OFFICE OF INSPECTOR GENERAL

FEMA Did Not Always Secure Information Stored on Mobile Devices to Prevent Unauthorized Access

Homeland Security

July 7, 2023
OIG-23-32

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security
Washington, DC 20528 / www.oig.dhs.gov

July 7, 2023

MEMORANDUM FOR: Charles R. Armstrong
Chief Information Officer
Federal Emergency Management Agency

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2023.07.06 17:08:12 -04'00'

SUBJECT: *FEMA Did Not Always Secure Information Stored on Mobile Devices to Prevent Unauthorized Access*

For your action is our final report, *FEMA Did Not Always Secure Information Stored on Mobile Devices to Prevent Unauthorized Access*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving FEMA's mobile device management. Your office concurred with all four recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 through 4 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.

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 Kristen Bernard, Acting Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG Highlights

FEMA Did Not Always Secure Information Stored on Mobile Devices to Prevent Unauthorized Access

July 7, 2023

Why We Did This Audit

Mobile devices, such as smartphones and tablets, are critical for FEMA's workforce to successfully complete its mission. While mobile devices increase workforce mobility and productivity, they also introduce risks including cyber threats or loss of sensitive Government data. We conducted this audit to determine whether FEMA secures its mobile devices to safeguard information accessed, stored, and processed on mobile devices.

What We Recommend

We made four recommendations to improve FEMA's mobile device 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 always secure information stored on mobile devices. Specifically, FEMA did not document whether it removed all data from mobile devices that were disposed of, lost or stolen, or taken on international travel. This occurred because FEMA did not ensure employees followed Department of Homeland Security policy and because FEMA did not have supplemental guidance with specific requirements for sanitizing lost or stolen mobile devices.

Additionally, FEMA did not always disable unauthorized mobile devices taken outside the United States or its territories, as required by DHS policy, which prohibits employees from taking their Government-issued mobile devices internationally for any personal or official foreign travel, unless specifically authorized by their supervisor. If an unauthorized device is detected internationally, it must be disabled. However, FEMA only disabled two of the nine unauthorized devices (22 percent) detected internationally in our sample. This occurred because FEMA did not update its policy to reflect DHS' foreign travel guidance requiring all devices detected internationally be disabled.

Lastly, FEMA's configuration management controls comply with the *Defense Information Systems Agency Security Technical Implementation Guides*. These controls provide reasonable assurance that the mobile device management system enforces security controls and that FEMA's mobile devices are configured and operating securely, as intended.

FEMA's Response

FEMA concurred with all four recommendations. Appendix A contains FEMA's management response in its entirety.

Background

The Federal Emergency Management Agency's (FEMA) mission is helping people before, during, and after disasters. FEMA uses mobile devices to perform daily work activities and access FEMA's network remotely. Mobile devices, such as smartphones and tablets, are critical tools for increasing workforce mobility and productivity. During disasters, FEMA employees use mobile devices with strong connectivity to keep in touch with survivors and the home office and take pictures, among other uses. Figure 1 shows a FEMA official using a smartphone to photograph the effects of Hurricane Delta. As of May 2022, FEMA had approximately 67,000 mobile devices in its inventory — 23,000 issued devices and 17,000 pending disposal. According to a FEMA official, the remaining 27,000 devices were ready to deploy.

Figure 1. FEMA Official Gathering Data on the Effects of Hurricane Delta.
Source: www.fema.gov

Mobile device security is critical to ensuring devices are used securely and sensitive information, such as email, personally identifiable information, and other confidential Government data is properly safeguarded. FEMA uses a cloud-based mobile device management (MDM) system to secure and manage its mobile devices. The MDM performs several important functions, such as connecting mobile devices to FEMA's network, monitoring the security and configuration settings on the devices, and removing data upon disposal. Within FEMA, the Office of the Chief Information Officer (OCIO) oversees the management, operation, and maintenance of the MDM.

Although mobile devices offer opportunities to improve business productivity, they also introduce the risk of cyber threats. Mobile devices containing sensitive Government data can also be disposed of, lost, stolen, or misused, increasing the risk that information may be compromised. FEMA follows the *Department of Homeland Security 4300A Sensitive Systems Handbook,*[1] which implements National Institute of Standards and Technology (NIST) and other department-wide mobile device requirements to secure mobile devices. Specifically, the Handbook requires FEMA to remove sensitive data from storage media, such that there is reasonable assurance the data cannot be

[1] *DHS 4300A Sensitive Systems Handbook*, Version 12.0, Nov. 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 Sept. 20, 2022.

easily retrieved and reconstructed, a process known as sanitization.[2] NIST *Special Publication 800-88, Revision 1, Guidelines for Media Sanitization,* provides guidelines for the sanitization of numerous types of information storage media, including mobile devices.[3] The guideline describes three sanitization methods:[4]

- Clear: resets the device to the factory settings.
- Purge: renders data recovery infeasible.
- Destroy: renders the device incapable of storing data, making the data inaccessible.

Mobile devices are also at risk for malicious software and misconfigured security settings. FEMA must ensure the MDM adheres to the *Defense Information Systems Agency Security Technical Implementation Guides*,[5] which are designed to make mobile device hardware and software as secure as possible. To supplement these policies, FEMA developed standard operating procedures for, among other things, international travel, sanitization, and vulnerability management. Within OCIO, FEMA's Mobility Service Center (MSC) is responsible for the sanitization of mobile devices and the management of the MDM. In addition, the FEMA Security Operations Center serves as the first tier for security monitoring, incident response, and forensics. The Security Operations Center is responsible for detecting incidents pertaining to mobile devices detected outside the United States or its territories.

We conducted this audit to determine whether FEMA secures its mobile devices to safeguard information accessed, stored, and processed on mobile devices.

Results of Audit

FEMA Did Not Document Whether All Data Was Removed from Mobile Devices to Prevent Unauthorized Access

The Handbook requires all smartphones and tablets containing sensitive information to be sanitized:

- before disposal;
- when users report them as lost or stolen;[6] or

[2] *DHS 4300A Sensitive Systems Handbook, Section 4.3.3, Media Sanitization and Disposal*, Nov. 15, 2015.
[3] *The National Institute of Standards and Technology Special Publication 800-88, Revision 1, Guidelines for Media Sanitization, Section 2.5, Types of Sanitization*, Dec. 2014.
[4] When the device is lost or stolen, sanitization can be achieved via a remote wipe command.
[5] *Interim Policy Memorandum: DHS Information System Configuration Standards,* June 25, 2019.
[6] Mobile devices that are reported lost, stolen, or otherwise unaccounted for are deemed disposed.

- when employees who have taken them on authorized international travel return.

According to FEMA's sanitization guidance,[7] once the device has been sanitized, FEMA's Mobile Service Center is required to complete a sanitization certificate (FEMA Form 137-1-1) certifying all data has been made inaccessible. See Appendix B for a copy of the sanitization certificate. FEMA provides additional guidance,[8] which requires all fields in the sanitization certificate to be filled out prior to returning the device to the employee. A copy of the sanitization certificate must be attached to the device, and another copy must be retained for 3 years. However, no guidance is provided for handling the form when lost or stolen devices are sanitized.

During fiscal years 2020 through 2021, we identified a total of 16,444 mobile devices that fell into one of the two categories below requiring sanitization. Specifically, in FYs 2020 through 2021, FEMA reported:

- 15,330 disposals; and
- 1,114 lost or stolen devices.

Additionally, FEMA reported no devices taken on international travel during FYs 2020 through 2021. There were 39 instances of devices taken on authorized international travel from November 2021 through June 2022 that were required to be sanitized.

MSC could not provide sanitization certificates for any of the 15,330 mobile devices disposed of during FYs 2020 and 2021. We requested sanitization certificates for a sample of devices disposed of during this timeframe. According to staff, they were unaware sanitization certificates were required and said they did not have them for any of the devices in our scope. We were not able to physically test the devices that had been disposed of to determine whether they were, in fact, properly sanitized.

[7] *FEMA's RX SOP Electronic and Hard Copy Media Sanitization and Release, Section VI, Responsible Office,* Jan. 1, 2016.
[8] *FEMA Sanitization Standard Operating Procedure*, Sept. 26, 2018.

MSC could not provide sanitization certificates for any of the 1,114 devices reported as lost or stolen in FYs 2020 and 2021. OCIO has the capability to issue a remote wipe command to a device, via the MDM. We reviewed the data logs from the MDM to determine whether MSC sent wipe commands to erase all data stored on the lost or stolen phones. Although FEMA employees reported 890 lost or stolen smartphones in FYs 2020 and 2021, we found MSC only sent wipe commands to 50 of the 890 (6 percent) phones, as shown in Figure 2. We could not determine the number of wipe commands sent to the 224 lost or stolen tablets because FEMA did not track this type of information prior to May 2022.[9] According to OCIO personnel, they only issue wipe commands upon request.

Figure 2. Percentage of Lost or Stolen Phones Properly Erased

Source: DHS Office of Inspector General analysis of FEMA's lost and stolen phone data

Finally, MSC did not document whether the 39 mobile devices taken on authorized international travel were properly sanitized upon employees' return. *FEMA Directive 122-1*, *Official International Travel* prohibits all travelers from taking their Government-issued mobile devices internationally.[10] Based on the directive, FEMA travelers who obtain approval for official international travel may initiate a request to be issued a loaner travel device from MSC. FEMA may then issue the employee a loaner device to use while on authorized travel. The loaner device cannot be connected to any FEMA systems or network after the employee returns to the United States and must be properly sanitized upon completion of travel.

We requested sanitization certificates for all 39 loaner devices that employees were given for official international travel. However, MSC could not provide the certificates certifying that all data was erased prior to reissuance of devices to other FEMA users. According to MSC personnel, they were sanitizing the devices, but were unaware they needed to complete the sanitization certificates. We did not confirm whether these devices were properly sanitized as part of this audit.

We attribute the absence of documentation to FEMA's OCIO not ensuring employees in MSC followed FEMA policy. Although FEMA OCIO created the sanitization certificate to help with the documentation process, MSC did not provide the form to employees or stress the importance of completing it to

[9] FEMA uses two types of MDMs to manage mobile devices, the Mobility Environment for FEMA and Automated Construction Estimating (ACE) Software. ACE only has tablets enrolled, and ACE did not track remote wipe commands prior to May 2022. Therefore, we could not include tablets in the scope of this test.

[10] *FEMA Directive 122-1, Official International Travel, Section B, FEMA Traveler Responsibilities*, Jan. 16, 2020.

comply with the Handbook. Some of the employees we interviewed were unaware the sanitization certificate existed. After bringing this to FEMA's attention, FEMA officials acknowledged that the sanitization certificate may not have been properly implemented and confirmed that sanitization certificates should have been completed for all 16,483 devices.

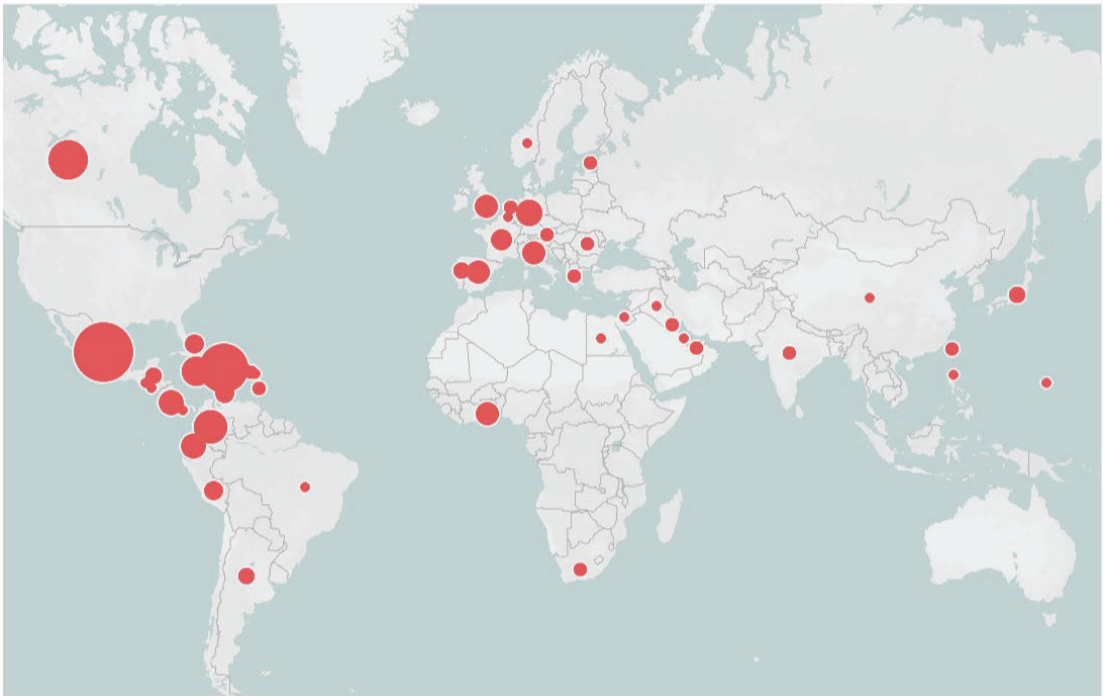
FEMA did not sanitize most devices reported lost or stolen in FYs 2020 and 2021 due to insufficient guidance. Although the Handbook requires lost or stolen devices to be remotely wiped, FEMA did not have supplemental guidance with more stringent, component-specific requirements for sanitizing lost or stolen mobile devices. FEMA has a personal property instruction[11] for reporting lost or stolen devices, but the instruction does not include detailed sanitization procedures. Specifically, the instruction does not specify the timeframe in which a lost or stolen device should be wiped or who is responsible for initiating the remote wipe command. The instruction also does not include a requirement to document the sanitization process. It is critical for FEMA to ensure all data has been properly erased in a timely manner since these devices are no longer in FEMA's possession.

FEMA Did Not Disable All Mobile Devices Taken Outside the United States or Its Territories without Prior Travel Authorization

The Handbook prohibits all travelers from taking their Government-issued mobile devices internationally for any personal or official foreign travel, unless specifically authorized by their supervisor. In August 2021, the DHS Office of the Chief Security Officer and DHS OCIO issued additional guidance on foreign travel[12] requiring that all mobile devices detected outside the United States or its territories without prior authorization be disabled and their information be forwarded to the corresponding office's OCIO, the Office of the Chief Security Officer, and the Office of Professional Responsibility. From October 2020 through April 2022, FEMA's Security Operations Center detected 227 unauthorized mobile devices internationally. See Figure 3 for a map of the locations.

[11] FEMA *Instruction 119-7-1, FEMA Personal Property Asset Management Program*, Nov. 20, 2020.
[12] *Joint DHS Office of the Chief Security Officer and Office of the Chief Information Officer Guidance on Foreign Travel*, Aug. 18, 2021.

Figure 3. Unauthorized Mobile Devices Detected by FEMA's Security Operations Center outside the United States or Its Territories



Source: DHS OIG analysis of FEMA's unauthorized mobile devices detected internationally

We reviewed a sample of nine unauthorized mobile devices detected internationally after the guidance was issued to determine whether the devices were properly disabled, as required by policy. We found FEMA only disabled two of nine devices (22 percent) detected internationally. This occurred because FEMA is only disabling devices identified as having been detected in hostile countries on the International Traffic in Arms Regulations (ITAR)[13] list. See Appendix C for a list of all ITAR countries.

As of November 2022, FEMA had not updated its policy to reflect DHS' August 2021 foreign travel guidance requiring that all devices detected internationally be disabled. According to *FEMA's Response Playbook Standard Operating Procedure,*[14] updated in July 2021, once a connection has been detected from a country on the ITAR list, FEMA will disable the mobile account and it will not be reinstated until the employee has cleared an investigation by the Office of Professional Responsibility and the Office of the Chief Security Officer. If the device is detected in a non-ITAR country, FEMA's Security Operations Center will create a security event notification informing the Office of Professional

[13] According to the Department of State, Directorate of Defense Trade Controls, "ITAR (22 C.F.R. Parts 120-130) governs the manufacture, export, and temporary import of defense articles, the furnishing of defense services, and brokering activities involving items described on the United States Munitions List." *See also,* 22 C.F.R. § 126.1(a) "It is the policy of the United States to deny licenses and other approvals for exports and imports of defense articles and defense services, destined for or originating in certain countries."
[14] *FEMA Response Playbook Standard Operating Procedure,* Jan. 2022.

Responsibility, the Office of the Chief Security Officer, and the Office of Privacy, as well as the traveler's supervisor by email, of the security incident. However, the traveler will be permitted to continue working remotely unless directed otherwise by an investigative authority.

We determined that the two disabled devices in our sample were both detected in countries on the ITAR list. In one example, FEMA identified an employee who brought a FEMA-issued mobile device to Iraq without authorization and connected it to the FEMA network. In the second instance, an employee accessed FEMA's network from Port-au-Prince, Haiti. According to the results of the investigations, these employees were not authorized for official travel and violated FEMA policy.

Due to the absence of documentation, we could not determine whether FEMA sanitized the nine unauthorized devices taken internationally. FEMA does not have a requirement to sanitize unauthorized mobile devices — FEMA's policy only requires sanitizing authorized loaner devices. FEMA may be increasing its risk of compromise and potentially exposing the network to malicious malware by allowing employees in non-ITAR countries to continue to work without disabling their Government-issued device and by not requiring employees' devices to be sanitized upon their return to the United States. The disabling of mobile devices is as important as sanitization to protect FEMA's network from compromise.

FEMA's MDM System Adhered to Configuration Requirements

We conducted a technical review and testing of FEMA's MDM system and applications to determine whether security settings were properly configured on mobile devices, and if FEMA's mobile applications were updated to prevent unauthorized access to information stored, accessed, and processed by the mobile devices. We determined FEMA's configuration management controls comply with the *Defense Information Systems Agency Security Technical Implementation Guides.* These controls provide reasonable assurance that the MDM enforces security controls and that FEMA's mobile devices are configured and operating securely, as intended. However, in our technical review of FEMA's security management controls, specifically the vulnerability and patch management, we identified six vulnerabilities[15] that could potentially expose the devices to mobile application attacks. For example, one vulnerability may provide users with more access than required, while another may lead to weak temporary passwords. At the time of our audit, FEMA was taking steps to remediate the vulnerabilities.

[15] We excluded three vulnerabilities from our results because the vulnerabilities existed on devices that were not enrolled in the MDM and on a platform FEMA no longer supports.

Conclusion

FEMA did not always secure information stored on mobile devices. Without better security controls in place, information accessed, stored, and processed on FEMA's mobile devices may be at risk of unauthorized access and susceptible to cyberattacks. Mobile devices have evolved to become the critical link between remote users and their home office; providing travelers access to business applications and data they would otherwise not have. Mobile device software and hardware have inherent vulnerabilities. Successful exploitation may allow adversaries to remotely activate microphones and cameras, track locations, or steal information stored on a device. FEMA must act to secure both the physical assets and the network from evolving cyber threats.

Recommendations

Recommendation 1: We recommend FEMA's Chief Information Officer develop and implement a process, with specific roles and responsibilities, for sanitizing mobile devices prior to disposition.

Recommendation 2: We recommend FEMA's Chief Information Officer update existing guidance with the proper sanitization steps for all lost or stolen mobile devices.

Recommendation 3: We recommend FEMA's Chief Information Officer implement and formally communicate to employees the requirement to document sanitization of mobile devices taken outside the United States or its territories, on authorized travel upon employees' return to the United States from such travel.

Recommendation 4: We recommend FEMA's Chief Information Officer update *FEMA's Response Playbook Standard Operating Procedure* to comply with the *Joint DHS Office of the Chief Security Officer and Office of the Chief Information Officer Guidance on Foreign Travel,* requiring the disabling of all unauthorized mobile devices that have been taken on international travel.

Management Comments and OIG Analysis

FEMA's Associate Administrator of the Office of Policy and Program Analysis provided written comments on the draft report, which are included in their entirety in Appendix A. In the comments, FEMA indicated it appreciated our work on this audit. FEMA stated that it is steadfastly committed to strengthening its cybersecurity posture to ensure information stored on mobile devices remains secure while enhancing the use of such devices for improved productivity. FEMA concurred with all four recommendations in this report. FEMA submitted technical comments separately, which we addressed as appropriate. We consider all four recommendations open and resolved. A summary of FEMA's management responses and our analysis follow.

FEMA Response to Recommendation 1: Concur. FEMA OCIO implemented a ServiceNow workflow to ensure that all wipe command requests have an official record. Additionally, the OCIO Information Technology Management (ITM) Policy and Governance Division, in coordination with the FEMA Office of the Chief Administrative Officer (OCAO) Property stakeholders, will review and, if necessary, modify existing device sanitization standard operating procedures. Estimated Completion Date (ECD): December 29, 2023.

OIG Analysis: FEMA's corrective actions are responsive to the recommendation. We consider this recommendation resolved and open until FEMA provides documentation to support the corrective actions have been completed and until FEMA identifies specific roles and responsibilities for sanitizing mobile devices prior to disposition.

FEMA Response to Recommendation 2: Concur. The FEMA OCIO ITM Policy and Governance Division, in coordination with FEMA OCAO Property stakeholders, will review and, if necessary, modify existing device sanitization standard operating procedures. ECD: December 29, 2023.

OIG Analysis: FEMA's corrective actions are responsive to the recommendation. We consider this recommendation resolved and open until FEMA provides documentation to support the corrective actions have been completed.

FEMA Response to Recommendation 3: Concur. FEMA OCIO will review existing policy and determine the best approach for meeting mission requirements and maximizing flexibility for FEMA staff while remaining in compliance with all Federal policies and regulations. Upon conclusion of this review, FEMA OCIO will distribute communications to FEMA staff outlining any policy changes and best practices, as appropriate. ECD: December 29, 2023.

OIG Analysis: FEMA's corrective actions are responsive to the recommendation. We consider this recommendation resolved and open until FEMA provides documentation to support the corrective actions have been completed.

FEMA Response to Recommendation 4: Concur. FEMA OCIO will review existing policy and determine the best approach for meeting mission requirements and maximizing flexibility for FEMA staff while remaining in compliance with all Federal policies and regulations. Upon conclusion of this review, FEMA OCIO will distribute communications to FEMA staff outlining any policy changes and best practices, as appropriate. ECD: December 29, 2023.

OIG Analysis: FEMA's corrective actions are responsive to the recommendation. We consider this recommendation resolved and open until FEMA provides documentation to support the corrective actions have been completed.

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*.

The objective of this audit was to determine whether FEMA secures its mobile devices to safeguard information accessed, stored, and processed on mobile devices. To answer our objective, we limited the scope of the audit to the sanitization and documentation procedures for mobile devices:

- disposed of;
- reported lost or stolen; and
- taken on international travel (authorized and unauthorized).

To gain an understanding of how FEMA secures its mobile devices to safeguard information accessed, stored, and processed, the team interviewed selected FEMA officials from the Office of Chief Administrator Officer, the Office of the Chief Information Officer, the Office of Policy and Program Analyses, the Office of the Chief Procurement Officer, and the Office of the Chief Security Officer. We reviewed Federal laws, Department directives, and FEMA policies and procedures related to the management and security of mobile devices.

To determine the universe of mobile devices that should have been sanitized, the team requested FEMA's mobile device data for FYs 2020 and 2021, for disposition and lost or stolen devices. The audit team received the following datasets:

- Disposition: Two datasets, one containing 9,929 smartphones and the other 6,200 tablets. The DHS OIG Data Services Division separated the disposed from lost or stolen,[16] which yielded a total of 15,330 mobile devices that had been disposed of.

- Lost or stolen: One dataset of 1,120 lost or stolen mobile devices. However, it contained six data entries for laptops, which were removed. As a result, the reported total number of lost or stolen devices is 1,114. To determine whether remote wipes were executed, we also requested a data log of all remote wipes sent for FYs 2020 and 2021. We compared the serial numbers of the mobile devices reported lost and stolen to those of the mobile devices that received a remote wipe.

To determine the universe of mobile devices that should have been sanitized after authorized travel, the team requested and received FEMA's mobile device data from November 2021 through June 2022. The audit team received a dataset of 39 mobile devices issued for approved international travel.

To determine whether remote wipes were sent to the 890 lost and stolen smartphones, we received a list of all remote wipe commands for FYs 2020 and 2021 sent from the MDM. The DHS OIG Data Services Division analyzed the datasets and determined 50 wipe commands were issued to smartphones that were reported lost or stolen in our scope.

To determine whether unauthorized mobile devices detected outside the United States or its territories were disabled, we requested data from the Security Operations Center for all unauthorized mobile devices detected internationally from October 2019 through April 2022. We received a dataset with 244 entries for unauthorized mobile devices detected internationally. We removed all double entries for a total universe of 227. We then requested 20 judgmentally selected investigations from the Office of Professional Responsibility. We analyzed the results of the investigations, including information on FEMA's recommended action. We then selected nine entries to sample with incident dates after the August 2021 *Joint DHS Office of the Chief Security Officer and Office of the Chief Information Officer Guidance on Foreign Travel* memorandum.

We assessed the reliability of information we received pertaining to mobile devices and determined the data was sufficiently reliable for the purpose of the audit.

[16] FEMA also provided a separate dataset of 1,120 lost and stolen mobile devices. As a result, the DHS OIG Data Services Division removed 799 duplicate lost and stolen mobile devices from the disposition dataset. These 321 discrepancies between the datasets occurred because disposition data is recorded at the time the device is removed from the system of record and lost or stolen data is recorded at the time a report of survey is submitted.

We assessed internal controls related to FEMA's mobile device management. The internal control deficiencies we found are discussed in the Results of Audit section of this report. 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.

As part of this audit, we coordinated with the DHS OIG Office of Innovation's Cybersecurity Risk Assessment (CRA) division, which provided technical support for this audit. The CRA division performed technical testing to evaluate the compliance of security controls implemented related to *Defense Information Systems Agency Security Technical Implementation Guides*. The CRA division collaborated with FEMA staff to review each *Defense Information Systems Agency Security Technical Implementation Guides'* configuration setting within the system. Additionally, the CRA division reviewed the static code configuration settings and observed FEMA staff perform static application security scans on FEMA's mobile applications. FEMA provided comments to the test results.

We conducted this performance audit between January 2022 and March 2023 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

DHS OIG's Access to DHS Information

During this audit, FEMA provided timely responses to our requests for data and information and did not deny or delay access to the data and information we requested.

The Office of Audits major contributors to this report are Richard Harsche, Director; Tarsha Cary Director; Peter Christopher, Audit Manager; Juan Santana, Auditor-in-Charge; Rolando Chavez, Auditor; Vera Cropp, Auditor; Usman Mohammed, IT Specialist; Joseph Welton, Program Analyst; Daniel Grogan, Data Scientist; Lindsey Koch, Communications Analyst; and Michael Nasuti, Independent Reference Reviewer. The Office of Innovation major contributors are Thomas Rohrback, Director; Rashedul Romel, Supervisory IT Cybersecurity Specialist; Jason Dominguez, Supervisory IT Cybersecurity Specialist; Taurean McKenzie, IT Specialist; and Joseph Sanchez, IT Specialist.

Appendix A
FEMA Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20472

FEMA

May 31, 2023

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

FROM: Cynthia Spishak
Associate Administrator
Office of Policy and Program Analysis

CYNTHIA SPISHAK
Digitally signed by CYNTHIA SPISHAK
Date: 2023.05.31 18:17:43 -04'00'

SUBJECT: Management Response to Draft Report: "FEMA Did Not Always Secure Information Stored on Mobile Devices to Prevent Unauthorized Access"
(Project No. 22-020-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The Federal Emergency Management Agency (FEMA or the Agency) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

Agency leadership is pleased to note OIG's positive recognition that FEMA's Mobile Device Management (MDM) system configuration management controls comply with the Defense Information Systems Agency Security Technical Implementation Guides and provide reasonable assurance that mobile devices are operating securely, as intended. FEMA presently has no evidence of data breaches or leaks, and the Agency is steadfastly committed to strengthening its cybersecurity posture to ensure information stored on mobile devices remain secure while enhancing the use of such devices for improved productivity.

The draft report contained four recommendations with which FEMA concurs. Enclosed find our detailed response to each recommendation. FEMA previously submitted technical comments addressing accuracy and sensitivity 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 again in the future.

Enclosure

Enclosure: Management Response to Recommendations Contained in 22-020-AUD-DHS

OIG recommended that FEMA's Chief Information Officer (OCIO):

Recommendation 1: Develop and implement a process, with specific roles and responsibilities, for sanitizing mobile devices prior to disposition.

Response: Concur. On July 6, 2022 FEMA OCIO implemented a ServiceNow workflow to ensure that all requests for device wipes have an official record for future review. Additionally, the OCIO Information Technology Management (ITM) Policy and Governance Division – in coordination with the FEMA Office of the Chief Administrative Officer (OCAO) Property stakeholders – will review and, if necessary, modify existing device sanitization standard operating procedures. Estimated Completion Date (ECD): December 29, 2023.

Recommendation 2: Update existing guidance with the proper sanitization steps for all lost or stolen mobile devices.

Response: Concur. FEMA OCIO ITM Policy and Governance Division – in coordination with FEMA OCAO Property stakeholders – will review and, if necessary, modify existing device sanitization standard operating procedures. ECD: December 29, 2023.

Recommendation 3: Implement and formally communicate to employees the requirement to document sanitization of mobile devices taken outside of the continental United States on authorized travel upon employees' return to the United States from such travel.

Response: Concur. FEMA OCIO will review existing policy and determine the best approach for meeting mission requirements and maximizing flexibility for FEMA staff while remaining in compliance with all federal policies and regulations. Upon conclusion of this review, FEMA OCIO will distribute communications to FEMA staff outlining any policy changes and best practices, as appropriate. ECD: December 29, 2023.

Recommendation 4: Update FEMA's Response Playbook Standard Operating Procedure to comply with the Joint DHS Office of the Chief Security Officer and Office of the Chief Information Officer Guidance on Foreign Travel requiring the disabling of all unauthorized mobile devices that have been taken on travel outside the continental United States.

2

Response: Concur. FEMA OCIO will review existing policy and determine the best approach for meeting mission requirements and maximizing flexibility for FEMA staff while remaining in compliance with all federal policies and regulations. Upon conclusion of this review, FEMA OCIO will distribute communications to FEMA staff outlining any policy changes and best practices, as appropriate. ECD: December 29, 2023.

3

Appendix B
FEMA's Sanitization Certificate

DEPARTMENT OF HOMELAND SECURITY
FEDERAL EMERGENCY MANAGEMENT AGENCY
OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO)
ATTACHMENT A - MULTI-PART FORM TO BE USED FOR SANITIZATION CERTIFICATION

Section 1 - Custodian (End User) Completes (Only One Item Per Form)

1. Organization/Office Symbol	2. Print Custodian (End User) Name	3. Custodian Phone No.

4. Item Description (Check One)

☐ Laptop ☐ Desktop ☐ Mobile Device ☐ Cell Phone ☐ Thumb Drive ☐ Other (describe below)

5. Item Description (if Other)

6. Item Manufacturer	7. Part Number	8. IMEI or MEID	9. Item Serial Number	10. Barcode Number

Section 2 - Local IT Helpdesk / IT Site Support Completes

By signing below I certify that I have received the property listed above for sanitization ***and provided a copy of this document to the custodian.***

11. Printed Name & Organization of Individual *Accepting* Equipment From Custodian	12. Date Received from Custodian

13. Signature of Individual listed in Box 11	Custodian Initial here confirming a copy has been provided	

14. ***Has Apple/Google account been removed? Circle one (YES NO N/A)***

15. Sanitization Method Used (e.g., software used)

By signing below I am certifying that I have sanitized the property listed above in accordance with procedures found on the OCIO's Planning, Policy, Architecture and Governance Web page at: https://intranet.fema.net/org/ms/ocio/bob/OPPAG/Pages/OCIOSOPs.aspx, rendering data inaccessible, and have notified the Custodian (End User) that the property is ready to be picked up. In addition I have sent a copy of this signed form to the Cyber Security Division, OCIO, FEMA via Fax to: 540-686-4259 or e-mail to OfficeofCyberSecurity@fema.dhs.gov

16. Printed Name of IT Technician *Performing Sanitization*	17. Signature of IT Technician Who *Performed Sanitization*	18. Sanitization Date

Section 3 - Custodian (End User) Completes

By signing below I am certifying that I have received my equipment/media from the Helpdesk / IT Site Support.

19. Signature of Custodian	20. Date Received

Instructions for Custodian (End User): The Custodian turns-in the property to their issuing Custodial Officer (CO) or Accountable Property Officer (APO) only after equipment has been sanitized and this form is signed in all applicable locations by the individual who performed sanitization. Custodian must ensure that the CO or APO signs their hand receipt indicating that the property has been turned in and should retain the hand receipt, along with this form, as evidence of the turn-in. Custodian: when giving the item to IT support, make a copy for your records prior to giving them the item after the IT person has signed box 14; as proof of chain of custody until it is returned.

All smart phones and tablets must be sanitized prior to turn-in. This includes removal of the Apple/Google account as appropriate.

3 Part Form: White copy is for APO (remains with the property until final disposition or reissue), Blue copy for Custodian (End User); Yellow copy for IT Helpdesk/IT Site Support. Order of Colors (top to bottom) is Yellow, Blue, White (with adhesive to stick to property).

FEMA Form 137-1-1, MAR 2016 **White copy (remains with the property until final disposition or reissue)**

Appendix C
ITAR Countries

Country
Afghanistan
Central African Republic
China
Cuba
Cyprus
Democratic Republic of Congo
Eritrea
Haiti
Iran
Iraq
Lebanon
Libya
North Korea
Russia
Somalia
South Sudan
Sudan
Syria
Zimbabwe

Source: *FEMA Response Playbook Standard Operating Procedure*, Version 4.3, January 2022

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, U.S. Government Accountability Office/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
FEMA Administrator

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" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, 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