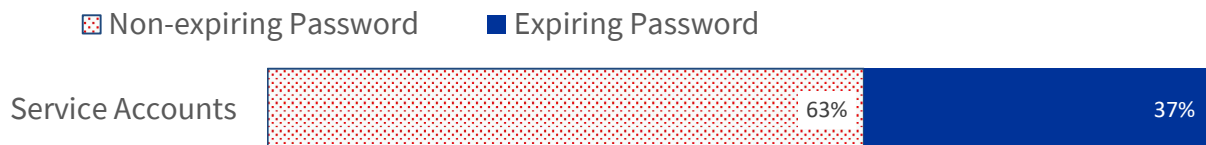
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

FEMA Did Not Adequately Manage and Monitor Service Account Access

FEMA uses service accounts to help execute automated tasks, such as running system commands or exchanging data with other systems. Service accounts pose unique security risks because they are non-human accounts and may have highly privileged access. FEMA did not monitor service accounts as required. For example:

- DHS Change Memorandum 13.1.1 to *DHS Sensitive Systems Policy Directive 4300A*¹² requires that service account passwords be changed annually to reduce the risk of unauthorized access. However, 1,454 of 2,302 (63 percent) FEMA service accounts were configured to have non-expiring passwords (see Figure 3). FEMA did not change passwords as required because it did not have access to automated tools that would have managed password updates. Instead, according to FEMA, it used a manual email process to notify system owners when passwords expired and chose not to enforce service account password expiration requirements. Although FEMA had planned to obtain automated tools to address service account issues, FEMA officials said they could not do so due to budget constraints.

Figure 3. Service Account Password Expiration Settings



Source: DHS OIG, based on Active Directory scans and FEMA documentation

- FEMA’s IT security policies and procedures do not address interactive logon.¹³ We found that FEMA did not appropriately restrict access to 2,302 service accounts. This occurred because FEMA believed its operations could be adversely affected if it implemented the settings needed to restrict access.

¹² Change Memorandum 13.1.1. to *DHS Sensitive Systems Policy Directive 4300A*, October 2, 2019, provided the requirements used for our audit. DHS published a new policy directive, *DHS 4300A Information Technology Systems Security Program, Sensitive Systems*, Version 13.2. on September 20, 2022.

¹³ Interactive logon is when a user accesses a computer through an account.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- DHS IT Security Policy requires that all service accounts be appropriately encrypted. However, we identified 48 service accounts that did not meet encryption requirements. FEMA did not appropriately encrypt the service accounts because it believed the required level of encryption could negatively affect operations for its legacy IT assets.
- FEMA's Standard Operating Procedure requires that service accounts be reviewed semiannually to confirm their access is appropriate. However, FEMA did not conduct semiannual reviews for any of its 2,302 service accounts. FEMA officials explained that this occurred because of resource constraints and because FEMA does not have a comprehensive list of service accounts for each IT system. Instead, FEMA relied on system owners to develop their own processes to review service accounts and did not provide oversight to ensure the task was completed.

FEMA Did Not Implement Required Settings and Address Vulnerabilities Timely for IT Infrastructure and Workstations

DHS relies on security setting updates, vulnerability management programs, and regular security reporting to identify and manage threats to its systems and network. These processes help reduce the impact if attackers exploit access control weaknesses.

Although FEMA's IT systems and workstations generally complied with DHS' security standards, FEMA did not implement all required security settings and updates. Additionally, we identified potential risks in FEMA's process for reporting the status of its security settings to the Federal Information Security Modernization Act (FISMA) Scorecard¹⁴ that required further analysis by FEMA and DHS OCISO to ensure compliance with requirements.

FEMA Did Not Comply with DHS' Required Security Settings

According to DHS IT Security Policy, components must use system security settings that are consistent with technical frameworks, including the Defense Information System Agency's *Security Technical Implementation Guides*

¹⁴ *The Federal Information Security Modernization Act of 2014*, Public Law 113-283, December 18, 2014, requires Chief Information Officers to report the effectiveness of the agency information security program to the agency head. Additionally, *DHS Information Security Performance Plan*, Version 5.0, January 18, 2022, requires the DHS FISMA Scorecard to be published monthly to communicate the Department's security posture to senior management.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

(STIG).¹⁵ DHS has a process in place¹⁶ for components to obtain waivers or risk acceptance approval from the DHS OCISO to not implement STIG settings. We tested two FEMA systems and determined that their security settings were not fully compliant with DHS-required security settings for its systems. The IT systems and workstations we tested were between 58 percent and 92 percent compliant with STIG requirements.

According to FEMA, it chose not to implement these required settings due to concerns that the settings may interrupt the work of FEMA employees supporting disaster locations. In support of these concerns, in year 2020, FEMA developed a component-specific process through its *Enterprise Compliance Baselines Standard Operating Procedure* to determine whether specific STIG settings could be implemented. FEMA officials explained that they opted to follow this component-level process, rather than seek DHS-level approval to implement their own selection of STIG settings. We checked with the DHS OCISO to verify that FEMA's *Enterprise Compliance Baselines Standard Operating Procedure* complied with DHS requirements, but we were not able to validate this during the audit. The OCISO official explained that historically, other DHS components have submitted STIG waiver and risk acceptance requests for DHS OCISO approval. FEMA's Office of the Chief Information Officer acknowledged that it may be beneficial for FEMA to obtain the DHS Chief Information Officer's approval of its compliance baseline procedure.

FEMA Did Not Promptly Update its IT Infrastructure and Workstations to Address Known Vulnerabilities

FEMA must timely address vulnerabilities in its systems, according to timeframes published in the DHS Enterprise Security Operations Center's Information Security Vulnerability Management notices.¹⁷ However, we determined that FEMA did not remediate all critical and high-risk vulnerabilities for IT infrastructure and workstations within DHS' required timelines. For example, we identified one FEMA system with five unique critical vulnerabilities (with 124 occurrences) and 20 unique high-risk vulnerabilities (with 552 occurrences) for which remediation was overdue by as

¹⁵ *DHS Sensitive Systems Policy Directive 4300A*, Version 13.1, July 27, 2017, provided the initial requirements used for our audit. We also evaluated the requirements provided in the new policy directive DHS published, *DHS 4300A Information Technology Systems Security Program, Sensitive Systems*, Version 13.2. on September 20, 2022.

¹⁶ Components may submit a written request to the DHS Chief Information Security Officer to forgo the implementation of STIG settings.

¹⁷ The Information Security Vulnerability Management notices alert components of current vulnerabilities, risks and threats to DHS information systems that need attention.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

long as two years. For the two systems we analyzed, the longest outstanding vulnerability should have been remediated by September 24, 2019, but it still had not been addressed at the time we performed system scans in April 2022. Without implementing corrective patches to fix vulnerabilities identified at the time of our testing, FEMA risked access control weakness exploitation, as well as the confidentiality, integrity, and availability of sensitive systems and information. FEMA said it had not yet addressed known vulnerabilities because it faced resource limitations, challenges with its large number of IT assets, and constantly changing cybersecurity priorities.

FEMA's Process for Submitting Data to the DHS FISMA Scorecard Should be Reviewed Further by DHS OCISO

DHS OCISO uses its monthly FISMA Scorecard and metrics to manage information system security risk. To develop its scorecard, DHS collects information from its components to provide senior management a monthly snapshot of each component's information security standing and the Department's overall security posture. Although FEMA reports its compliance with STIG settings to DHS for the FISMA Scorecard, we identified potential risks with its process for representing failed settings.¹⁸ Specifically, during our audit testing of FEMA's configuration management compliance, FEMA explained that it recategorizes failed settings to informational¹⁹ in its FISMA Scorecard data if it believes the settings cannot be implemented. Further, FEMA explained that its recategorization process could be incorrectly increasing its Configuration Management Metric in the FISMA Scorecard. For example, FEMA's Configuration Management Metric in the August 2022 FISMA Scorecard increased 1 percent due to the recategorization of failed security settings.

In September 2022, we met with DHS OCISO and obtained scorecard documentation to verify if FEMA's process complied with FISMA Scorecard requirements. DHS OCISO explained that it had initiated an evaluation to assess FEMA's compliance with the FISMA Scorecard and that it believed FEMA's data was accurate. After our fieldwork was completed, DHS OCISO officials reported their evaluation was finalized and FEMA's monthly FISMA scorecard data submissions complied with requirements. Further, DHS OCISO reported that after the Office of Inspector General completed its initial testing, FEMA upgraded its software scanning tools to help further refine its processes for FISMA Scorecard reporting.

¹⁸ Failed settings are not properly implemented or not implemented at all.

¹⁹ Informational settings provide details on setting status but are not counted as failed settings.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Conclusion

FEMA's access control deficiencies increase the risk that unauthorized individuals could gain access to sensitive information, including the personally identifiable information and financial data that FEMA collects to provide disaster support. Additionally, FEMA's security settings on systems and workstations may limit its ability to overcome a major cybersecurity incident or to mitigate an access control weakness if an unauthorized individual gains access. DHS' overall security posture relies on all components to implement effective IT security processes. Therefore, FEMA's access control and system security deficiencies may limit the Department's ability to reduce the risk of unauthorized access to its network and disruption of mission operations.

Recommendations

Recommendation 1: We recommend the FEMA Chief Security Officer provide training to supervisors, contracting officer's representatives, contracting officers, human resource liaisons, and timekeepers on FEMA's offboarding processes for removing IT access.

Recommendation 2: We recommend the FEMA Chief Security Officer develop and implement internal controls to monitor and enforce supervisors and contracting officer's representatives' compliance with the Access Lifecycle Management system's offboarding process for removing IT access.

Recommendation 3: We recommend the FEMA Chief Security Officer implement a process to identify and verify that transferred personnel's unneeded access is removed in accordance with FEMA requirements.

Recommendation 4: We recommend the FEMA Office of the Chief Information Officer implement a standardized process to conduct and monitor privileged and service account reviews in accordance with FEMA requirements.

Recommendation 5: We recommend the FEMA Office of the Chief Information Officer remove the unnecessary privileges that allowed additional users to access the sensitive security account we identified.

Recommendation 6: We recommend the FEMA Office of the Chief Information Officer implement automated tools or additional controls and policies to change service account passwords as required and prevent interactive logon.

Recommendation 7: We recommend the FEMA Office of the Chief Information Officer establish a risk-based approach to implement DHS' required encryption



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

standards where possible or submit requests for waivers or risk acceptance to the DHS Chief Information Security Officer to forgo this setting on affected FEMA service accounts.

Recommendation 8: We recommend the FEMA Office of the Chief Information Officer submit its FEMA *Enterprise Compliance Baselines Standard Operating Procedure* to the DHS Chief Information Security Officer to verify FEMA's compliance with DHS' waiver and risk acceptance requirements for *Security Technical Implementation Guides* settings that are not implemented.

Recommendation 9: We recommend the FEMA Office of the Chief Information Officer perform an evaluation to identify additional automated tools to help address known vulnerabilities within required timeframes and implement where possible or formally accept the risk in accordance with DHS requirements.

Recommendation 10: We recommend the DHS Chief Information Security Officer finalize its evaluation of FEMA's compliance with DHS' FISMA Scorecard requirements and ensure any necessary remedial action.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from FEMA and the DHS Office of the Chief Information Officer through the Director of the Departmental GAO-OIG Liaison Office. In the comments, the Department indicated it appreciated our work on this audit. The Department stated that it remains committed to continuous improvement and implementation of access management strategies across the Department.

We reviewed FEMA and DHS Office of the Chief Information Officer comments, as well as the technical comments previously submitted under separate cover, and updated the report as appropriate. Recommendations 1 through 9 are resolved and open. Recommendation 10 is resolved and closed. A summary of FEMA and DHS responses and our analysis follows.

DHS Response to Recommendation #1: Concur. FEMA Office of the Chief Security Officer (OCSO) will provide digital training resources on collaboration and shared spaces for responsible official access. FEMA OCSO will also provide regularly available customized training and demonstration sessions to all FEMA-designated responsible officials, including practical application learning modules to support knowledge retention and execution of policy-based access management tasks. Further, FEMA OCSO commits to re-engaging the



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

workforce with updated and policy-based training to ensure up-to-date knowledge and application in the execution of access management-related tasks by the end of fiscal year 2023.

OIG Analysis: FEMA's actions are responsive to this recommendation, which will remain open and resolved until it provides documentation showing it has developed and provided training to supervisors, contracting officer's representatives, contracting officers, human resource liaisons, and timekeepers on FEMA's offboarding processes for removing IT access. FEMA estimates a completion date of September 30, 2023.

DHS Response to Recommendation #2: Concur. FEMA OCSO, with the support of other FEMA Mission Support program offices, will create a policy document to prioritize coordination with interdepartmental organizations to codify component-level policies and procedures to comply with overarching governance regarding the removal of unnecessary IT access to the FEMA Enterprise Network. Once complete, this policy document will outline how FEMA responsible officials will implement and monitor compliance with mandated offboarding and access control processes in the removal of IT access.

OIG Analysis: FEMA's actions are responsive to this recommendation, which will remain open and resolved until it provides the updated policies and associated implementation plan to monitor compliance with mandated IT offboarding procedures. FEMA estimates a completion date of March 29, 2024.

DHS Response to Recommendation #3: Concur. FEMA OCSO, with the support of other FEMA Mission Support program offices, will create a policy document to prioritize coordination with interdepartmental organizations to codify component-level policies with definable criteria to dictate access management necessities to comply with overarching governance regarding the removal of unnecessary IT access to the FEMA Enterprise Network. FEMA OCSO will also coordinate the development of policies to outline how responsible officials will identify and verify internal movement of personnel, ensuring unneeded access is removed in accordance with DHS and Homeland Security Presidential Directive 12 requirements.

OIG Analysis: FEMA's actions are responsive to this recommendation, which will remain open and resolved until it provides updated policies and associated implementation plan to identify and verify internal movements of personnel, ensuring the removal of unnecessary IT access to FEMA resources and assets. FEMA estimates a completion date of March 29, 2024.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

DHS Response to Recommendation #4: Concur. In FY 2020, FEMA OCISO Identity, Credential, and Access Management Division chartered a study to assess FEMA's readiness to move to the cloud and explore options for modernized identity and access management. In October 2022, FEMA OCISO established the FEMA Enterprise Cloud Authentication Provisioning Services (FECAPS) program. FECAPS will modernize identity and access management with a Software as a Service solution to mature the Identity Access Zero Trust Architecture pillar.

OIG Analysis: FEMA's actions are responsive to this recommendation, which will remain open and resolved until it implements access management monitoring for service and privileged accounts through policy development and migration to Software as a Service solution. FEMA estimates a completion date of April 30, 2025.

DHS Response to Recommendation #5: Concur. FEMA's OCISO Identity, Credential, and Access Management Division will include privilege account management in the FECAPS Software as a Service solution to ensure only necessary privileges are allowed.

OIG Analysis: FEMA's actions are responsive to this recommendation, which will remain open and resolved until it provides documentation to demonstrate the FECAPS privileged account management process is implemented to ensure only necessary privileges are allowed. FEMA estimates a completion date of April 30, 2025.

DHS Response to Recommendation #6: Concur: FEMA's OCISO Identity, Credential, and Access Management Division will incorporate account management, including password management, in the FECAPS Software as a Service solution.

OIG Analysis: FEMA's actions are responsive to this recommendation, which will remain open and resolved until it implements the FECAPS Software as a Service solution to manage service accounts passwords and prevent interactive logon. FEMA estimates a completion date of April 30, 2025.

DHS Response to Recommendation #7: Concur. FEMA OCISO Risk Management Division Director will evaluate the status of FEMA service accounts against current standards and system requirements. Once this evaluation is complete, waivers or risk acceptance requests will be submitted, when necessary, to the appropriate authority for approval.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG Analysis: FEMA's actions are responsive to this recommendation, which will remain open and resolved until it implements appropriate encryption standards for service accounts, or documentation showing that requirements were waived by the appropriate authority. FEMA estimates a completion date of January 31, 2024.

DHS Response to Recommendation #8: Concur. FEMA OCISO Risk Management Division staff are reviewing the FEMA *Enterprise Compliance Baselines Standard Operating Procedure*, Version 1.2 for compliance with the revised DHS 4300A, *Information Technology Systems Security Program, Sensitive Systems*, Version 13.2 (dated September 20, 2022). Once the review is complete, the Risk Management Division will submit the procedure to the DHS Chief Information Security Officer for verification of compliance with DHS' waiver and risk acceptance requirements.

OIG Analysis: FEMA's actions are responsive to this recommendation, which will remain open and resolved until it provides documentation showing DHS Chief Information Security Officer's review and approval of FEMA's *Enterprise Compliance Baseline Standard Operating Procedure*, Version 1.2 to demonstrate the procedure's compliance with DHS' waiver and risk acceptance requirements. FEMA estimates a completion date of August 31, 2023.

DHS Response to Recommendation #9: Concur. FEMA OCISO will conduct an evaluation of existing and available automated tools to address known vulnerabilities on FEMA workstations. Once complete, this evaluation will inform OCISO's risk assessment for vulnerability management of workstations.

OIG Analysis: FEMA's actions are responsive to this recommendation, which will remain open and resolved until it completes its evaluation of existing tools to address known vulnerabilities and incorporates findings into OCISO's risk assessment for vulnerability management of workstations. FEMA estimates a completion date of January 31, 2024.

DHS Response to Recommendation #10: Concur. In November 2022, DHS OCISO coordinated with FEMA OCISO to identify and, if necessary, resolve any discrepancies in FEMA's data submissions for the DHS Monthly Scorecard. Following this outreach, FEMA officials clarified to DHS OCISO that FEMA's internal custom reports were not part of what was sent to DHS as part of the FISMA scorecard submissions. Furthermore, since September 2022, FEMA has upgraded its software scanning tools, and discontinued the use of internal custom reports. DHS OCISO previously provided OIG documentation showing these efforts on January 12, 2023. We request that OIG consider this recommendation resolved and closed, as implemented.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG Analysis: DHS provided documentation showing its corrective actions in response to recommendation 10. Specifically, DHS OCISO officials reported FEMA’s monthly FISMA scorecard data submissions complied with requirements. Further, DHS OCISO reported that FEMA upgraded its software scanning tools to help further refine its processes for FISMA scorecard reporting. These materials were responsive to the intent of the recommendation. Recommendation 10 is resolved and closed.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine the extent to which FEMA applied IT access controls to restrict unnecessary access to systems and information. We evaluated FEMA's account management processes for authorizing, validating, and disabling users' access. We performed technical assessments of FEMA's domain and selected systems to identify weaknesses and security risks. Additionally, we assessed internal controls and compliance in accordance with laws and regulations necessary to satisfy the audit. In particular, we assessed information system control effectiveness. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

To conduct this audit, we gathered system documentation related to access control implementation and evidence of access control-related actions for user account creation, removal, and validation. We researched and used Federal and departmental criteria for access control requirements. We also obtained data from the FEMA Office of the Chief Component Human Capital Officer to identify personnel who separated or transferred offices from October 2020 through March 2022. From this data, we identified a population of 4,205 separated individuals and selected a statistical sample of 352 for our testing. Additionally, we identified a population of 2,797 individuals who transferred offices within FEMA during the same timeframe. We also observed IT systems to understand FEMA's processes for creating, disabling, and removing accounts. We interviewed system owners; information system security officers; and personnel from FEMA's OCISO, Identity, Credential and Access Management Division, Enterprise Identity Management System, and Office of the Chief Component Human Capital Officer.

Additionally, we relied on the work of internal specialists from DHS OIG's Office of Innovation, Cybersecurity Risk Assessment Division to perform technical assessments of FEMA's systems and domain. Specifically, they assessed how FEMA manages vulnerabilities and security settings on domain controllers, servers, and workstations within the FEMA Enterprise Network and FEMA Workstation System authorization boundaries. The internal specialists also completed an Active Directory assessment scan of the FEMA Enterprise Network. We used the information obtained from these assessments to identify



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

system vulnerabilities such as missing security updates, misconfigured security settings, the presence of unsupported operating systems, and Active Directory weaknesses or misconfigurations. Our audit timeline did not allow for an assessment of whether FEMA users' access to specific resources was appropriate. Additionally, our audit scope focused on FEMA's compliance with system settings required by DHS and did not include an evaluation of FEMA's data provided to DHS OCISO for its FISMA Scorecard or FEMA's processes for submitting waivers for settings that were not implemented.

To ensure the accuracy of our testing results and reporting, we gave FEMA the opportunity to review our preliminary observations, verify the initial results, and identify any "false-positive" results. We reviewed FEMA's feedback and updated our analysis as needed. Additionally, when writing the report, we considered the potential for sensitivity issues under DHS Management Directive 11042.1, *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*, and generalized our findings as appropriate to avoid disclosing information designated as sensitive by the Department. DHS headquarters and FEMA officials also reviewed the report for sensitivity concerns.

We conducted this performance audit between January and December 2022 pursuant to the *Inspector General Act of 1978, as amended*, and according to Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
DHS Comments to the This Report

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

January 27, 2023

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Jim H. Crumacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

SUBJECT: Management Response to Draft Report: "FEMA Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information" (Project No. 22-016-AUD-FEMA)

**JIM H
CRUMPACKER**

Digitally signed by JIM H
CRUMPACKER
Date: 2023.01.27 16:22:17
-05'00'

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS leadership is pleased to note OIG's acknowledgement that the Federal Emergency Management Agency (FEMA) incorporates access control practices to support and secure FEMA data and Information Technology (IT) systems. DHS remains committed to maintaining the confidentiality, integrity, and availability of systems that serve the Department and the public. FEMA's mission to help people before, during, and after disasters relies on the strength of information systems' access controls, and FEMA is committed to continuous improvement and implementation of access management strategies across the Department such as the implementation of the Department-wide system for access lifecycle management.

The draft report contained ten recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, sensitivity, and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Enclosure



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

**Enclosure: Management Response to Recommendations
Contained in 22-016-AUD-FEMA**

OIG recommended that the FEMA Chief Security Officer:

Recommendation 1: Provide training to supervisors, contracting officer's representatives, contracting officers, human resource liaisons, and timekeepers on FEMA's offboarding processes for removing IT access.

Response: Concur. FEMA's Office of the Chief Security Officer (OCSO), Field Security Division (FSD) currently manages the interconnection of the DHS Access Lifecycle Management (ALM) system. ALM automates access controls by providing a tool that Component responsible officials—including supervisors, human resources liaisons, timekeepers, contracting officers, and contracting officers representatives and others—utilize for their access management duties. FEMA OCSO provides a suite of ALM-related training resources to FEMA responsible officials, as appropriate, and also liaises with DHS system administration and development teams as members in the ALM integrated project teams (IPTs), which are utilized to generate support or enhancements to ALM for DHS-wide Component stakeholders.

In addition to these ongoing efforts, FEMA OCSO will provide digital training resources on collaboration and shared spaces for responsible official access. FEMA OCSO will also provide regularly available customized training and demonstration sessions to all FEMA designated responsible officials, to include practical application learning modules to support knowledge retention and execution of policy-based access management tasks. FEMA OCSO also commits to re-engaging the workforce with updated and policy-based training to ensure up-to-date knowledge and application in the execution of access management-related tasks by the end of fiscal year (FY) 2023.

Estimated Completion Date (ECD): September 30, 2023.

Recommendation 2: Develop and implement internal controls to monitor and enforce supervisors and contracting officer's representatives' compliance with the Access Lifecycle Management system's offboarding process for removing IT access.

Response: Concur. FEMA OCSO FSD, with the support of other FEMA Mission Support program offices, will create a policy document to prioritize coordination with interdepartmental organizations to codify component-level policies and procedures to comply with overarching governance regarding the removal of unnecessary IT access to the FEMA Enterprise Network. Once complete, this policy document will outline how FEMA responsible officials will implement and monitor compliance with mandated



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

offboarding and access control processes in the removal of IT access. As part of this effort, FEMA OCSO will take the following actions:

Actions	ECD
FEMA OCSO will identify key points of contact and responsibility for membership on an IPT to develop the policy.	February 28, 2023
FEMA OCSO will formalize the IPT, which will codify processes to mitigate gaps and risks per audit findings and complete draft policy documents for agency review.	October 31, 2023
The IPT will submit the proposed policy for executive signature and then execute an implementation plan.	November 30, 2023
FEMA OCSO will begin closure processes and submit necessary artifacts to OIG to show policy socialization and effective new implementation of codified processes and procedures.	March 29, 2024

Overall ECD: March 29, 2024.

Recommendation 3: Implement a process to identify and verify that transferred personnel’s unneeded access is removed in accordance with FEMA requirements.

Response: Concur. FEMA OCSO FSD, with the support of other FEMA Mission Support program offices, will create a policy document to prioritize coordination with interdepartmental organizations to codify Component-level policies with definable criteria to dictate access management necessities to comply with overarching governance regarding the removal of unnecessary IT access to the FEMA Enterprise Network. FEMA OCSO will also coordinate the development of policies to outline how responsible officials will identify and verify internal movement of personnel, ensuring unneeded access is removed in accordance with DHS and Homeland Security Presidential Directive 12 requirements.¹ As part of these efforts, FEMA OCSO will take the following actions:

Actions	ECD
FEMA OCSO will identify key points of contact and responsibility for membership on an IPT for the purpose of governance development.	February 28, 2023
FEMA OCSO will formalize the IPT for the purposes of assessment and identification of governance requirement(s) relevant to Component-level access management.	March 31, 2023
The IPT will develop new and/or modernized processes and codify all to mitigate gaps and risks per audit findings and	June 30, 2023

¹ Homeland Security Presidential Directive 12: “Policy for a Common Identification Standard for Federal Employees and Contractors,” August 27, 2004. <https://www.dhs.gov/homeland-security-presidential-directive-12>



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

recommended actions, as well as the resultant implementation strategy.	
The IPT will complete the draft governance documents for agency review.	October 31, 2023
The IPT will submit the final iteration of governance for executive signature and then execute an implementation plan.	November 30, 2023
FEMA OCSO will begin closure processes and submit necessary artifacts to OIG to show governance socialization and effective new implementation of codified processes and procedures.	March 29, 2024

Overall ECD: March 29, 2024.

OIG recommended that the FEMA Office of the Chief Information Officer:

Recommendation 4: Implement a standardized process to conduct and monitor privileged and service account reviews in accordance with FEMA requirements.

Response: Concur. In FY 2020, FEMA’s Office of the Chief Information Security Officer (OCISO), Identity, Credential, and Access Management (ICAM) Division chartered a study to assess FEMA’s readiness to move to the cloud and explore options for modernized identity and access management. The study, which was finalized in March 2020, informed FEMA’s CISO’s response to Executive Order 14028, “Improving the Nation’s Cybersecurity,” (dated May 12, 2021),² and Office of Management and Budget Memorandum M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,” (dated January 26, 2022),³ which both require the Federal Government to secure cloud services, implement Zero Trust Architecture (ZTA), and deploy multifactor authentication and encryption. As a result, in October 2022, FEMA CISO established the FEMA Enterprise Cloud Authentication Provisioning Services (FECAPS) program. FECAPS will modernize identity and access management with a Software as a Service (SaaS) solution to mature the Identity/Access ZTA pillar.

In addition to these efforts, FEMA will take the following actions:

Actions	ECD
FEMA OCISO ICAM Division will complete a Proof-of-Concept assessment.	May 31, 2023
FEMA OCISO ICAM Division will complete a Proof-of-Concept for SaaS migration.	January 31, 2024

² <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

³ <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

FEMA OCISO ICAM Division will publish key policy documents and complete remaining systems migration to the SaaS solution.	April 30, 2025
---	----------------

Overall ECD: April 30, 2025.

Recommendation 5: Remove the unnecessary privileges that allowed additional users to access the sensitive security account we identified.

Response: Concur. FEMA’s OCISO ICAM Division will include privilege account management in the FECAPS SaaS solution to ensure only necessary privileges are allowed. ECD: April 30, 2025.

Recommendation 6: Implement automated tools or additional controls and policies to change service account passwords as required and prevent interactive logon.

Response: Concur: FEMA’s OCISO ICAM Division will incorporate account management, including password management, in the FECAPS SaaS solution. ECD: April 30, 2025.

Recommendation 7: Establish a risk-based approach to implement DHS’ required encryption standards where possible or submit requests for waivers or risk acceptance to the DHS Chief Information Security Officer to forgo this setting on affected FEMA service accounts.

Response: Concur. FEMA’s OCISO Risk Management Division (RMD) Director will evaluate the status of FEMA service accounts against current standards and system requirements. Once this evaluation is complete, waivers or risk acceptance requests will be submitted, when necessary, to the appropriate authority for approval. ECD: January 31, 2024.

Recommendation 8: Submit its FEMA Enterprise Compliance Baselines Standard Operating Procedure to the DHS Chief Information Security Officer to verify FEMA’s compliance with DHS’ waiver and risk acceptance requirements for Security Technical Implementation Guides settings that are not implemented.

Response: Concur. FEMA’s OCISO RMD staff are reviewing the FEMA Enterprise Compliance Baselines Standard Operating Procedure (SOP) Version 1.2 for compliance with the revised DHS 4300A, “Information Technology Systems Security Program, Sensitive Systems,” Version 13.2 (dated September 20, 2022). Once the review is complete, RMD will submit the SOP to the DHS CISO for verification of compliance with DHS’ waiver and risk acceptance requirements. ECD: August 31, 2023.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 9: Perform an evaluation to identify additional automated tools to help address known vulnerabilities within required timeframes and implement where possible or formally accept the risk in accordance with DHS requirements.

Response: Concur. FEMA's OCISO will conduct an evaluation of existing and available automated tools to address known vulnerabilities on FEMA workstations. Once complete, this evaluation will inform the OCISO's risk assessment for vulnerability management of workstations. ECD: January 31, 2024.

OIG recommended that the DHS CISO:

Recommendation 10: Finalize its evaluation of FEMA's compliance with DHS' FISMA Scorecard requirements and ensure any necessary remedial action.

Response: Concur. In November 2022, DHS OCISO coordinated with FEMA OCISO to identify and, if necessary, resolve any discrepancies in FEMA's data submissions for the DHS Monthly Scorecard. Following this outreach, FEMA officials clarified to DHS OCISO that FEMA's internal custom reports were not part of what was sent to DHS as part of the FISMA scorecard submissions. Furthermore, since September 2022, FEMA has upgraded its software scanning tools, and discontinued the use of internal custom reports. DHS OCISO previously provided OIG documentation of these efforts on January 12, 2023.

We request that OIG consider this recommendation resolved and closed, as implemented.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C
Office of Audits Major Contributors to This Report

Tarsha Cary, Director
Alexander Stewart, Audit Manager
Tessa Clement, Auditor-in-Charge
Alexandria Castaneda, Program Analyst
Kenneth Schoonover, Program Analyst
Stephanie Matthews, Auditor
Tanisha Bethea, Auditor
Donna Zavesky, Auditor
Saad Amjed, IT Specialist
Maria Romstedt, Communications Analyst
Enrique Leal, Independent Referencer

Office of Innovation, IT and Data Specialist Support

Thomas Rohrback, Director
Jason Dominguez, Supervisory IT Cybersecurity Specialist
Rashedul Romel, Supervisory IT Cybersecurity Specialist
Taurean McKenzie, IT Specialist
Joseph Sanchez, IT Specialist
Jon Wyatt, IT Specialist/System Administrator
Josh Wilshere, Supervisory Data Architect
Nandini Parvathareddygari, Senior Data Architect



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at:
www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General
Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.



OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" box. If you cannot access our website, call our hotline at (800) 323-8603, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305