

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**TABLE OF CONTENTS**

<b>Topics</b>	<b>Sections</b>
<a href="#"><u><b>OVERVIEW</b></u></a>	3.1 What is the purpose of this chapter? 3.2 What is the scope of this chapter? 3.3 What are the objectives of this chapter? 3.4 What are the authorities for this chapter? 3.5 What terms do you need to know to understand this chapter?
<a href="#"><u><b>RESPONSIBILITIES</b></u></a>	3.6 Who is responsible for mobile device management and security? 3.7 What requirements must employees meet to have and keep a Government-furnished mobile device?
<a href="#"><u><b>MANAGING MOBILE DEVICES AND THE MOBILE DEVICE MANAGEMENT (MDM) SYSTEM</b></u></a>	3.8 What is the process for registering a mobile device in the Department-approved MDM system? 3.9 How often do mobile device users have to access the MDM system?
<a href="#"><u><b>SECURING AND MANAGING MOBILE DEVICES</b></u></a>	3.10 What mobile devices are employees authorized to use? 3.11 What are the security requirements for mobile devices, mobile device operating systems, and mobile applications? 3.12 What might happen if an employee doesn't comply with the security or other requirements for a Service-issued mobile device? 3.13 What must employees do if they lose a mobile device or it is stolen? 3.14 What are the requirements for international travel with mobile devices?
<a href="#"><u><b>THE SERVICE WIRELESS NETWORK AND MOBILE DEVICES</b></u></a>	3.15 How does the Service secure its wireless network while providing for mobile device access?
<a href="#"><u><b>ELECTRONICALLY STORED INFORMATION (ESI) ON MOBILE DEVICES</b></u></a>	3.16 How is sensitive Government data protected when using a mobile device? 3.17 What are the requirements for storing and backing up ESI on mobile devices? 3.18 What are the requirements for removing ESI from mobile devices when the devices are retired?
<a href="#"><u><b>PRIVACY AND MOBILE DEVICES</b></u></a>	3.19 What are the expectations for privacy while using Government-furnished mobile devices?

**OVERVIEW**

**3.1 What is the purpose of this chapter?** This chapter:

**A.** Establishes the U.S. Fish and Wildlife Service's (Service) policy and procedures to secure and manage its Government-furnished mobile devices, associated systems and networks, and

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 272 Telecommunications**

**Chapter 3 Managing and Securing Government-Furnished Mobile Devices 272 FW 3**

Electronically Stored Information (ESI) in accordance with Department of the Interior (Department) and Federal guidelines; and

**B.** Requires that all Government-furnished mobile devices be registered in the Department-approved Mobile Device Management (MDM) system.

**3.2 What is the scope of this chapter?**

**A.** This policy applies to all Service employees, volunteers, and contractors who:

**(1)** Are authorized to use Service-provided mobile devices (i.e., smartphones and tablets) for official Service business and to access Departmental and Service resources, information, and data via the Service wireless network using those devices; and

**(2)** Plan, manage, and secure the Service's mobile devices and related networks and systems.

**B.** This policy does not apply to:

**(1)** Devices that run using a fully-fledged computer operating system (such as Windows Enterprise, Windows Professional, etc.), including rugged laptops. Such devices must comply with the requirements associated with computer workstations;

**(2)** Devices other than smartphones and tablets that are generally considered "mobile," such as Global Positioning System (GPS) units and smart watches, that employees cannot register and track using the MDM system;

**(3)** Personal (not Government-furnished) mobile devices. Employees must not conduct official business on personal mobile devices; and

**(4)** Mobile devices that Office of Law Enforcement (OLE) officials use for dedicated law enforcement functions, such as undercover operations or technical support. OLE retains full administrative control of these devices, which are not:

**(a)** Connected to any Service network,

**(b)** Associated with the MDM system, or

**(c)** Subject to MDM protocols.

**3.3 What are the objectives of this chapter?** Our objectives are to:

**A.** Explain how to implement the Department's MDM system, and

**B.** Ensure employees are following security and management requirements related to:

**(1)** Government-furnished mobile devices (including the physical device, device operating system, and applications downloaded on the device),

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 272 Telecommunications**

**Chapter 3 Managing and Securing Government-Furnished Mobile Devices**

**272 FW 3**

- (2) The Service wireless network (including remote access technology), and
- (3) ESI on Government-furnished mobile devices.

**3.4 What are the authorities for this chapter?**

- A. [Department of the Interior Security Control Standard: Access Control, September 2016.](#)
- B. [Department of the Interior Office of the Chief Information Officer \(OCIO\) Directive 2016-005; Enterprise Mobile Device Management \(MDM\) Mandatory Use; November 7, 2016.](#)
- C. [Department of the Interior OCIO Directive 2013-003; Security Requirements for International Travelers and the Use of Electronics on International Travel; September 30, 2013.](#)
- D. [Executive Order 13589, Promoting Efficient Spending; November 9, 2011.](#)
- E. Federal Information Security Management Act of 2002 (FISMA) ([Public Law 107-347, Title III](#)).
- F. Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), [Division E \(Public Law 104-106\)](#).
- G. [Office of Management and Budget \(OMB\) Circular A-130, Managing Federal Information as a Strategic Resource.](#)
- H. [OMB Memorandum M-16-20; Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services; August 4, 2016.](#)
- I. [410 Departmental Manual \(DM\) 2, Limited Personal Use of Government Office Equipment and Library Collections.](#)

**3.5 What terms do you need to know to understand this chapter?**

- A. Cloud computing.** A model for enabling convenient, on-demand network access to a shared pool of computing resources (e.g., networks, servers, applications, services). Users can have access to cloud computing services with minimal management effort or service provider interaction. For more information about cloud computing, employees should read the [National Institute of Standards and Technology's \(NIST\) Special Publication 800-145, \*The NIST Definition of Cloud Computing\*](#).
- B. Electronic Discovery (eDiscovery).** The process of collecting, preparing, reviewing, and producing ESI.
- C. Electronically Stored Information (ESI).** Any information that is created, received, maintained, or stored on mobile devices. Examples include, but are not limited to, email,

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 272 Telecommunications**

**Chapter 3 Managing and Securing Government-Furnished Mobile Devices 272 FW 3**

calendars, word processing documents, spreadsheets, databases, videos, video files, digital images, text messages, voicemails, and activity logs. ESI includes metadata.

**D. Government-furnished mobile device.** A smartphone or tablet that the Service provides to an employee to accomplish certain business purposes. See [NIST SP 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise](#) for a full listing of all characteristics of a mobile device.

**E. Limited personal use.** Activity that an employee conducts for purposes other than accomplishing official or otherwise authorized activities. Such use must not adversely affect the employee's job performance, must be of negligible cost, and must be limited to those situations where the Government is already providing equipment or services.

**F. Mobile Device Management (MDM).** Refers to any routine or tools that distribute applications, data, and configuration settings to mobile devices. MDM comprises a range of potential software and hardware solutions designed to optimize the functionality and security of mobile computing devices and networks, while minimizing costs and downtime.

**G. Mobile Device Management (MDM) system.** A software solution that the Service uses to help perform MDM functions, such as deploying devices and applications, creating an inventory of Service devices, ensuring that devices are up-to-date with the latest security patches/operating systems, and more.

**H. Sensitive data or Personally Identifiable Information (PII).** Includes, but is not limited to:

(1) Information that someone could use to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. This includes a name, Social Security number, date and place of birth, mother's maiden name, account number, license number, or any other type of information created specifically to identify or authenticate. PII, if improperly disclosed, can be used to steal an individual's identity, violate the individual's right to privacy, or otherwise harm the individual.

(2) Organizational information that is not in the public domain and if improperly disclosed might cause a significant or severe degradation in mission capability or result in significant or major damage to organizational assets; major financial loss; or significant, severe, or catastrophic harm to individuals.

## RESPONSIBILITIES

**3.6 Who is responsible for mobile device management and security?** See Table 3-1.

**Table 3-1: Responsibilities for Mobile Device Management**

These employees...	Are responsible for...
<b>A. The Director</b>	Approving or declining to approve Servicewide policy for mobile devices.

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

These employees...	Are responsible for...
<p><b>B. Assistant Chief Information Officer (ACIO) for the Service, i.e., the Assistant Director - Information Resources and Technology Management (IRTM)</b></p>	<p>(1) Ensuring compliance with this policy through electronic reviews, automated tools, and other means as necessary;</p> <p>(2) Approving or declining to approve updates to this policy and any associated guidelines;</p> <p>(3) Designating the Service's Mobile Devices Operations Manager (MDOM);</p> <p>(4) Issuing requirements regarding which mobile devices Service managers can purchase based on the security requirements in this chapter; and</p> <p>(5) Responding to security risks to Service information on Government-furnished mobile devices and associated networks by establishing additional security measures, as necessary.</p>
<p><b>C. Chief, IRTM, Branch of Enterprise Services and Operations</b></p>	<p>(1) Implementing and maintaining enterprise level processes for securing and managing mobile devices;</p> <p>(2) Providing direction to the MDOM and Chief Technology Officers (CTO) to help them implement mobile device security policies and manage mobile devices; and</p> <p>(3) Implementing solutions for employees to securely access the Service wireless network from mobile devices with the assistance of the Associate Chief Information Security Officer.</p>
<p><b>D. Associate Chief Information Security Officer (ACISO)</b></p>	<p>(1) Serving as the point of contact for all cybersecurity concerns for mobile devices;</p> <p>(2) Working with the Department's OCIO to:</p> <ul style="list-style-type: none"> <li>(a) Evaluate and assess mobile devices and ensure compliance with Departmental baseline requirements, and</li> <li>(b) Review and provide guidance on the security vulnerabilities presented by updated mobile device operating systems;</li> </ul> <p>(3) Helping to implement Departmental guidance regarding what features are needed on mobile devices; and</p> <p>(4) Advising the ACIO about the security risks associated with supporting a particular mobile device model.</p>

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 272 Telecommunications**

**Chapter 3 Managing and Securing Government-Furnished Mobile Devices**

**272 FW 3**

These employees...	Are responsible for...
<p><b>E. Mobile Devices Operations Manager (MDOM)</b></p>	<p><b>(1)</b> Serving as the primary liaison between the Department and the Service for matters related to MDM;</p> <p><b>(2)</b> Serving as the point of contact for major mobile device issues within the Service;</p> <p><b>(3)</b> Keeping this chapter up-to-date and making policy recommendations to the ACIO;</p> <p><b>(4)</b> Advising the ACIO on which mobile devices the Service should support;</p> <p><b>(5)</b> Developing and maintaining a Help Desk process for mobile issues with the assistance of CTOs;</p> <p><b>(6)</b> Overseeing Service implementation of the Department's MDM system;</p> <p><b>(7)</b> Ensuring that:</p> <ul style="list-style-type: none"> <li><b>(a)</b> Employees use the practices in Departmental Security Technical Implementation Guides and other guidance related to mobile device security and the MDM system,</li> <li><b>(b)</b> Devices registered in the MDM system can meet the Department's baseline security requirements and removing those devices that cannot comply, and</li> <li><b>(c)</b> Lost or stolen devices are properly wiped and secured in conjunction with Regional/Headquarters (HQ) Help Desk personnel and Regional/HQ MDM Administrators;</li> </ul> <p><b>(8)</b> Working with mobile device users to remove applications that pose security risks or that are unauthorized;</p> <p><b>(9)</b> Approving or declining to approve waivers for the requirements in this policy in consultation with the Chief, IRTM Branch of Enterprise Services and Operations and the ACISO; and</p> <p><b>(10)</b> Publishing guidance on mobile device security and a list of approved mobile devices on the Service's <a href="#">MDM SharePoint site</a>.</p>

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 272 Telecommunications**

**Chapter 3 Managing and Securing Government-Furnished Mobile Devices**

**272 FW 3**

These employees...	Are responsible for...
<p><b>F. Regional Chief Technology Officers (CTO) (the Service's National CTO in IRTM is the CTO for HQ)</b></p>	<p>(1) Ensuring all mobile devices issued to Service employees comply with Departmental and Service policies;</p> <p>(2) Ensuring that employees are aware of:</p> <p style="padding-left: 40px;">(a) The requirement to register their Government-furnished mobile devices in the MDM system, and</p> <p style="padding-left: 40px;">(b) The other mobile device security requirements in this policy;</p> <p>(3) Coordinating with HQ IRTM Security personnel, as necessary, to evaluate the security risks posed by mobile applications prior to approving them for purchase;</p> <p>(4) Working with managers/supervisors to ensure that employees are aware of requirements to upgrade devices to meet Departmental baseline requirements;</p> <p>(5) Coordinating with managers/supervisors to resolve issues related to inappropriate use of mobile devices and networks;</p> <p>(6) Implementing Help Desk processes for mobile devices in coordination with the MDOM; and</p> <p>(7) Sanitizing mobile devices that may be compromised by international travel or other forms of cyber intrusion.</p>
<p><b>G. Regional/HQ MDM Administrators</b></p>	<p>(1) Ensuring that mobile devices are enrolled in the Department-mandated MDM system;</p> <p>(2) Retiring devices and wiping data from the Department's MDM system;</p> <p>(3) Supporting the MDOM to ensure employees are following Departmental and Service requirements (e.g., limited personal use policy, Security Technical Implementation Guides, patches);</p> <p>(4) Helping the MDOM to secure lost or stolen devices in conjunction with Help Desk personnel;</p> <p>(5) Ensuring that only authorized devices are connected to the Service wireless network;</p> <p>(6) Performing remotely executed corrective actions for devices that are not in compliance with policy or that pose a security risk; and</p>

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

These employees...	Are responsible for...
	<p>(7) Assisting Help Desk employees with resolving mobile device-related issues.</p>
<p><b>H. Managers/ Supervisors</b></p>	<p>(1) Determining employees' need for a device;</p> <p>(2) Ensuring employees follow mobile device use policies and that their agreements and Rules of Behavior documents are on file;</p> <p>(3) Monitoring employee compliance with relevant mobile device guidelines, including registration of the device in the MDM system;</p> <p>(4) Using monthly wireless/data communications billing to re-evaluate the continuing need for a device and discover indications of potential inappropriate use; and</p> <p>(5) Working with program, IRTM, and Office of the Solicitor staff to help ensure paper and electronic records are accessible for eDiscovery purposes.</p>
<p><b>I. Employees who are mobile device users</b></p>	<p>(1) Using Government-furnished mobile devices according to this policy (also see <a href="#">section 3.7</a>);</p> <p>(2) Ensuring that the device is enrolled in the MDM system upon receipt;</p> <p>(3) Becoming familiar with the guidelines and practices we describe on the <a href="#">MDM SharePoint site</a>;</p> <p>(4) Complying with security guidelines as directed by MDM personnel;</p> <p>(5) Ensuring their Government-furnished device is secured at all times and refraining from attempting to alter or disable mobile device configurations and security settings without prior authorization;</p> <p>(6) Notifying their Help Desk before and after international travel and following international travel security procedures, e.g., trips to some countries require IRTM to wipe the device before you use it again on the network (also see <a href="#">section 3.14</a>);</p> <p>(7) Immediately reporting suspected security incidents, privacy incidents, and loss or destruction of Federal records by following Service incident response procedures;</p>

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

These employees...	Are responsible for...
	<p><b>(8)</b> If a device is lost or stolen, notifying their supervisor, filing a report within 24 hours, and following the policy in this chapter and in Exhibit 1, Instructions for Lost and Stolen Mobile Devices;</p> <p><b>(9)</b> Whenever possible, connecting to a trusted wireless network to use devices to avoid data overages and additional costs for the Service;</p> <p><b>(10)</b> Removing any installed application that the MDM requires them to remove; and</p> <p><b>(11)</b> Upgrading the device as directed by MDM personnel, the ACIO, and Departmental guidance.</p>

**3.7 What requirements must employees meet to have and keep a Government-furnished mobile device?**

**A.** Employees who are authorized to use Government-furnished mobile devices must follow mobile device management guidelines.

**(1)** Employees must complete [FWS Form 3-2235, Non-Disclosure Agreement \(NDA\)](#), and the [Department’s Rules of Behavior \(ROB\) Form](#) before they’re assigned the device.

**(2)** Employees must read and follow Departmental policy on limited personal use of Government-furnished equipment in [410 DM 2, Limited Personal Use of Government Office Equipment and Library Collections](#), and on telephone use. IRTM has a list of the Department’s telephone use policy and guidelines on its [intranet site](#).

**(3)** Employees must comply with the requirements and limits established by their device’s associated wireless service contract.

**B.** The Service issues Government-furnished mobile devices to employees to assist in accomplishing its mission and to meet specific business needs. As a result, employees must use them primarily to conduct official Service business and not as a substitute for a personal mobile device. We recognize that employees may want to use Government-furnished devices for personal reasons during non-duty time or while on official travel (e.g., to contact family members or check the weather, traffic, or news). Such use is allowed if:

**(1)** Employees follow the Department’s Rules of Behavior and refrain from using their Government-furnished mobile devices for activities that are illegal or inappropriate as described in [410 DM 2](#) and [5 CFR 2635, Standards of Ethical Conduct for Employees of the Executive Branch](#);

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 272 Telecommunications**

**Chapter 3 Managing and Securing Government-Furnished Mobile Devices 272 FW 3**

(2) It meets the requirements for limited personal use, as we describe in [section 3.7A\(2\)](#), which means that use:

(a) Does not affect the performance of official duties by the employee or the employee's organization,

(b) Is of reasonable duration and frequency, and

(c) Creates no additional cost for the Service (such as through data overages); and

(3) Mobile applications and other files downloaded to the devices meet all applicable security requirements (see [section 3.11](#)). Employees should consult with their Regional/HQ CTO before downloading and installing any mobile application.

## **MANAGING MOBILE DEVICES AND THE MDM SYSTEM**

### **3.8 What is the process for registering a mobile device in the Department-approved MDM system?**

**A.** Within 72 hours of being issued a mobile device, employees must register it in the Department's MDM system. This allows the Service to manage the devices effectively and to optimize their functionality and security.

**B.** Employees should contact the Help Desk for assistance in registering their devices. You can also find details of how to register your device using the information in the [New Device Setup & Configuration](#) library on the MDM SharePoint site.

### **3.9 How often do mobile device users have to access the MDM system?**

**A.** To avoid paying for unused mobile devices, we must remove inactive devices from the MDM system after they have been inactive for more than 60 days. Because of this, mobile device users must connect to the MDM system at least once a month.

**B.** There are two exceptions to this requirement:

(1) Devices used infrequently for mission-critical requirements, such as for law enforcement or emergencies, are tracked and inventoried separately from other mobile devices; and

(2) Devices that IRTM owns and uses to replace lost or damaged devices or as loaner devices for international travel (see [section 3.14](#) for more information) are updated and tracked separately.

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 272 Telecommunications**

**Chapter 3 Managing and Securing Government-Furnished Mobile Devices**

**272 FW 3**

## **SECURING AND MANAGING MOBILE DEVICES**

### **3.10 What mobile devices are employees authorized to use?**

**A.** IRTM publishes a list of authorized and recommended mobile devices on the Service's [MDM SharePoint site](#).

**B.** The devices on this list are the only ones that employees may use to connect to the Service wireless network and to functions like BisonConnect and the intranet. The devices must meet Federal and Departmental security and management requirements (see [section 3.11](#)).

**C.** IRTM will update the list of supported devices in accordance with new Departmental, manufacturer, or wireless service carrier guidance.

**D.** To manage which mobile devices are issued to employees, Service MDM personnel must:

**(1)** Evaluate which devices the Service can no longer support to ensure that the devices we buy have a reasonable service life, and

**(2)** Retire devices that are no longer able to meet the Department's baseline requirements.

### **3.11 What are the security requirements for mobile devices, mobile device operating systems, and mobile applications?**

**A.** Employees must handle devices in accordance with applicable Federal laws, regulations, and standards, including Departmental security guidelines and policies. These include NIST standards and checklists governing the use of mobile devices, such as:

**(1)** [NIST SP 800-53 Revision 4 \(or current version\), Security and Privacy Controls for Federal Information Systems and Organizations, April 2013](#); and

**(2)** [NIST SP 800-124 Revision 1 \(or current version\), Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013](#).

**B.** We must remove devices from the MDM system that cannot meet the approved device configuration baseline. IRTM monitors the operating system of every mobile device and notifies the employee if the device does not meet the configuration baseline. Employees who are assigned devices that cannot support the baseline operating system must contact their supervisors to begin the process of replacing the devices.

**C.** Employees must ensure that their devices are running on the appropriate operating systems.

**(1)** Employees must not update their mobile devices' operating systems to the next full operating system version (e.g., version 11 to version 12), even if prompted, without the authorization of MDM personnel.

**(2)** They may complete incremental updates (e.g., version 11.1 to 11.2) at their discretion.

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 272 Telecommunications**

**Chapter 3 Managing and Securing Government-Furnished Mobile Devices**

**272 FW 3**

(3) IRTM will issue communications on upgrading operating systems when necessary.

D. Employees must not download or install mobile applications that pose a security risk to the Service. MDM personnel will block applications that they or other IRTM Security personnel determine may pose a security risk.

(1) Before committing funds to purchase a new mobile application, employees must seek approval from their supervisor and Regional/HQ CTO.

(2) The Regional/HQ CTO will consult with IRTM Security personnel as necessary to ensure that the application meets security requirements before approving it for purchase.

**3.12 What might happen if an employee doesn't comply with the security or other requirements for a Service-issued mobile device?** If an employee doesn't comply with the security or other requirements we describe in [sections 3.10](#) and [3.11](#) above, the Regional/HQ CTO or Service MDM personnel will notify the employee and his/her supervisor that the employee is not in compliance. If the non-compliance continues, Service MDM personnel may remove the device from the MDM system and issue a selective wipe of corporate data from it.

**3.13 What must employees do if they lose a mobile device or it is stolen?** Employees must report a lost or stolen device to their supervisor, Regional/HQ CTO, and Help Desk within 24 hours of the event. Employees can find detailed procedures for reporting a lost or stolen device in Exhibit 1, Instructions for Lost and Stolen Devices.

**3.14 What are the requirements for international travel with mobile devices?**

A. At least 3 weeks before they plan to travel internationally, employees must take [IRTM's International Travel Survey](#) if they want to take a Government-furnished device. The International Travel Survey captures a traveler's compliance with Service policy. Each submission of the survey to the Help Desk generates a Help Desk ticket and serves to best prepare and document that the device(s) are set up for international travel. IRTM hosts the survey on its [intranet site](#).

B. Traveling to countries designated as "red" by the Department (see the Department's [International Travel Advisory site](#) for more information) requires that the employee's Government-furnished device be wiped before leaving and again upon return. This is accomplished by generating a Help Desk ticket through the survey.

(1) We recommend that HQ employees get a loaner device from IRTM, if available, to avoid any potential issues associated with wiping devices.

(2) We advise Regions to establish their own pools of loaner devices, as resources allow, to help Regional employees avoid any potential issues related to wiping their Government-furnished devices.

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

## **THE SERVICE WIRELESS NETWORK AND MOBILE DEVICES**

### **3.15 How does the Service secure its wireless network while providing for mobile device access?**

**A.** We control remote access to Service networks, systems, and information according to [the Department's Security Control Standard](#). Employees who are trying to gain access to the Service wireless network using a Government-furnished mobile device must do so securely by using one of the Service's approved remote connection technologies, such as a Virtual Private Network (VPN) connection or a virtual desktop (i.e., Citrix). You can find details about using these solutions and information on approved remote connection technologies on IRTM's [MDM SharePoint site](#).

**B.** To protect the integrity of Service networks, systems, and data, IRTM:

- (1)** Monitors network traffic to and from mobile devices connected to the Service, and
- (2)** Will disconnect from the network any device that poses a security risk or is otherwise disrupting network or system functions. Disconnecting the device from the Service wireless network prevents the device from accessing an employee's Service email, the Service intranet, and any other data that is stored on a Service network drive until we can resolve the security risk.

## **ELECTRONICALLY STORED INFORMATION ON MOBILE DEVICES**

**3.16 How is sensitive Government data protected when using a mobile device?** Sensitive data or PII stored, transmitted, or viewed on mobile devices must be protected and encrypted in accordance with relevant standards. Employees ensure this by registering their mobile devices in the Service's MDM system so that we can verify that they meet necessary security requirements and configurations.

### **3.17 What are the requirements for storing and backing up ESI on mobile devices?**

Employees:

**A.** Should back up ESI stored on Government-furnished mobile devices using Department-approved methods (e.g., on a Service-managed server/share drive), and

**B.** Must not upload Service-owned data to any unapproved cloud computing or storage service.

**3.18 What are the requirements for removing ESI from mobile devices when the devices are retired?** We must ensure that ESI on mobile devices is removed according to applicable device sanitization requirements before the devices are recycled, traded in, transferred, or otherwise retired.

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 272 Telecommunications**

**Chapter 3 Managing and Securing Government-Furnished Mobile Devices      272 FW 3**

- A.** Employees must submit a Help Desk ticket for assistance from the appropriate MDM Administrator. The MDM Administrator must ensure that the device is removed from the MDM system and that all data has been wiped.
- B.** With help or oversight from the MDM Administrator, employees must:
- (1)** Sign out of any accounts associated with the mobile device, and
  - (2)** Perform a factory reset to return the device to default settings and wipe all data.
- C.** The device can then either be transferred or disposed of according to Service personal property management policies, including [310 FW 5, Property Management - Reuse, Transfer, Loan, Donate, Sales/Exchange, Recycling, or Disposal](#).
- D.** Service providers may have other procedures and requirements for trading in a device when upgrading. Employees should refer to their wireless service contract for those requirements, but they still must follow the sanitization procedures we describe above before trading in the device.

## **PRIVACY AND MOBILE DEVICES**

### **3.19 What are the expectations for privacy while using Government-furnished mobile devices?**

- A.** Employees using Government-furnished mobile devices should have no expectation of privacy when using the devices. In accordance with existing Department privacy agreements, Federal laws, and regulations, an employee's Government-furnished mobile device, its contents, and related transmissions may be monitored, intercepted, searched, recorded, and seized. These related transmissions include, but are not limited to, text messages, digital photos, and files.
- B.** Service-owned and managed mobile devices and the associated data are subject to eDiscovery for business purposes. In some cases, we may have to collect the devices to retrieve data and return them later.

/sgd/ James W. Kurth  
DEPUTY DIRECTOR

Date: July 3, 2018