NATIONAL ARCHIVES

OFFICE *of the* CHIEF RECORDS OFFICER

Portable Electronic Devices

Assessment Report

National Archives and Records Administration
January 13, 2023

INTRODUCTION

The National Archives and Records Administration (NARA), based on authority granted by 44 United States Code (U.S.C.) 2904(c), is responsible for assessing the proper management of records in all media within federal agencies to protect rights, assure government accountability, and preserve and make available records of enduring value. Under this authority, NARA conducts records management (RM) oversight of federal agencies, including agency inspections, electronic system audits, and assessments.

An assessment is a multi-agency evaluation of a specific topic, issue, or activity affecting RM processes, procedures, or policies to identify agency risks and challenges, as well as any leading practices that can be shared throughout the federal RM community.

In the third quarter of FY 2022, NARA conducted an assessment of five agencies' policies, practices, and procedures related to the use of portable electronic devices (PEDs), with a focus on evaluating how agencies ensure the proper management of federal records on or accessed by these devices. This report synthesizes NARA's analysis of the information gathered during the assessment.

Assessment Scope

This assessment evaluated each participating agency's policies, practices, procedures, and information technology (IT) tools used to manage government-furnished and personally-owned smartphones, tablets, and laptops for agency business, with a particular emphasis on the management of federal records created, stored or accessed by these devices.

Assessment Methodology

During the assessment, agencies responded to a pre-assessment questionnaire, provided documentation relevant to the scope of the assessment, and participated in interviews. NARA's assessment questions and documentation review focused on the PED program, device, and RM.

TOPIC DISCUSSION

Portable Electronic Devices

According to the Office of Personnel Management's Status of Telework in the Federal Government Report to Congress Fiscal Year 2020,

> … agencies used telework as a strategic management tool to enhance their capability to achieve critical outcomes during an unprecedented time. Where

> appropriate, agencies throughout the Federal Government expanded telework to the maximum extent possible to protect the health and safety of the Federal workforce and the American people. Indeed, 90 percent of eligible Federal employees participated in telework—a significant increase compared to previous years.

The expansion of telework during the COVID-19 pandemic has exponentially increased the need for and usage of PEDs across the federal government, and it is highly probable that agencies' reliance on these devices to conduct business will not decrease.

Federal agencies must create and maintain authentic, reliable, and usable records and ensure they remain in place for the length of their authorized retention period (36 CFR 1220.32). Additionally, federal agencies must establish reference and retrieval procedures and controls that ensure that access to electronic records minimizes the risk of unauthorized deletions or removal of federal records (36 CFR 1222.34 (d)(2)). These two regulations must be primary considerations for all agencies as the reliance on PEDs continue to grow and as technology and remote work alters the way we perform RM.

To effectively ensure that PED usage complies with all federal RM regulations, agencies must evaluate how government-furnished, and personally-owned devices create, access, store and manage federal records. This evaluation must include not only word processing documents, but also text and instant messages, email, photographs, videos, and audio recordings made or received on a PED while conducting agency business.

Furthermore, PEDs often connect to enterprise-wide networks, systems, and applications to support data exchange and storage via remote interactions. This requires agencies to establish specific RM controls that can mitigate potential risks associated with PEDs accessing these networks, systems, and applications from locations that are outside of an agency’s physical control.

Potential Risk Factors

Based on the assessment interviews, the following list highlights some of the most common risk factors associated with PED usage that has an impact on proper records management.

- Improper storage of agency data/records in locations outside of the agency's control.
- Ineffective segregation of federal and personal activities when agencies permit the use of personally-owned devices or do not restrict what users can do on government-furnished devices.

- Non-capture of text/instant messages, photographs, videos, or audio recordings from the local storage on devices.

To further ensure that the use of PEDs complies with federal RM regulations, agencies should be mindful of these common RM risk factors, as several of them have direct or indirect impacts on an agency's ability to maintain control of electronic records.

Unauthorized Disposition

According to 36 CFR 1230, federal agencies are required to promptly report to NARA any actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records within an agency's custody, otherwise known as an unauthorized disposition (UD) of agency records.

NARA manages the UD process and has encountered several cases associated with PEDs. Most of these UD cases were tied to an agency's inability to capture (or verify the capture) of federal records from smartphones and tablets. Often this was due to not having correct passwords to gain access into those devices, or because departing employees intentionally reset/wiped devices before returning them to agency IT services.

Other PED-related UD cases involved:

- Lost/stolen/unreturned laptops that potentially had federal records stored on the device's local hard drive;
- Unintentional resetting or wiping of cellphones;
- Inability to detect or prevent the intentional unauthorized removal of federal records from recordkeeping systems by remote interactions;
- Ineffective use of audit logs to track user interactions in recordkeeping systems;
- Failure to adequately backup information systems; and
- Not limiting what applications employees can download and use on government-furnished devices, which allowed employees to engage in unauthorized electronic communications.

SUMMARY AND ANALYSIS

All participating agencies provided approved personnel, including contractors, with laptops and smartphones. Four agencies also issued tablets. Agencies furnish staff with either Android or Apple smartphones and tablets and primarily issue laptops that use Microsoft Windows; only one agency issued a small number of Apple laptops. Four agencies approved the use of personally-

owned devices to conduct agency business and access enterprise-wide networks, systems, and applications.

All agencies routinely disseminate policies and specific guidance to govern PED usage and inform PED users of their recordkeeping responsibilities as it pertains to these devices. Also, each agency, in varying ways, uses IT software applications to manage the dissemination, deployment, and use of government-furnished devices, as well as to manage how approved personally-owned devices access and interact with agency networks, systems, and applications.

Overall, NARA found that even though each agency had specific policies and guidance outlining the appropriate use of PEDs, most agencies do not have processes that significantly ensure the consistent capture and preservation of federal records for the lifecycle of the PED or PED-associated records. (See Appendix B for a table summarizing participating agencies' responses to the pre-assessment questionnaire).

KEY POINTS

Agency Documentation

Each agency provided copies of its policies, directives, and training materials related to PED usage and RM. In summary, every agency had policies that specifically outlined the appropriate use of government-furnished and personally-owned devices, two agencies had a mobile device management (MDM) policy, four agencies had a specific policy regarding IT system security, four agencies provided RM policies, and three agencies had guidance that discussed frequently asked questions (FAQ) or rules of behavior for PED usage and use of IT networks and systems. Only one agency submitted training materials that discussed IT security of mobile devices and general RM.

During assessment interviews, agency representatives were asked how these policies are transmitted to staff and how often. Most agencies indicated that staff are typically first introduced to these policies when onboarded and that all agency policies reside on agency intranets for staff to access as needed. When policies are newly drafted or revised, agencies distribute them via email. Some agencies indicated that staff who were issued government-furnished devices or were approved to use personally-owned devices, or have access to IT systems and networks, are required to annually review and sign forms that summarize agency policies and rules of behavior for using IT assets.

All participating agencies pointed out that they primarily rely on agency RM policies and annual RM training to promote how records associated with PEDs should be managed. PED users are responsible for managing and safeguarding records and information created or received on these

devices, and ensuring that all federal records are retained and managed within the appropriate agency recordkeeping systems.

Findings and Recommendations

Although agencies issued policies that discuss the roles, responsibilities, and even some processes relied on to govern the usage of PEDs, many policies did not substantially address the relationships that exist between IT networks and systems, PEDs, agency records and RM. In other words, most of the reviewed documentation offered limited guidance that explicitly connected PEDs to the management of records while using these devices.

Additionally, most agencies do not have effective mechanisms in place to assess whether or not PED users consistently adhered to agency policies, guidance and training. If agencies expect PED users to manually transfer records from these devices to recordkeeping systems, agencies should develop and implement procedures and processes that consistently assess and validate user compliance. Distributing written policies does not equate to compliance with said policies.

To increase compliance with RM regulations, as it pertains to PEDs, there should be consistent and strong collaboration between IT and RM programs to ensure that policies being created do not simply address recordkeeping requirements and RM regulations in a vacuum, but within the context of PED functionalities, IT systems and network access, administrator and user rights, overall user behaviors and the ever-changing realities agencies are facing with remote work environments.

Agencies should also:

- Determine the best format of policy transmission for different audiences.
- Employ multiple mechanisms that frequently communicate policy mandates.
- Ensure the policies being created are executable for all program offices and agency personnel.
- Disseminate reference tools of policy mandates to ensure accessibility and execution of behaviors that comply with policy requirements.
- Set annual deadlines for policy guidance to be acknowledged by PED users.
- Determine methods to measure staff understanding of policy guidelines and behaviors users must practice.
- Develop and implement processes that periodically assess and validate user compliance with recordkeeping requirements related to PEDs.
- Develop and implement strategies to mitigate user non-compliance.

NARA Guidance and RM Regulations

NARA does not have specific guidance that speaks directly to the implications PEDs pose when managing federal records. Consequently, findings varied as to how each agency specifically addressed the management of records associated with PEDs.

Most agencies expressed that rapid changes in technology forces them to lead the charge in investigating and acquiring new tools to meet business demands, and ever-evolving work environments, with little time and resources left to fully consider the implications these new technologies create when trying to meet RM regulations. Furthermore, agency representatives felt that NARA does not issue specific enough guidance that keeps up with the technological advancements agencies are facing, Agencies indicated that much of NARA's guidance seems entrenched in a paper records management paradigm.

Findings and Recommendations

Agencies want NARA to provide specific "how-to" strategies and "thou-shalt" guidance. Most agencies expressed frustration with NARA guidance because agency records officers often get pushback from senior leadership who cite that NARA's guidance reads as recommendations that are optional rather than mandatory. The ultimate consequence is that agency RM programs do not get senior leadership buy-in to acquire sufficient resources to meet the demands of technology and even to establish policies and practices that would promote better RM. One agency stated that NARA should drive the ship and take the lead in creating a path for agencies to follow.

Agencies also asked for specific guidance on WhatsApp, Microsoft 365 and cloud-related technologies. One agency felt that NARA should engage with cloud service providers to develop standard features that would ensure compliance with federal RM regulations. Another agency suggested that NARA find ways to encourage agencies to collaborate more on issues related to emerging technologies and RM.

Mobile Device Management

MDM refers to a set of functions and features that control the use of PEDs in compliance with organizational policies. These functions include the management of software applications, device inventory, policy, security, and services for PEDs.

All five agencies reported varying levels of use of MDM tools for both government-furnished and personally-owned devices. Most of the agencies used MDM to apply IT administration rules, monitor, manage, and troubleshoot security controls, apply data and device encryption and block

or allow permission to specific devices, applications and systems, authenticate passwords, remotely wipe lost or stolen devices and manage physical IT assets.

Findings and Recommendations

NARA found that the volume of devices, availability of financial resources, the nature of agency business, as well as the level of collaboration between RM and IT departments were determining factors of how MDM tools are being used at each agency. Some agencies are able to capitalize on several different MDM features and others simply use it to manage the lifecycle of devices. Additionally, most of the agencies used MDM primarily for smartphones and tablets, while only a few agencies employed MDM features on laptops.

The growing use of PEDs presents agencies with a number of things to consider to ensure sufficient capture, storage and retention of federal records. For example, agencies should consider the risks associated with allowing users to store records locally on PEDs or allowing remote access to agency recordkeeping systems and applications from personally-owned devices.

MDM tools have features that can control how records are stored and accessed on both government-furnished and personally-owned devices. There are features that can segregate agency data from personal data, prevent data from being stored locally on the device, and even remotely capture and wipe agency data without removing personal data. All agencies should consider what MDM features could enhance the agency's ability to consistently retain control over federal records associated with each type of device.

Tablets, Smartphones and Laptops

Table 1 illustrates the number of PEDs issued by participating agencies before and after the COVID-19 pandemic.

Table 1. Number of Government-Issued PEDs pre- and post-COVID-19

	Agency 1	Agency 2	Agency 3	Agency 4	Agency 5
Pre	Laptops: **15,934** Smartphones: **770** Tablets: **309** Portable drives: **799**	**20** Smartphones, tablets, & laptops	**500** Smartphones, tablets, & laptops	**935** Smartphones & laptops	Laptops: **1741** Smartphones: **456** Tablets: **48**

	Agency 1	Agency 2	Agency 3	Agency 4	Agency 5
Post	Laptops: **15,142** Smartphones: **757** Tablets: **278** Portable drives: **792**	**34** Smartphones, tablets, & laptops	**3000** Smartphones, tablets, & laptops	**973** Smartphones & laptops	Laptops: **3748** Smartphones: **998** Tablets: **79**

Government-issued Devices

Across all agencies, smartphones are more commonly issued than tablets and smartphones, and tablets are only issued to small subsets of agency personnel. For example, one agency only issued smartphones to supervisory staff and tablets were only issued to senior agency officials. One agency reported that only about 25% of staff were issued smartphones and another agency only had 5% of staff with government-issued smartphones.

One agency reported that they advise against using government-issued phones for text messaging, three agencies advise staff to forward any text message that rises to the definition of a federal record to their agency email, and one agency uses a mobile communication archiving application, Telemessage, to automatically forward all text messages, sent or received, on a government-issued smartphone to the users' agency email account.

Most agencies restricted what applications could be downloaded on a government-issued device, placing restrictions on specific social media and electronic messaging applications like Wickr, Signal, and WhatsApp. Only one agency did not restrict what applications users could download but utilized MDM features to monitor downloaded applications and had the capability to remove non-compliant applications from devices without user involvement.

Due to the nature of one agency's business, certain government-issued devices are allowed to use WhatsApp to facilitate communication during international travel. This agency expressed a need for specific guidance and training from NARA on how to manage records associated with WhatsApp.

Device applications such as video and audio recording and electronic messaging can present capture and retention issues when records created by these applications are not transferred to agency recordkeeping systems by users or an automated process.

One agency reported that it does use MDM tools to automatically ingest all electronic files created on agency-issued laptops into agency network drives. All other agencies lack automated capture processes, and do not have auditing processes in place to ensure that users consistently transfer any type of electronic record from a PED to an agency recordkeeping system.

Overall, most agencies have implemented different IT security controls to provide protection against alteration, loss or disclosure of government information and have specific procedures in place to report lost or stolen devices, as well as processes to protect information when agency personnel do not retain custody of a device.

Finally, all agencies rely heavily on written policies to inform users of their federal recordkeeping responsibilities as it relates to these devices and most agencies required staff to manually transfer photos or videos to an agency recordkeeping system when necessary, and asserted that any word-processed documents should only be stored and accessed through an agency cloud-based application or in an agency recordkeeping system.

Personally-owned Devices

All agencies allowed varying levels of access to agency systems and applications from personally-owned PEDs. Two agencies allowed personally-owned devices to access agency email applications only, where one agency allowed access through the service provider's mobile app, and the other agency only allowed access through the service provider's website, where access would only be for a specified duration to ensure that users could not indefinitely remain logged in. All agencies had written policies and guidance to communicate user responsibilities and the appropriate use of personally-owned devices when conducting agency business.

Three agencies required staff to obtain permission, sign documentation and download a data management application in order to use personally-owned devices for agency business. These applications create a segregated environment on the devices, often referred to as "the container." The container is installed on the user's personal device and provides an enabled password or personal identification number (PIN), data encryption and a segregated government operating space for authorized functions. Data in the container is isolated from the user's personal data and device applications, allowing the agency to apply configurations to the container, primarily for security reasons. Those agencies that allow personally-owned devices restricted senior officials from using any personally-owned device.

Although two agencies reported that they do not allow the use of personal laptops for conducting business, NARA found that these agencies did not actually have mechanisms in place to prevent personnel from using personal smartphones, tablets or laptops from gaining access to the agency email and cloud-based environments. Functionalities with access had some limitations, but as it relates to RM, users were not restricted from downloading agency information to local storage on personally-owned devices.

Findings and Recommendations

Both government-issued and personally-owned PEDs provide users with easy access to agency IT networks and systems and require users to adhere to security protocols such as device encryption, download and storage restrictions, access application requirements, and remote wiping.

Most agencies reported that upon notification of an incident, IT programs could remove data remotely by wiping compromised government-issued devices. This security measure ensures that agency networks, systems and records can no longer be accessed from missing devices by unauthorized users. However, once PEDs are wiped, some agencies cannot recover data, especially data stored on the device locally.

Remotely wiping lost and stolen devices can lead to unauthorized disposition of agency records if PED users had not adequately transferred records to official recordkeeping systems prior to security incidents. To mitigate this risk agencies should consider using IT rules that restrict users from storing information on local hard drives or IT applications that automatically, in real-time, capture records from PEDs and transfer them to agency's recordkeeping systems, or implementing processes, manual or automated, that consistently audit devices for federal records.

For example, one agency indicated that it has the capability to remotely reset devices and capture information prior to wiping data. Another agency used MDM tools to ingest all electronic information created and saved on local device storage into Microsoft 365 and also reported that wiping devices does not compromise any electronic records because of the required use of "the container."

While agencies are able to place tighter controls on government-issued devices via MDM solutions, sub-optimal use of MDM functionalities can increase risks of unauthorized disposition of federal records. Additionally, even though agencies provide specific guidance reminding users of their responsibilities to manually transfer records to agency recordkeeping systems, agencies should consider developing and implementing processes that can validate whether or not records created or accessed by a PED are being consistently captured by device users.

Agency RM and IT Program Collaboration

Two agencies reported that due to their small size, there are several instances of direct and frequent communication between programs regarding the development, vetting and adoption of new policies and IT investments. Other agencies expressed that their IT and RM programs collaborate infrequently or only as needed, mostly during the onboarding and offboarding of high-level agency personnel, application of records schedules within IT systems, and during development and issuance of PED policies and guidance.

One agency's RM program described its collaboration with IT to prioritize the capture of records from devices of senior officials during offboarding. The agency records officer meets with senior officials to review exit clearance checklists and offboarding procedures and consults with IT to ensure that records on the senior official's devices are accounted for and captured within the appropriate recordkeeping systems before the senior official leaves the agency.

Findings and Recommendations

It is customary for many agencies to engage in more hands-on and direct exit procedures for senior officials and not apply those exit procedures for other types of agency personnel Agencies typically expect non-senior level staff to manually download and transfer records from their devices into approved systems without verification before they leave.

RM programs should have more involvement during the issuance and receipt of PEDs to establish users' understanding of RM responsibilities and device functionalities and to ensure that records on PED devices are appropriately captured when returned.

IT programs are primarily tasked with IT asset procurement, issuance, management, security, and receipt of PEDs and do not typically focus on RM. RM programs need to support IT programs during all stages of the PED lifecycle and should collaboratively assess device functionalities and develop solutions to ensure better control and management of PED-related records.

Additionally, IT programs should aim to eliminate as many manual processes as possible to avoid the liabilities of human error and non-compliance with RM regulations. Agencies should consider enterprise information archiving solutions that can automate manual tasks with a complete audit trail, full metadata, and immutability, and also seek out customizable solutions that give IT administrators the ability to precisely control and define collection parameters and retention policies for electronic records.

BEST PRACTICES

Throughout this report several best practices and recommendations were noted for agencies to consider, below are a few others.

Agency Documentation

One agency's policy for "*Use and Monitoring of Agency Office and Information Technology Equipment and Resources"* listed potential consequences for not safeguarding agency records on PEDs. Agency policies are steeped in regulatory and esoteric language that sometimes make them inaccessible to users or too vague to correlate to day-to-day staff practices.

Reminding staff of consequences can help staff understand how non-compliance with policy guidelines can directly affect the agency and themselves. For instance:

- If non-public information is saved to a personal laptop or mobile device, and that device is stolen or shared with an unauthorized person via the remote IT environment, the agency would no longer have control of the electronic records stored on the device.
- If that information contains PII, the agency may have to notify every individual whose information is contained in the electronic records about the breach and may have to offer them credit monitoring services.
- Responsible offices will bear the cost of any breach from their budget.
- If the agency receives a FOIA request covering these electronic records (those stored only on your personal devices), it may be difficult to retrieve and provide these electronic records to a requester.
- If these documents are considered confidential or part of the agency's deliberative process, the agency's ability to maintain legal privilege is dependent on the agency having complete control of the electronic records and being able to promise that no one else has seen them. If, for example, electronic records are left on a hotel computer, the agency may not be able to maintain a legal privilege.
- If you share your personal computing devices with other members of your family, other family members may load file-sharing software on your computer, making these electronic records publicly available without your knowledge.
- If you maintain agency records on your personal device, and these records become relevant to litigation, the agency may need to access your entire personal device, and you may no longer have the right to claim personal privacy.

Another best practice, pertaining to agency documentation, is the use of FAQs. One agency periodically distributes FAQs via agency email. Similar to the list of consequences, providing responses to frequently asked questions based on NARA policy and agency guidance can promote compliance when handling agency records and information.

Additionally, requiring PED users to annually review and sign user agreements is an effective way to check user understanding and to reiterate user responsibilities. Agencies should ensure

that user agreements offer contextual and specific guidance that help connect PED usage to the proper management of records while using these devices.

Device Process Automation

One agency's use of a mobile communication archiving application addresses the potential for not capturing text messages. Use of the application automates the retention process, requiring no action from device users. This ensures that electronic messages sent or received on the device are captured and preserved in the appropriate recordkeeping system.

CONCLUSION

Even though NARA does not have targeted regulations or specific guidance for PEDs, federal agencies must create and maintain authentic, reliable, and usable records and ensure preservation of these records for their entire retention period (36 CFR 1220.32). Additionally, federal agencies must establish processes and controls that ensure access to electronic records and minimize the risk of unauthorized additions, deletions, or alterations to federal records (36 CFR 1222.34 (d)(2)).

These two regulations require agencies to assess how well users of PEDs are managing federal records created, stored or accessed by the device. Agencies need to also evaluate the efficacy of employee execution and adherence to IT, PED and RM policies, guidance, and training, and make meaningful modifications to these resources.

Finally, agencies need to measure the effectiveness of manual processes for capturing electronic records from PEDs. If manual processes are not effective, agencies must develop solutions to ensure all federal records are being properly managed. As agencies allow more employees to work remotely, IT and RM programs should consider dedicating more resources to IT solutions that automate records retention for all PEDs.

APPENDIX A

List of Participating Agencies

1. United States Patent and Trademark Office, Department of Commerce
2. Office of the Secretary, Department of the Interior
3. Millennium Challenge Corporation
4. Corporate Records Management, National Archives and Records Administration
5. Occupational Safety and Health Review Commission

APPENDIX B

Table 2. Summary of Pre-assessment Questionnaire Responses

Questions	Summary of agencies' responses
Which offices are involved in the deployment and receipt of PEDs? (example - IT, security, etc)	Office of Administrative Services, Office of Executive Director, IT, Office of Chief Information Officer
Does your agency issue PEDs to all employees or by specific positions?	Yes- all employees. No- PEDs are issued for all staff for telework purposes and select Administrative staff are issued phones. Yes- prior to COVID no, now the agency provides laptops to all employees. No- supervisors approve employee requests. PEDs are based on need based on duties. No- Position specific.
Does your agency issue PEDs to contractors?	Yes Yes- if requested for telework (laptops) Yes- as needed Yes Yes- position specific
What portable devices are issued by the agency:	
Laptops	All agencies answered yes
Tablets	Four agencies answered yes
Smartphones	All agencies answered yes
Other Device(s)	Three agencies answered yes, of them one listed mobile hotspots as requested and approved
Do you use third-party applications that are used to create federal records to conduct federal business (i.e. WhatsApp, Wickr, Signal)?	Blackberry App (iPhones) & MS Exchange Yes- MS Office & Google Suite No Yes No- only native SMS and MS Teams Chat are used on PEDs
If yes, does your agency have tools to capture records from the applications?	Three agencies answered yes
If yes, please identify the tool(s).	Blackberry App (iPhones) MS Exchange ZLUA captures email and files Telemessage on mobile phones The agency trains and provides guidance that all records must be sent to an official email account w/n 20 days and stored on an approved SOR.
Does your agency have a	All agencies answered yes

Questions	Summary of agencies' responses
solution(s) in place to manage mobile/portable devices? If yes, what are they?	ITIL ServiceNow is used for Asset Management. Partial solution from Meraki - Mobile Device Management (free up to 20 devices) Google Suite MDM for mobile device management MaaS360 to manage portable devices MaaS360 is the mobile device management solution for iOS and Android Operating System smartphones and tablets, and Active Directory to manage laptops.
Please list and submit policies.	All agencies submitted policies, see Appendix C for details.
Do you allow employees to "bring your own device" (BYOD)?	Four agencies answered yes.
If yes, do you have a policy (please attach)?	All four agencies provided a policy.
Does your agency require training on how to manage records using PEDs?	Four agencies answered yes.
If not, is the management of records using PEDs included in any non-required training?	One agency responded that it is included in agency policy
How many devices were issued prior to the Covid pandemic?	Four agencies issued less devices prior to COVID, see page 10 for details.
How many devices are issued presently?	One agency had a minor decrease in the number of issued devices Two agencies had increased the number of issued devices by ~ 125% Two agencies had increased the number of issued devices by ~ 4%
Were there changes made to PED policies due to the COVID pandemic?	Only one agencies responded yes

APPENDIX C

Table 3. Summary of agency documentation

Agency 1	Agency 2	Agency 3	Agency 4	Agency 5
Enterprise Mobile Device Management Mandatory Use	Personal Use of Government Office Equipment	Telework	Cybersecurity Newsletter	Office of Chief Information Officer Rules of the Road
Mandatory Deployment of Agency Enterprise System for All Bureaus and Offices	Records Management	Computer and Information System Security	IT Policy FAQ	Information Governance and Records Management
Use of Personally-Owned SmartPhones and Tablets for Official Government Business	Corporation Information System Security Policy	Rules of Behavior for Agency Network Use/Access	Use and Monitoring of Agency Office and Information Technology Equipment and Resources	Limited Personal Use of Government Equipment
Records Management Policy - Preserving Text and Instant Messages as Federal Records	Mobile Device Use Policy	Use of Personally-owned Devices	Information Technology Systems Security	FAQ on the Appropriate Handling of Information during COVID-19 Mandatory Telework Status
		Use of Government Equipment	Interim Guidance Managing Electronic Messages	Appropriate Use of Agency Information and Resources
				Mobile Device Management
				Information Security Foreign Travel
				Safeguarding Agency Assets
				Agency Information

Agency 1	Agency 2	Agency 3	Agency 4	Agency 5
				Technology Guardrails
				Social Media
				Records Management 101 Training
				IT Security Awareness Training

APPENDIX D

Table 4. List of additional resources

Title	Source
Managing Records in Mobile Environments: Addressing Records Management Implications	National Archives Records Express Blog
Mobile Lifecycle & Expense Management User Guide	General Services Administration
Guidelines for Managing the Security of Mobile Devices in the Enterprise	National Institute of Standards and Technology
FAQ about Telework	National Archives Records Administration
Enterprise Mobility: The Centralized Source of Governmentwide Mobile Solutions	General Services Administration
Wireless Mobility Solutions	General Services Administration
Mobile Application Playbook	Department of Homeland Security


NATIONAL
ARCHIVES
OFFICE of the
CHIEF RECORDS
OFFICER