



U.S. DEPARTMENT OF HOMELAND SECURITY **OFFICE OF INSPECTOR GENERAL**

OIG-24-61

September 26, 2024

FINAL REPORT

ICE Did Not Always Manage and Secure Mobile Devices to Prevent Unauthorized Access to Sensitive Information





OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

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

September 26, 2024

MEMORANDUM FOR: The Honorable Patrick J. Lechleitner
Deputy Director and Senior Official Performing
The Duties of the Director
U.S. Immigration and Customs Enforcement

FROM: Joseph V. Cuffari, Ph.D. GLENN E SKLAR Digitally signed by GLENN E SKLAR for
Inspector General E SKLAR Date: 2024.09.25 18:14:50 -04'00'

SUBJECT: *ICE Did Not Always Manage and Secure Mobile Devices to Prevent Unauthorized Access to Sensitive Information*

Attached for your action is our final report, *ICE Did Not Always Manage and Secure Mobile Devices to Prevent Unauthorized Access to Sensitive Information*. We incorporated the formal comments provided by your office.

The report contains eight recommendations aimed at improving ICE's mobile device security. Your office concurred with all eight recommendations. Based on information provided in your response to the draft report, we consider recommendation 3 open and unresolved. As prescribed by Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for the recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendation will be considered open and unresolved.

We consider recommendations 1, 2, 4, 5, 6, 7, and 8 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 and of the disposition of any monetary amounts.

Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, 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 contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General for Audits at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

ICE Did Not Always Manage and Secure Mobile Devices to Prevent Unauthorized Access to Sensitive Information

September 26, 2024

Why We Did This Audit

ICE issues its personnel and contractors mobile devices (e.g., smartphones and tablets) to help them perform duties related to enforcing Federal laws governing border control, customs, trade, and immigration. Although mobile devices increase workforce mobility and productivity, they also increase the risk of cyberattacks or loss of sensitive data. We conducted this audit to determine the extent to which ICE manages and secures its mobile devices.

What We Recommend

We made eight recommendations to improve ICE'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

U.S. Immigration and Customs Enforcement (ICE) did not effectively manage and secure its mobile devices or the infrastructure supporting the devices. Specifically, ICE did not implement security settings required to protect its mobile devices and did not mitigate vulnerabilities from applications installed on these devices. In addition, ICE did not use its Mobile Device Management software and other threat defense tools to fully manage and secure some mobile devices and did not address vulnerabilities within the Mobile Device Management software and the servers supporting it. Further, ICE did not implement increased monitoring and protection for devices used outside the United States, which were at a higher risk of cyberattacks. Finally, ICE did not always perform required steps to reduce risks associated with disposal, loss, or theft of its mobile devices.

These management and security concerns occurred primarily because ICE did not establish or implement sufficient security policies and processes. ICE personnel were unaware of some security requirements and relied on unclear or contradictory guidance. As a result, ICE mobile devices and the sensitive information they contain may be at a higher risk of unauthorized access and more susceptible to cyberattacks.

ICE Response

ICE concurred with all eight recommendations. Appendix B contains ICE's management response in its entirety.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Table of Contents

Background	1
Results of Audit	3
ICE Did Not Effectively Manage Its Mobile Device Settings and Applications	3
ICE Did Not Properly Manage and Secure Infrastructure Supporting Mobile Devices.....	5
ICE Did Not Properly Monitor or Secure Devices Used Outside the United States	8
ICE May Not Have Properly Sanitized Devices for Disposal or Properly Handled Lost and Stolen Mobile Devices	9
Conclusion.....	11
Recommendations.....	12
Management Comments and OIG Analysis.....	13
Appendix A: Objective, Scope, and Methodology.....	16
DHS OIG’s Access to DHS Information.....	18
Appendix B: ICE Comments on the Draft Report	19
Appendix C: Report Distribution.....	27

Abbreviations

CISO	Chief Information Security Officer
DISA	Defense Information Systems Agency
ICE	U.S. Immigration and Customs Enforcement
MDM	Mobile Device Management
MTD	Mobile Threat Defense
OCIO	Office of the Chief Information Officer
SOC	Security Operations Center
STIG	Security Technical Implementation Guide
UEM	Unified Endpoint Manager



Background

U.S. Immigration and Customs Enforcement (ICE) is the largest investigative arm of the Department of Homeland Security and is responsible for enforcing Federal laws governing border control, customs, trade, and immigration. ICE eliminates vulnerabilities domestically and abroad and combats terrorism; transnational threats; and criminal organizations that seek to exploit legitimate trade, travel, and finance systems. As of 2024, ICE has more than 20,000 law enforcement and support personnel in more than 300 offices across the United States and more than 90 offices in over 50 countries around the world, as shown in Figure 1.

Figure 1. Map of ICE International Offices



Source: Prepared by DHS Office of Inspector General from data on the ICE Homeland Security Investigations website

ICE issues its personnel, and contractors, mobile devices (e.g., smartphones and tablets) to help them carry out their duties, as shown in Figure 2. ICE maintains an inventory of approximately 21,000 mobile devices. These devices provide telecommunications capabilities, connectivity to ICE information systems, and work-related applications. For example, one ICE-owned application allows ICE personnel to capture and search for the biometric information of people they encounter in real time. In addition to work-related applications, ICE allows personnel to download and install applications directly from official third-party application stores, such as applications related to maps, weather, and airlines for personal convenience.

ICE's Office of the Chief Information Officer (OCIO) oversees the security of ICE's information system infrastructure and ensures ICE complies with information system security requirements, including those related to mobile devices. ICE OCIO is responsible for, among other things, establishing security standards for ICE-issued mobile devices; providing distribution, operation,



and administrative support for ICE-issued mobile devices; maintaining a list of applications and digital media approved for official Government business use; and monitoring the activity on all ICE-issued mobile devices to ensure compliance with ICE policies.

Although mobile devices increase workforce mobility and productivity, they also increase the risk of cyberattacks or loss of sensitive data. To reduce those risks, ICE OCIO centrally manages ICE's mobile devices using a Mobile Device Management (MDM) system that can enforce ICE security policies. The main goal of MDM technology is to ensure that devices are secure before allowing access to sensitive government data. ICE OCIO can perform several important functions through the MDM, such as managing how mobile devices connect to ICE's network, restricting device capabilities, remotely erasing device data, and implementing and monitoring security settings on the devices. To further protect mobile devices, ICE OCIO uses Mobile Threat Defense (MTD), a software application, to monitor device activity and detect improper settings, malicious software, cyberattacks, and other vulnerabilities on mobile devices.

Figure 2. ICE Officer Using Mobile Device



Source: Photo from ICE website

The MDM is an essential tool for securing and managing mobile devices. However, if the technology is improperly used or not properly protected, hackers could exploit it to illegally access ICE's network or devices. Accordingly, ICE OCIO designated the system supporting the MDM (including hardware, firmware, and software) as a high value asset for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to national security interests.

We conducted this audit to determine the extent to which ICE manages and secures its mobile devices.

As part of this audit, we issued a separate management alert identifying risks posed by ICE's management of user-installed mobile applications.¹ We issued five recommendations to the ICE Chief Information Officer to address these risks. We also issued a recommendation to the DHS Chief Information Security Officer (CISO) to determine whether similar issues exist for other DHS components and to take immediate action as appropriate. A summary of the issues identified in

¹ *Management Alert – ICE Management and Oversight of Mobile Applications*, OIG-24-02, October 30, 2023.



our management alert and the status of the recommendations are provided in the “ICE Did Not Effectively Manage Its Mobile Device Settings and Applications” section of this report.

Results of Audit

ICE did not effectively manage and secure its mobile devices or the infrastructure supporting the devices. Specifically, ICE did not implement security settings required to protect its mobile devices and did not mitigate vulnerabilities from applications installed on these devices. In addition, ICE did not use its MDM software and other threat defense tools to fully manage and secure some mobile devices and sufficiently address vulnerabilities within the MDM and the servers supporting it. Further, ICE did not implement increased monitoring and protection for devices used outside the United States, which were at a higher risk of cyberattacks. Finally, ICE did not always perform required steps to reduce risks associated with disposal, loss, or theft of its mobile devices.

These management and security concerns occurred primarily because ICE did not establish or implement sufficient security policies and processes. ICE personnel were unaware of some security requirements and relied on unclear or contradictory guidance. As a result, ICE mobile devices and the sensitive information they contain may be at a higher risk of unauthorized access and more susceptible to cyberattacks.

ICE Did Not Effectively Manage Its Mobile Device Settings and Applications

ICE did not effectively manage its mobile device settings and applications to reduce the risks associated with ICE-issued mobile devices. ICE did not use appropriate mobile device security settings, installed custom-developed mobile applications that contained vulnerabilities onto mobile devices, and allowed employees and contractors to download risky applications onto mobile devices.

ICE Did Not Use Appropriate Mobile Device Security Settings

In 2019, DHS required² components to apply the Defense Information Systems Agency’s (DISA) Security Technical Implementation Guides (STIGs) when establishing mobile device security settings. DHS also requires³ components to complete a security authorization process to measure and mitigate mobile device risks.

² Paul Beckman, DHS CISO memorandum, *Interim Policy Memorandum: DHS Information System Configuration Standards*, June 25, 2019.

³ DHS 4300A, Attachment I, *Sensitive Mobile Devices*, January 2022.

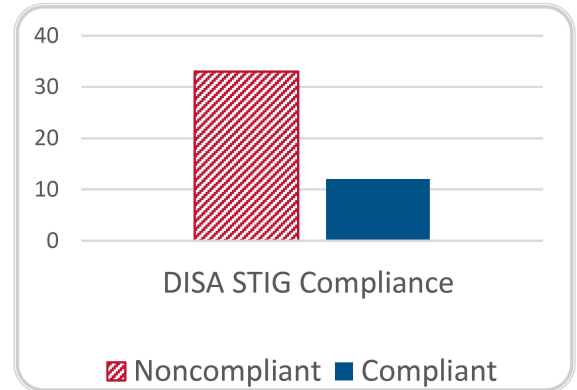


However, ICE did not always apply DISA STIGs when establishing mobile device security settings. We reviewed 45⁴ security settings on ICE’s mobile devices to determine if the settings were set as required. Of the 45 settings we reviewed, 33 (73 percent) did not meet DISA STIG guidance, as shown in Figure 3. These settings are meant, for example, to restrict devices’ capability to transfer sensitive information to other devices, move sensitive information to a less secure part of the device, or allow built-in virtual assistant tools to transmit recorded information to third-party servers.

This occurred because ICE OCIO officials were initially unaware of DHS’ requirement to use DISA STIGs as guidance or were unaware that DISA STIG guidance was available for the types of mobile devices ICE uses.

Although, according to ICE officials, the component implemented compensating controls that reduced associated risks, ICE did not complete the proper security authorization process, which would have included assessing whether the security settings on its mobile devices met requirements and implementing best practices to acceptably reduce risk. In January 2023, ICE OCIO created a remediation plan in which it formally documented that it had not met the requirement to use DISA STIGs. The remediation plan did not identify compensating controls or include detailed actions to facilitate implementation of the required security settings.

Figure 3. ICE Mobile Device Security Settings



Source: Developed by DHS OIG based on analysis of ICE data

ICE Installed Custom-Developed Mobile Applications that Contained Vulnerabilities onto Mobile Devices

Since at least 2014, DHS policy requires that components review the source code of custom-developed applications for vulnerabilities.⁵ DHS’ policy⁶ also requires that components analyze application source code when developing and updating high-impact systems.

ICE OCIO developed two custom mobile device applications to support ICE’s mission. We performed vulnerability testing to assess the level of security on these two applications. Although we did not identify any critical or high-risk vulnerabilities on one, the second application contained three critical and five high-risk vulnerabilities. ICE was unaware of these vulnerabilities until we shared our testing results.

⁴ DISA STIGs include 51 required settings and approximately 100 recommended settings. We limited our testing to the 45 required settings for which the information needed for testing was available.

⁵ DHS 4300A, *DHS Sensitive Systems Policy Directive*, V.11.0, April 30, 2014.

⁶ DHS 4300A, Attachment CC, *NIST 800-53r5 Control Baselines and ODPs*.



ICE did not identify the critical and high-risk vulnerabilities in the second mobile application because it did not review the source code of its custom-developed application. In addition, ICE did not have policies and procedures to test for vulnerabilities in the source code of its applications. ICE management stated that it plans to address the vulnerabilities identified in the second mobile application and update its policies and procedures to require reviews of custom-developed application source code.

ICE Allowed Employees and Contractors to Download Risky Applications onto Mobile Devices

As part of this audit, we issued a separate management alert identifying risks posed by ICE's management of user-installed mobile applications.⁷ These mobile applications posed a risk to ICE's operations and its employees, as well as to the Department. This risk was intensified given some of the mobile applications identified are associated with foreign adversaries. ICE's outdated and overly permissive personal use policy enabled nearly unlimited personal use of the ICE-issued mobile devices. Further, ICE did not sufficiently manage, monitor, or assess most user-installed applications for potential impacts on device or data security because ICE considered them to be personal applications.

To address the risks identified, we issued five recommendations to the ICE Chief Information Officer and one to the DHS CISO. ICE and the Department have developed corrective action plans or have already taken action to address our recommendations. As of September 2024, all six recommendations are resolved but will remain open until we verify implementation of the corrective actions.

ICE Did Not Properly Manage and Secure Infrastructure Supporting Mobile Devices

ICE did not effectively manage and secure the information technology infrastructure supporting ICE-issued mobile devices. Specifically, ICE did not fully use MDM and threat defense tools to manage and protect some of its mobile devices. Nor did ICE identify or sufficiently address vulnerabilities of web applications within the mobile device infrastructure, vulnerabilities of mobile device infrastructure servers, and noncompliant mobile device infrastructure security settings.

ICE Did Not Fully Use MDM and Threat Defense Tools to Manage and Protect Some of Its Mobile Devices

DHS policy⁸ requires ICE to monitor and configure mobile devices using a centralized MDM system and recommends MTD be installed on devices. DISA STIGs require that mobile devices be added to the MDM in such a way that they can be properly protected using the MDM.

⁷ *Management Alert – ICE Management and Oversight of Mobile Applications*, OIG-24-02, October 30, 2023.

⁸ DHS 4300A, Attachment I, *Sensitive Mobile Devices*, January 2022.



ICE used its MDM system to require that mobile devices have passwords and encryption, auto-lock after a preset time-period, and disconnect from ICE network resources when devices have not been used for a certain time period. ICE also used its MDM system to monitor whether devices' operating systems were up to date. Yet ICE did not effectively manage all its mobile devices using its MDM system. Specifically, as of July 12, 2023, ICE had added 765 ICE-issued mobile devices⁹ to the MDM with fewer security and management controls and less oversight. These devices did not have MTD protection, which ICE OCIO's Security Operations Center (SOC) uses to monitor mobile devices to detect the presence of malicious applications, network-based attacks, improper configurations, and known vulnerabilities. Of note, 65 of the 243 ICE staff permanently stationed overseas (27 percent) had mobile devices that lacked MTD protection and, therefore, were not fully monitored. These staff included high-ranking officials, who were at greater risk of cybersecurity threats while outside the United States.

27% of ICE staff permanently stationed overseas lacked MTD protection on their mobile devices and therefore were not fully monitored.

ICE staff explained that only devices purchased using ICE's centralized mobile device contract vehicle are added to the MDM in a way that allows for MTD protection. ICE allowed some devices to be purchased outside the centralized contract vehicle, but it did not have procedures to ensure these devices were properly monitored by the ICE SOC after being added to the MDM. ICE staff also stated that the component had mission needs for allowing devices to be added to the MDM with less monitoring and protection. ICE could not provide documentation that it had approved allowing devices to be added to the MDM system without MTD protection based on mission needs.

ICE Did Not Identify or Sufficiently Address Vulnerabilities of Web Applications within the Mobile Device Infrastructure

DHS policy¹⁰ requires component OCIOs to perform periodic credentialed vulnerability scans of information systems. Credentialed scans are conducted by users with high-level privileges, such as system administrators, who perform a deeper assessment of the system than what could be achieved through a non-credentialed scan. Components must inform DHS when unable to complete these scans or when vulnerabilities discovered by these scans cannot be addressed in a timely manner.

We found ICE did not perform credentialed vulnerability scans for all web applications installed on the information systems supporting central management of mobile devices. We tested two web applications and identified three high-risk vulnerabilities. Two of these vulnerabilities were not previously known to ICE staff. Although ICE staff identified the third vulnerability in 2020, ICE had

⁹ Our analysis was limited to ICE-issued devices. ICE managed approximately 1,400 additional devices not fully monitored within its MDM system for other DHS components.

¹⁰ DHS 4300A, Attachment O, *Vulnerability Management*, August 2022.



not addressed the vulnerability until after we completed our tests, in May 2023. Further, ICE did not notify DHS of the limitation posed by performing non-credentialed scans.

ICE did not perform credentialed vulnerability scans because the responsible ICE teams did not maintain up-to-date privileged accounts. In addition, ICE was unable to identify the last time it performed a credentialed scan, indicating the teams responsible did not review prior results to ensure they were credentialed. ICE did not notify DHS it had not performed credentialed scans because it lacked a policy or process to do so. Although ICE had a policy to notify DHS of vulnerabilities that cannot be addressed in a timely manner, ICE officials stated that ICE did not follow this policy for the vulnerability identified in 2020.

ICE Did Not Sufficiently Address Vulnerabilities of Mobile Device Infrastructure Servers

DHS policy¹¹ requires components to conduct monthly vulnerability assessments and install information security patches or vulnerability fixes per the timeframe or direction published by the DHS Enterprise SOC.

Although ICE officials stated that ICE conducts monthly vulnerability assessments, the assessments did not identify all vulnerabilities. Moreover, when the assessments identified vulnerabilities, ICE did not install the necessary patches or fixes in a timely manner. We performed vulnerability testing of server assets supporting ICE mobile devices and ICE's MDM and identified one critical and two high-risk vulnerabilities. ICE's vulnerability scans did not identify the one critical vulnerability. Although the scans identified the two high-risk vulnerabilities, ICE had no existing plans to address them.

ICE officials explained they did not identify the critical vulnerability because their monthly vulnerability assessments were mistakenly not scanning the entire system for the server assets. For one of the known vulnerabilities, ICE officials stated that ICE's information technology vendor routinely delayed applicable security updates. ICE did not document this recurring issue because it would eventually be remediated once the next update was released. For the other known vulnerability, ICE officials assumed it had been remediated but were unaware of the process that would have been necessary to fully remediate the vulnerability.

ICE Did Not Properly Address Noncompliant Mobile Device Infrastructure Security Settings

DHS policy¹² requires ICE to follow the DHS CISO's security configuration settings for its information systems. ICE must develop program-level remediation plans when enterprise weaknesses impact multiple systems and submit a risk acceptance request to the DHS CISO when it cannot implement the required settings in a timely manner.

¹¹ DHS 4300A, Attachment O, *Vulnerability Management*, August 2022.

¹² DHS 4300A, *Information Technology System Security Program, Sensitive Systems*, September 2022.



Our examination of ICE’s security configuration settings for its mobile device infrastructure showed that ICE had implemented 225 of the 243 (93 percent) required security settings. ICE had not implemented the remaining 18 required settings. In addition, ICE did not have remediation plans or approved risk acceptance requests, as required, for the settings that were noncompliant.

According to ICE officials, ICE did not create program-level remediation plans to formally address the risk for noncompliant enterprise-level security settings because ICE OCIO leadership directed system teams to address these at the system level. Because this direction deviated from ICE remediation policy and the system team did not have other specific guidance, ICE did not create formal remediation plans to track and timely remediate these weaknesses. Consequently, ICE did not submit a risk acceptance request to the DHS CISO since remediation plans were not formally developed.

ICE Did Not Properly Monitor or Secure Devices Used Outside the United States

ICE did not properly monitor or secure ICE-issued mobile devices that were used outside the United States. Specifically, ICE did not monitor unauthorized network access from foreign locations, and it did not take security precautions for devices used on official international travel.

ICE Did Not Monitor Unauthorized Network Access from Foreign Locations

DHS does not allow any employee or contractor to take their government-issued devices outside of the United States for any personal or official foreign travel unless such use is pre-authorized. Since 2021, DHS¹³ has required components to monitor and block any unauthorized network access attempts from foreign locations and disable unauthorized devices. Components must report their individual monitoring efforts to the DHS Network Operations and Security Center.

We requested foreign connection data from the ICE SOC to determine whether ICE-issued mobile devices were used outside the United States without proper authorization. We were unable to perform a full analysis because the data ICE

ICE did not monitor foreign connections of mobile devices to block unauthorized use.

provided was incomplete and unreliable. We did identify foreign connection data for a limited number of ICE employees and determined that unauthorized use did occur. We also found that ICE did not monitor or block unauthorized foreign connections of mobile devices. While gathering information for this audit, the ICE SOC and ICE Office of Professional Responsibility explained that one of the devices used internationally without prior authorization had connected to an unsecure Wi-Fi network that may have routed communications to a country that poses a high-level

¹³ *Joint DHS Office of the Chief Security Officer and Office of the Chief Information Officer Guidance on Foreign Travel*, August 18, 2021.



cybersecurity threat. The ICE SOC was not aware of the foreign connections we identified before our request for information.

ICE employees were able to use their ICE-issued mobile devices internationally without authorization because the ICE SOC was not aware of the requirement to monitor and block unauthorized foreign use of mobile devices and had no process or procedures in place to do so.

ICE Did Not Take Security Precautions for Devices Used on Official International Travel

DHS policy¹⁴ requires that components take enhanced precautions to address the increased risk inherent with foreign travel when the same devices are used both domestically and internationally. ICE's 2017 international travel policy¹⁵ included steps to update security settings and monitor devices during and after travel.

ICE allows its employees and contractors to use their ICE-issued mobile devices both domestically and internationally during official travel. Approximately 3,300 ICE employees traveled outside the United States during fiscal year 2023. However, ICE did not ensure their devices were adequately protected for use outside the United States. Specifically, ICE did not ensure devices used during overseas travel had the most recent operating system. ICE also did not disable non-essential capabilities or remove unnecessary applications for these devices.

This occurred because ICE stopped using its 2017 international travel policy, which applied mostly to loaner devices no longer used by ICE employees. ICE officials acknowledged that the international travel policy should be updated to align with DHS policy and ICE's practice of using the same mobile devices domestically and internationally.

ICE May Not Have Properly Sanitized Devices for Disposal or Properly Handled Lost and Stolen Mobile Devices

ICE did not effectively implement controls over disposed-of, lost, or stolen ICE-issued mobile devices. Specifically, ICE did not maintain documentation stating that it sanitized all mobile devices before disposal, and the documentation that was available was not always completed properly. In addition, ICE did not ensure incidents of lost or stolen mobile devices were properly addressed.

¹⁴ DHS 4300A, Attachment Q, *International Travel with Mobile Devices*, April 2022.

¹⁵ ICE Standard Operating Procedure, *International Travel with Mobile Devices*, August 2017.



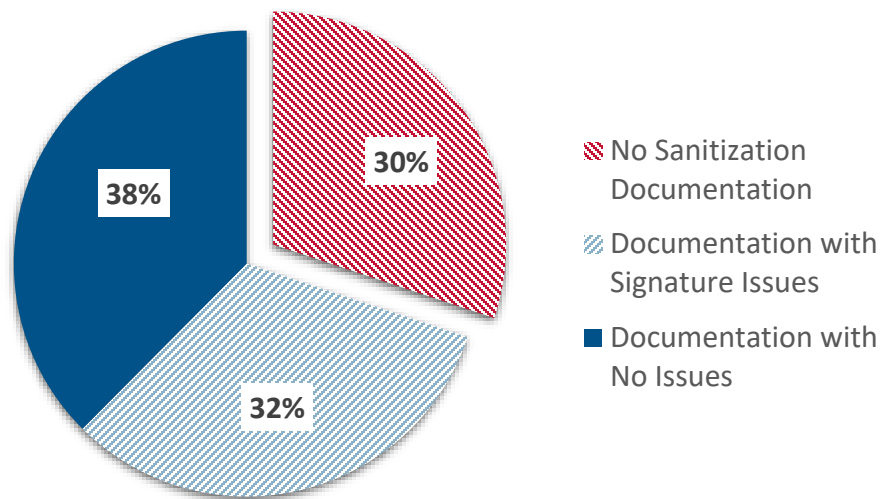
ICE May Not Have Sanitized All Mobile Devices before Disposal

DHS policy¹⁶ and ICE’s standard operating procedures¹⁷ require that all mobile devices be sanitized before they leave ICE’s custody for disposal (i.e., to be reused or destroyed). ICE must also document the sanitization of each device subject to disposal.

More than 5,000 ICE mobile devices may not have been sanitized before disposal.

We found ICE could not provide evidence that it had sanitized all disposed-of mobile devices before the devices left ICE custody. ICE disposed of 20,810 mobile devices between October 2021 and July 2023. We randomly sampled 269 disposed-of devices and reviewed the associated sanitization documentation. ICE had documentation that it sanitized 188 of the 269 selected devices before the devices left ICE custody. However, ICE did not have documentation that it had sanitized the remaining 81 (30 percent) mobile devices, as shown in Figure 4. Based on our sample results, we estimate with 90 percent confidence that between 5,309 and 7,224 out of 20,810 disposed-of ICE mobile devices lacked documentation and therefore may not have been sanitized before leaving ICE custody.¹⁸ Additionally, the documentation for 87 of the 188 mobile devices that were sanitized before disposal was missing signatures or included signatures of ICE staff who potentially did not have the proper authority.

Figure 4. Mobile Devices with and without Evidence of Sanitization



Source: Developed by DHS OIG based on analysis of ICE data

¹⁶ DHS 4300A, *Information Technology System Security Program, Sensitive Systems*, September 2022.

¹⁷ *ICE Media Sanitization IA Program Guidance*, Version 1.3, May 2019.

¹⁸ Our statistical sampling methodology is described in more detail in Appendix A of this report.



This occurred because ICE’s procedures do not clearly outline the roles and responsibilities for sanitizing mobile devices before their disposal. Also, ICE’s standard operating procedures do not provide clear guidance for documenting sanitization when using independent contractors to transport mobile devices for destruction.

ICE Did Not Ensure Incidents of Lost or Stolen Devices Were Properly Addressed

DHS policy¹⁹ classifies lost or stolen mobile devices as security incidents. According to the ICE SOC’s standard operating procedures²⁰ and discussion with ICE OCIO staff, the ICE Service Desk must route incident tickets²¹ for lost or stolen mobile devices to the ICE SOC for elevated security screening and remote wipe of the device.

We found the ICE Service Desk did not route the incident tickets for all lost or stolen mobile devices to the ICE SOC. We reviewed all reports of lost or stolen mobile devices received by the ICE Service Desk from October 2021 through July 2023. Our analysis revealed that the Service Desk did not route 161 of the 569 (28 percent) incident tickets to the ICE SOC for review. Instead, these incident tickets were handled and closed by the Service Desk, and the devices were not wiped.

This occurred because the Service Desk guidance for handling lost, or stolen, device incidents does not align with the ICE SOC procedures or DHS policy. The guidance allows the Service Desk to resolve the lost or stolen incident as a “non-security incident” without routing the information to the ICE SOC if the device user confirms that the lost or stolen mobile device did not contain sensitive information. Although the Service Desk did not route the incident tickets for mobile devices to the ICE SOC in these cases, it did collect device and user information, lock the devices remotely using the MDM, and advise the users to submit an additional lost or stolen report to their supervisor and property custodian.

Conclusion

Due to the issues that we identified, ICE mobile devices and the sensitive information they contain may be at higher risk of unauthorized access and more susceptible to cyberattacks. For example, less secure configurations could result in sensitive data breaches. Also, the vulnerabilities we identified in ICE’s mobile devices and supporting infrastructure could allow an attacker to execute malicious code and compromise ICE systems or gain unauthorized access to sensitive data. If devices are not monitored for foreign connections or not properly prepared for international use, ICE increases the risk that foreign adversaries could intercept ICE communications and that bad actors could gain access to ICE systems and information. Finally, allowing devices to leave ICE

¹⁹ DHS 4300A, Attachment I, *Sensitive Mobile Devices*, January 2022.

²⁰ ICE SOC Standard Operating Procedure, *Checklist: Lost or Stolen*, December 2021.

²¹ ICE uses an internal reporting tool to address all incidents, such as lost or stolen mobile devices. Reported incidents are issued an incident ticket.



custody without being sanitized increases the risk that unauthorized individuals or entities could access sensitive information.

Recommendations

Recommendation 1: We recommend that the ICE Office of the Chief Information Officer implement all necessary mobile device security settings per guidance from DHS and the Defense Information Systems Agency's Security Technology Implementation Guides.

Recommendation 2: We recommend that the ICE Office of the Chief Information Officer develop and implement policies and procedures to ensure source code scans are performed on ICE-developed applications as required.

Recommendation 3: We recommend that the ICE Office of the Chief Information Officer develop and implement policies and procedures to improve the vulnerability management process to ensure:

- credentialed scans are completed and assessed, per DHS guidance;
- limitations posed by non-credentialed scans are properly and promptly reported per DHS guidance;
- plans to address vulnerabilities are created and implemented promptly, per DHS guidance; and
- formal acceptance of, or mitigate the risk of, noncompliant enterprise-level system settings.

Recommendation 4: We recommend that the ICE Office of the Chief Information Officer develop and implement policies and procedures to monitor and block unauthorized network access attempts from mobile devices in foreign locations.

Recommendation 5: We recommend that the ICE Office of the Chief Information Officer revise and implement policies and procedures to protect ICE-issued mobile devices that have been authorized for use on international travel, per DHS and National Institute of Standards and Technology guidance.

Recommendation 6: We recommend that the ICE Office of the Chief Information Officer develop and implement policies and procedures to protect ICE-issued mobile devices used by employees permanently stationed outside the United States.

Recommendation 7: We recommend that the ICE Office of the Chief Information Officer update and implement policies and procedures to ensure mobile devices are sanitized before they are released from ICE custody for disposal.



Recommendation 8: We recommend that the ICE Office of the Chief Information Officer update and implement clear policies and procedures to ensure all lost and stolen mobile devices are treated as security incidents and the associated incident tickets are routed to the ICE Security Operations Center.

Management Comments and OIG Analysis

The Chief Financial Officer and Senior Component Accountable Official for ICE provided written comments on a draft of this audit report, which are included in their entirety in Appendix B. ICE concurred with our eight recommendations. We consider recommendation 3 open and unresolved. We consider recommendations 1, 2, 4, 5, 6, 7, and 8 open and resolved. ICE also submitted technical comments separately, which we addressed as appropriate. A summary of ICE's response and our analysis follows.

ICE Response to Recommendation 1: Concur. In October 2023, ICE OCIO initiated a process to meet DISA STIG guidance for mobile device security settings on the existing mobile infrastructure platform, Unified Endpoint Manager (UEM) 1.0. ICE OCIO plans to deploy an upgrade to UEM 1.0 and add the mobile devices to the new version, UEM 2.0, which includes updates to protect against unauthorized access, hacking, malware infections, and other threats. However, the UEM 2.0 migration depends on the DHS ID project, which is an enterprise identity and derived credential solution necessary for ICE mobile devices. ICE anticipates that the DHS ID project will be completed in December 2024. ICE noted that any delays to the DHS ID project will necessitate changes to timeline for the UEM 2.0 migration. ICE OCIO will subsequently document applicable risk acceptances. Estimated completion date: January 30, 2026.

OIG Analysis: ICE's actions are responsive to this recommendation. This recommendation will remain open and resolved until we receive evidence of ICE's implementation of the proposed actions.

ICE Response to Recommendation 2: Concur. ICE OCIO is implementing a tool to scan the source code of new ICE-developed mobile applications and will also review and update existing software development life cycle processes and procedures to require that the source code of ICE-developed mobile applications be scanned before deployment. Further, ICE OCIO will develop, publish, and enforce standard operating procedures for all internally developed mobile applications. Finally, ICE OCIO will provide additional training to ensure adherence to established processes and requirements for performing source code scans. Estimated completion date: June 30, 2025.

OIG Analysis: ICE's actions are responsive to this recommendation. This recommendation will remain open and resolved until we receive evidence of ICE's implementation of the proposed actions.



ICE Response to Recommendation 3: Concur. Per DHS Policy Directive 4300A, ICE OCIO maintains standard operating procedures for implementing compliance and vulnerability scanning and vulnerability management of all assets and applications within the ICE environment. ICE OCIO provides scan results to DHS in accordance with DHS Policy Directive 4300A and develops Plans of Action and Milestones in accordance with DHS Policy Directive 4300A Attachment H. On April 3, 2024, ICE OCIO implemented quality control testing to identify instances in which Plans of Action and Milestones were not generated or managed in accordance with DHS policy. Further, ICE OCIO will implement enhanced training to ensure continuous monitoring and vulnerability management procedures are followed for all systems and technologies. ICE OCIO is also developing a Risk Acceptance Memorandum for overdue Plans of Action and Milestones for mobile infrastructure assets for which credentialed scans cannot be completed. Estimated completion date: June 30, 2025.

OIG Analysis: ICE's actions are partially responsive to this recommendation. This recommendation will remain open and unresolved until ICE provides a corrective action plan that addresses enhanced processes to ensure credentialed scans are completed and noncompliant enterprise-level system risks are addressed.

ICE Response to Recommendation 4: Concur. ICE OCIO is updating and developing ICE standards and procedures to monitor and block unauthorized network access attempts from mobile devices in foreign locations that will align with DHS Policy Directive 4300A Attachment I. ICE clarified that ICE OCIO's solution to block unauthorized network access attempts from mobile devices in foreign locations is contingent on the upgrade and deployment of the UEM 2.0 and a mobile security tool, which will allow ICE OCIO to observe, monitor, and block traffic on mobile devices. As noted in ICE's response to Recommendation 1, DHS anticipates completing a modernization of the enterprise identity and derived credential solution by the end of December 2024. As new and existing devices are enrolled in UEM 2.0, additional capabilities will be deployed allowing the component to better monitor and block unauthorized network access attempts in foreign locations. Estimated completion date: January 30, 2026.

OIG Analysis: ICE's actions are responsive to this recommendation. This recommendation will remain open and resolved until we receive evidence of ICE's implementation of the proposed actions.

ICE Response to Recommendation 5: Concur. ICE OCIO is updating and developing standards, processes, and procedures for ICE mobile devices authorized for use while on international travel, which will align with DHS Policy Directive 4300A Attachment I and National Institute of Standards and Technology Special Publication 800-124 Rev. 2. ICE OCIO's solution to provide additional protections for devices that are authorized for international travel is also contingent on the UEM 2.0 upgrade. As devices are enrolled in UEM 2.0, additional capabilities will be deployed allowing ICE to better monitor and protect mobile devices authorized for international travel. ICE OCIO will



subsequently document applicable risk acceptances. Estimated completion date: January 30, 2026.

OIG Analysis: ICE's actions are responsive to this recommendation. This recommendation will remain open and resolved until we receive evidence of ICE's implementation of the proposed actions.

ICE Response to Recommendation 6: Concur. ICE OCIO is updating and developing standards and procedures to address mobile devices ICE issues to employees permanently stationed overseas that will align with DHS Policy Directive 4300A Attachment I. However, ICE OCIO's solution to provide additional protections for devices that are permanently stationed outside the United States is contingent on the upgrade and deployment of UEM 2.0, the mobile security tool discussed in ICE's response to Recommendation 4, and DHS ID. As devices are enrolled in UEM 2.0, additional capabilities will be deployed allowing ICE to better monitor and protect mobile devices permanently stationed outside the United States. ICE OCIO will subsequently document applicable risk acceptances. Estimated Completion Date: January 30, 2026.

OIG Analysis: ICE's actions are responsive to this recommendation. This recommendation will remain open and resolved until we receive evidence of ICE's implementation of the proposed actions.

ICE Response to Recommendation 7: Concur. ICE OCIO will update ICE media sanitization standards to explicitly include mobile device sanitization requirements and will also update associated procedures and processes for destruction and disposal to align with DHS Policy Directive 4300A and ICE property management practices, as appropriate. Estimated completion date: June 30, 2025.

OIG Analysis: ICE's actions are responsive to this recommendation. This recommendation will remain open and resolved until we receive evidence of ICE's implementation of the proposed actions.

ICE Response to Recommendation 8: Concur. ICE OCIO is updating policies and procedures to require that lost and stolen mobile devices be treated as security incidents and will also update the existing ticketing workflow for lost and stolen devices to route tickets to the SOC for incident handling. ICE OCIO will further review SOC incident response procedures to incorporate updated procedures for handling lost or stolen mobile devices, as appropriate. Estimated completion date: June 30, 2025.

OIG Analysis: ICE's actions are responsive to this recommendation. This recommendation will remain open and resolved until we receive evidence of ICE's implementation of the proposed actions.



Appendix A: Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107–296) by amendment to the *Inspector General Act of 1978*.

The objective of this audit was to determine the extent to which ICE manages and secures its mobile devices. For this audit, we defined mobile devices as smartphones and tablets. To answer our objective, we limited our audit scope to ICE’s processes related to:

- mobile device and mobile device infrastructure security settings;
- vulnerability management of the mobile device infrastructure and applications;
- international use and oversight of mobile devices;
- incidents of lost or stolen devices; and
- sanitization of disposed-of devices.

To gain an understanding of how ICE manages and secures its mobile devices, we interviewed selected ICE officials from OCIO, the Office of Asset and Facilities Management, the Homeland Security Investigations International Operations Division, and the Office of Professional Responsibility. We also reviewed relevant prior audit reports and congressional activities related to mobile devices. We reviewed Federal laws, Department directives, and ICE policies and procedures related to the management and security of mobile devices.

To determine the number of mobile devices ICE manages, we reviewed inventories of all mobile devices from ICE’s MDM system. We compared the reports to our observations from virtual walkthroughs and determined the reports accurately represented the devices within the MDM system.

To determine if ICE used adequate security settings on its mobile devices, we requested the security configuration baseline for ICE-issued mobile devices. ICE did not have a security configuration baseline but instead provided screenshots of security settings pushed to mobile devices by its MDM system as of March 2023. We compared ICE settings to the required DISA STIG guidelines applicable to ICE-issued devices. We also reviewed a limited number of physical devices while under ICE supervision.

As part of this audit, we coordinated with the DHS OIG Office of Innovation’s Cybersecurity Risk Assessment division, which provided technical support for this audit. The Cybersecurity Risk Assessment division performed software-based vulnerability patch and configuration management assessments based on DISA STIGs. The Cybersecurity Risk Assessment division also conducted dynamic application security testing assessments of ICE’s MDM web applications.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Additionally, the Cybersecurity Risk Assessment division performed static application security scans of ICE's custom-developed mobile applications. ICE provided comments on the test results. When vulnerabilities were identified, we met with ICE staff to determine root causes and requested documentation on any prior ICE efforts to address the vulnerabilities identified.

To determine the extent ICE monitors and blocks unauthorized foreign connections from mobile devices used outside the United States, we planned to compare the Internet Protocol addresses and geolocation data of mobile devices against travel voucher records of authorized ICE travel during FY 2023. We determined the foreign mobile device data was incomplete and not reliable to quantify the number of devices used outside the United States without proper authorization. However, we were able to identify personal use of devices outside the United States when we reviewed specific device connections and contacted a limited number of employees to verify their use of mobile devices. We also met with ICE's Office of Professional Responsibility regarding possible device use in a country that poses a high-level cybersecurity threat. We also reviewed ICE policies, travel forms, and checklists and interviewed officials to determine the extent ICE secures mobile devices authorized for use outside the United States. We compared travel dates, international connections, and ICE MDM information to identify mobile devices used outside the United States with outdated operating systems.

To determine if ICE properly responded to instances of lost and stolen mobile devices, we requested all lost and stolen reports from ICE's incident ticketing system created between October 2021 and July 2023. We also reviewed all other types of equipment that were reported lost or stolen during that time to ensure we identified any lost and stolen mobile devices that may have been incorrectly classified as a different type of equipment. We adjusted our testing to ensure we reviewed all mobile devices reported lost or stolen. We also met with ICE staff and watched the incident tracking system generate reports. We determined the information we received was sufficient and reliable for our testing purposes. We then reviewed all cases of reported lost and stolen devices to determine the extent incident tickets were routed to the ICE SOC.

To determine if ICE properly sanitized devices before disposal, we obtained a data extract from ICE's asset management system and identified all mobile devices disposed of between October 2021 and July 2023. In coordination with the DHS OIG Office of Innovation's Data Services Division, we worked with ICE to determine if the data was sufficiently reliable and to ensure the system data was properly extracted and accurately identified mobile devices within the asset management system. We also coordinated with ICE property management personnel to accurately identify devices that had been disposed of within the system. From a population of 20,810 mobile devices, with 90 percent confidence, 5 percent sampling error, and 50 percent population proportion, we drew a statistically valid sample size of 269 ICE mobile devices reportedly disposed of between October 2021 and July 2023. We requested sanitization records for all devices within our sample, reviewed the records for completeness and accuracy, and projected the results across the entire universe of the 20,810 disposed-of devices.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Before completing this audit, we issued a management alert related to unauthorized or banned mobile applications installed on ICE-managed devices. We discussed the status of the recommendations with ICE and DHS staff and included the updated status in this report.

We assessed internal controls related to how ICE manages its mobile devices. The internal control deficiencies we found are discussed in the Results of Audit section of this report. 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 our audit.

We conducted this audit from February 2023 through July 2024 pursuant to the *Inspector General Act of 1978*, 5 United States Code §§ 401–424, 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.

DHS OIG’s Access to DHS Information

During this audit, ICE denied the OIG’s request for direct access to the Sunflower Asset Management System and to Operational Reports in the Concur Travel Management System. ICE agreed to provide data extracts, but the initial extracts we received were incomplete, causing additional delays.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix B: ICE Comments on the Draft Report

Office of the Chief Financial Officer

U.S. Department of Homeland Security
500 12th Street, SW
Washington, D.C. 20536




U.S. Immigration
and Customs
Enforcement

BY ELECTRONIC SUBMISSION

September 18, 2024

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

FROM:  **FOR**
Jennifer Cleary
Chief Financial Officer and
Senior Component Accountable Official
U.S. Immigration and Customs Enforcement

SUBJECT: Management Response to Draft Report: “ICE Did Not
Always Manage and Secure Mobile Devices to Prevent
Unauthorized Access to Sensitive Information”
(Project No. 23-017-AUD-ICE)

Thank you for the opportunity to comment on this draft report. U.S. Immigration and Customs Enforcement (ICE) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

ICE leadership is pleased to note OIG’s recognition that ICE increases workforce mobility and productivity by issuing personnel and contractors mobile devices (e.g., smartphones and tablets) to help them perform duties related to enforcing Federal laws governing border control, customs, trade, and immigration. ICE remains committed to strengthening controls that safeguard sensitive information stored and processed on ICE-managed Government Furnished Equipment (GFE) mobile devices located domestically and abroad.

However, leadership disagrees with OIG draft report allegation that ICE “denied” access to the Sunflower Asset Management System (SAMS) and the Concur Travel Management System (Concur), and that data extracts provided were incomplete because this characterization is misleading and lacks important context. For example, the draft report does not mention that granting the OIG’s request for direct access to SAMS would

www.ice.gov



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

provide access to *all* DHS Component data, not just data relevant to the scope and objectives of this audit. Instead, ICE provided OIG SAMS data extracts using the exact parameters requested by OIG, such as the extract provided on April 5, 2023, for active and retired smartphones since 2017. In addition, ICE worked with DHS SAMS Business Support on April 6, 2023, to provide the OIG a comprehensive list of all official names of assets (such as smartphone, computer tablet, telephone, communication device, etc.) available in Sunflower so the OIG could select the exact ones they wanted included in the report. Following OIG's selection, ICE provided the requested information on April 26, 2023. OIG then requested a report showing every change made to each mobile device record in SAMS. However, this was not an available reporting option. To address the request in a format agreed to by OIG auditors, ICE subsequently provided OIG with screenshots of records on May 17, 2023, showing: (1) the history and timeline of the records requested; (2) explanations of each transaction on the record; and (3) a screenshot of the parameters used in the report.

It is also important to note that the OIG never requested any walkthroughs or live interactions of records in SAMS with ICE personnel, nor did OIG communicate any questions or concerns with the information provided by ICE until July 5, 2023—about 1 ½ months later. Even at this point, OIG only noted that some data was truncated when exported from SAMS and requested an updated extract by July 12, 2023. ICE addressed this timely, and ran the updated report on July 6, 2023, however, due to OIG requesting the information be uploaded to a secure filesharing platform—which required ICE to verify with IT security teams whether this was permissible—the report was not uploaded to the OIG's platform until July 11, 2023, which was still a day earlier than OIG's requested due date. Following this, OIG reached out again on August 23, August 24, and September 6, 2023, to request clarification on some of the reporting related to the disposal of ICE mobile devices. Clarification was provided on August 24, August 28, and September 7, 2023, respectively. OIG also contacted ICE on September 22, 2023, requesting Media Sanitization Forms for 269 SAMS records with a deadline of October 6, 2023. On September 25, 2023, ICE requested, and OIG granted an extension with a due date of October 13, 2023. ICE provided the requested documents on that date.

Regarding OIG's July 28, 2023, request for direct access to ICE's instance of the Concur Operational Reports and Intelligence module in the National Travel Services, ICE was unable to grant access because doing so would enable the OIG to potentially manipulate live data. However, on August 25, 2023, ICE did grant Traveler Auditor Roles to the OIG providing "View Only" access. On August 31, 2023, ICE requested from system owners the parameters of the required population of traveler reports needed for the OIG to complete their audit, and this information was provided to OIG on October 3, 2023. Further, after a meeting to discuss this information on October 14, 2023, OIG requested an updated report, which was submitted to OIG on October 23, 2023.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

The draft report contained eight recommendations with which ICE concurs. Attached find our detailed response to each recommendation. ICE previously submitted technical comments addressing several accuracies, contextual, and other issues under a separate cover for OIG's consideration, as appropriate.

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.

Attachment



**Attachment: Management Response to Recommendations
Contained in OIG 23-017-AUD-ICE**

OIG recommended the ICE Office of the Chief Information Officer (OCIO):

Recommendation 1: Implement all necessary mobile device security settings per guidance from DHS and the Defense Information System Agency’s Security Technology Implementation Guides [STIG].

Response: Concur. Beginning in October 2023, ICE OCIO initiated a process to meet Defense Information System Agency STIG guidance for mobile device security settings on the existing mobile infrastructure platform, Unified Endpoint Manager (UEM) 1.0. ICE OCIO is currently implementing a phased migration of existing mobile devices to UEM 2.0, which is “hardened” against unauthorized access, hacking, malware infections, and other threats, and will facilitate increased STIG compliance. However, it is important to note that the UEM 2.0 migration of existing users is dependent on the DHS ID project, which is an enterprise derived credentials solution necessary for ICE mobile devices that is currently anticipated to be completed in December 2024. Delays to the DHS ID project will necessitate changes to ECD based upon the contingent timelines. Once this modernization of the enterprise identity and derived credential solution is complete, ICE OCIO will take the following actions:

Action	Estimated Completion Date (ECD)
Test and deploy ICE UEM 2.0.	March 31, 2025
Deploy newly issued mobile devices to UEM 2.0.	April 30, 2025
Migrate existing mobile devices to ICE UEM 2.0.	December 31, 2025
Document, via risk acceptance, configuration settings that cannot be enabled without operational impacts.	January 30, 2026

Overall ECD: January 30, 2026.

Recommendation 2: Develop and implement policies and procedures to ensure source code scans are performed on ICE-developed applications as required.

Response: Concur. ICE OCIO is implementing a tool to perform source code scanning of new ICE-developed mobile applications, and will also review and update existing Software Development Life Cycle processes and procedures to require the performance of source code scans of ICE-developed mobile applications prior to production. Further, ICE OCIO will develop and publish Standard Operating Procedures (SOP)—and enforce mandatory use of the procedures outlined in the SOP—for all internally developed



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

mobile applications deployed into production. Finally, ICE OCIO will provide additional training to ensure adherence to established processes and requirements for performance of source code scanning. ECD: June 30, 2025.

Recommendation 3: Develop and implement policies and procedures to improve the vulnerability management process to ensure:

- credentialed scans are completed and assessed, per DHS guidance;
- limitations posed by non-credentialed scans are properly and promptly reported, per DHS guidance;
- plans to address vulnerabilities are created and implemented promptly, per DHS guidance; and
- formal acceptance of, or mitigate the risk of, noncompliant enterprise-level system settings.

Response: Concur. In accordance with DHS Policy Directive 4300A,¹ ICE OCIO maintains SOPs for implementing compliance and vulnerability scanning and vulnerability management of all assets and applications within the ICE environment. ICE OCIO provides scan results to DHS in accordance with DHS Policy Directive 4300A, and develops Plan of Action and Milestones (POA&Ms) in accordance with DHS Policy Directive 4300A Attachment H.² On April 03, 2024, ICE OCIO implemented quality control testing to identify instances where POA&Ms were not generated or managed in accordance with DHS policy. Further, ICE OCIO will implement enhanced training to ensure continuous monitoring and vulnerability management procedures are followed for all systems and technologies, and is also developing a Risk Acceptance Memo for overdue POA&Ms for mobile infrastructure assets in which credentialed scans cannot be completed. ECD: June 30, 2025.

Recommendation 4: Develop and implement policies and procedures to monitor and block unauthorized network access attempts from mobile devices in foreign locations.

Response: Concur. ICE OCIO is currently updating and developing ICE standards and procedures to monitor and block unauthorized network access attempts from mobile

¹ DHS Policy Directive 4300A, "Information Technology System Security Program, Sensitive Systems," dated February 13, 2023; https://www.dhs.gov/sites/default/files/2023-05/V2.508%20Working%20file_DHS_4300A%20ITSSP%20SS%20Policy%20Directive%20FINAL%202023.02.13_kwb.pdf

² DHS Policy Directive 4300A Attachment H "Plan of Action and Milestone (POA&M) Guide," Version 3.1, dated February 6, 2024; https://www.dhs.gov/sites/default/files/2023-06/4300A_ITSSP_SS_Attachment_H_Plan_of_Action_and_Milestone_%28POAM%29_Guide.pdf



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

devices in foreign locations that will align with DHS Policy Directive 4300A Attachment I.³

It is important to clarify that ICE OCIO’s solution to block unauthorized network access attempts from mobile devices in foreign locations is contingent upon the upgrade and deployment of the UEM infrastructure version 2.0 and a mobile security tool, which will allow ICE OCIO to observe, monitor and block traffic on mobile devices. As previously noted, DHS anticipates completing a modernization of the enterprise identity and derived credential solution by the end of December 2024. As new and existing devices are enrolled in the new ICE UEM 2.0 infrastructure, additional capabilities will be deployed allowing the agency to better monitor and block unauthorized network access attempts in foreign locations. Specific actions for this effort are as follows:

Action	ECD
Test and deploy ICE UEM 2.0.	March 31, 2025
Deploy newly issued mobile devices to UEM 2.0.	April 30, 2025
Migrate existing mobile devices to ICE UEM 2.0.	December 31, 2025
Deploy additional capabilities to ICE UEM 2.0 for monitoring and blocking unauthorized network access attempts.	January 30, 2026

Overall ECD: January 30, 2026.

Recommendation 5: Revise and implement policies and procedures to protect ICE-issued mobile devices that have been authorized for use on international travel, per DHS and National Institute of Standards and Technology [NIST] guidance.

Response: Concur. ICE OCIO is currently updating and developing ICE standards, processes, and procedures for GFE mobile devices authorized for use while on international travel, which will align with DHS Policy Directive 4300A Attachment I and NIST Special Publication 800-124 Rev. 2.⁴ As the upgrade and deployment of the UEM infrastructure version 2.0 and the mobile security tool previously discussed in this letter will allow ICE OCIO to observe, monitor and better protect mobile devices, ICE OCIO’s solution to provide additional protections for devices that are authorized for international travel is also contingent upon the effort to modernize the enterprise identity and derived credential solution. As devices are enrolled in the new ICE UEM 2.0 infrastructure

³ DHS Policy Directive 4300A Attachment I, “Information Technology System Security Program, Sensitive Systems: Sensitive Mobile Devices,” dated January 22, 2022; <https://www.dhs.gov/sites/default/files/2023-06/4300A%20ITSSP%20SS%20Attachment%20I%20Sensitive%20Mobile%20Devices.pdf>”

⁴ NIST Special Publication 800-124 Rev. 2 “Guidelines for Managing the Security of Mobile Devices in the Enterprise,” dated May 2023; <https://csrc.nist.gov/pubs/sp/800/124/r2/final>



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

additional capabilities will be deployed allowing the agency to better monitor and protect mobile devices authorized for international travel.

Action	ECD
Test and deploy ICE UEM 2.0.	March 31, 2025
Deploy newly issued mobile devices to UEM 2.0.	April 30, 2025
Migrate existing mobile devices to ICE UEM 2.0.	December 31, 2025
Document, via risk acceptance, configuration settings that cannot be enabled without operational impacts.	January 30, 2026

ECD: January 30, 2026.

Recommendation 6: Develop and implement policies and procedures to protect ICE-issued mobile devices used by employees permanently stationed outside the United States.

Response: Concur. ICE OCIO is currently updating and developing ICE standards and procedures to address GFE mobile devices issued to employees permanently stationed overseas that will align with DHS Policy Directive 4300A Attachment I. However, ICE OCIO's solution to provide additional protections for devices that are permanently stationed outside the United States is contingent upon the upgrade and deployment of the UEM infrastructure version 2.0 and the mobile security tool referenced previously discussed in this letter, as well as the DHS modernization of the enterprise identity and derived credential solution. As devices are enrolled in the new ICE UEM 2.0 infrastructure additional capabilities will be deployed allowing the agency to better monitor and protect mobile devices permanently stationed outside the United States.

Action	ECD
Test and deploy ICE UEM 2.0.	March 31, 2025
Deploy newly issued mobile devices to UEM 2.0.	April 30, 2025
Migrate existing mobile devices to ICE UEM 2.0.	December 31, 2025
Document, via risk acceptance, configuration settings that cannot be enabled without operational impacts.	January 30, 2026

ECD: January 30, 2026.

Recommendation 7: Update and implement policies and procedures to ensure mobile devices are sanitized before they are released from ICE custody for disposal.

Response: Concur. ICE OCIO will update ICE media sanitization standards to explicitly include mobile device sanitization requirements, and will also update associated procedures and processes for destruction and disposal processes to ensure



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

alignment with DHS Policy Directive 4300A and ICE property management practices, as appropriate. ECD: June 30, 2025.

Recommendation 8: Update and implement clear policies and procedures to ensure all lost and stolen mobile devices are treated as security incidents and the associated incident tickets are routed to the ICE Security Operations Center [SOC].

Response: Concur. ICE OCIO is currently updating policies and procedures to require lost and stolen mobile devices be treated as security incidents, and will also update the existing ticketing workflow for lost and stolen devices to route tickets to the SOC for incident handling. ICE OCIO will further review SOC incident response procedures to incorporate updated procedures for handling lost or stolen mobile devices, as appropriate. ECD: June 30, 2025.



Appendix C: 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
ICE Component Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov



DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

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