



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.40

JUNE 23, 2016

EFFECTIVE DATE

(06-23-2016)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.40, *Information Technology (IT) Security, Wireless Security Policy*.

BACKGROUND

- (1) A report by the Government Accountability Office (GAO) titled *Federal Agencies Need to Improve Controls over Wireless Networks* (GAO-05-383), found that federal agencies need to better secure wireless devices and networks to protect federal information and information systems. The GAO report emphasized that it is crucial for agencies to develop wireless security policies, configure security tools to meet policy requirements, monitor the wireless networks, and train their staff in wireless security.

MATERIAL CHANGES

- (1) The following sections have been updated/clarified with this version of policy:
 - a. The following sections have been updated with this revision:
 - IRM 10.8.40.1.4 Risk Acceptance and Risk Based Decisions
 - IRM 10.8.40.3 IT Security Controls
 - IRM 10.8.40.3.1 Access Control
 - IRM 10.8.40.3.4 SA&A
 - IRM 10.8.40.3.5 Configuration Management
 - IRM 10.8.40.3.10 Physical and Environmental Protection
 - IRM 10.8.40.3.12 Planning
 - IRM 10.8.40.3.13 Risk Assessments
 - IRM 10.8.40.3.14 System Services and Acquisition
 - IRM 10.8.40.3.15 System Communication Protection
 - IRM 10.8.40.3.15.1.2 WLAN IDS Sensor Scanning
 - IRM 10.8.40.3.15.1.3 Wireless Application Servers
 - IRM 10.8.40.3.15.6 Encryption Standards
 - b. The following sections, in whole or part, have been relocated to IRM 10.8.55 Information Technology (IT) Network Security Policy
 - IRM 10.8.40.3.15.1.4 Employees Residential WLAN
 - c. Updated links throughout the document to reflect new organizational links.
 - d. Clarified details in the Roles and Responsibilities section.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.40, dated August 11, 2014, is superseded.

AUDIENCE

IRM 10.8.40 shall be distributed to all personnel responsible for ensuring that adequate security is provided for IRS information and information systems. The policy applies to all employees, contractors and vendors of the IRS.

Terence V. Milholland
Chief Technology Officer

10.8.40

Wireless Security Policy

Table of Contents

10.8.40.1 Overview

- 10.8.40.1.1 Purpose
- 10.8.40.1.2 Authority
- 10.8.40.1.3 Scope
- 10.8.40.1.4 Risk Acceptance and Risk-Based Decisions

10.8.40.2 Roles and Responsibilities

- 10.8.40.2.1 Senior Management/Executives
 - 10.8.40.2.1.1 Computer Security Incident Response Center (CSIRC)
 - 10.8.40.2.1.2 User and Network Services (UNS)

10.8.40.3 IT Security Controls

- 10.8.40.3.1 Access Control
- 10.8.40.3.2 Security Awareness and Training
- 10.8.40.3.3 Audit and Accountability Policy and Procedures
- 10.8.40.3.4 Security Assessment and Authorization (SA&A)
- 10.8.40.3.5 Configuration Management
- 10.8.40.3.6 Identification and Authentication
- 10.8.40.3.7 Incident Response
- 10.8.40.3.8 Maintenance
- 10.8.40.3.9 Media Protection
- 10.8.40.3.10 Physical and Environmental Protection
- 10.8.40.3.11 Planning
 - 10.8.40.3.11.1 System Security Planning
- 10.8.40.3.12 Risk Assessment
- 10.8.40.3.13 System and Services Acquisition
- 10.8.40.3.14 System and Communication Protection
 - 10.8.40.3.14.1 Wireless Local Area Network (WLAN) Infrastructure
 - 10.8.40.3.14.1.1 WLAN Access Point
 - 10.8.40.3.14.1.2 WLAN IDS Sensor Scanning
 - 10.8.40.3.14.1.3 Wireless Application Servers
 - 10.8.40.3.14.1.4 Wireless Clients
 - 10.8.40.3.14.2 Bluetooth
 - 10.8.40.3.14.2.1 Bluetooth Connectivity
 - 10.8.40.3.14.2.2 Bluetooth Pairing and Authentication
 - 10.8.40.3.14.2.3 Bluetooth Legacy Pairing
 - 10.8.40.3.14.2.4 Secure Simple Pairing Security (Security Mode 4)

-
- 10.8.40.3.14.2.5 Bluetooth Encryption
 - 10.8.40.3.14.2.6 Bluetooth Headsets
 - 10.8.40.3.14.3 Wireless System Components
 - 10.8.40.3.14.4 Global Positioning System (GPS) Devices
 - 10.8.40.3.14.5 Radio Frequency Identification (RFID)
 - 10.8.40.3.14.6 Encryption Standards
 - 10.8.40.3.15 System and Information Integrity

Exhibits

- 10.8.40-1 Wireless Security Control Exhibit
- 10.8.40-2 Glossary and Acronym List
- 10.8.40-3 References

10.8.40.1
(08-11-2014)
Overview

- (1) While wireless communications can offer many benefits, such as portability, flexibility, increased productivity, and lower installation costs, they can also pose significant risks to the critical infrastructure and assets of the IRS if not properly implemented and secured. As new technologies are developed, they become a major source of new vulnerabilities for which security solutions must be developed and implemented.
- (2) This IRM establishes the minimum security controls and guidance for the design, implementation, and use of wireless networks and devices within the IRS in order to:
 - a. Protect the critical infrastructure and assets of the IRS against attacks that exploit wireless transmissions.
 - b. Prevent unauthorized wireless deployments.
 - c. Enable wireless technologies that meet the security requirements of this policy to support the business needs of the organization.
- (3) The wireless requirements defined within this IRM are applicable to all wireless systems/devices used to connect to an IRS network or to store, process, receive, or transmit IRS or taxpayer data.
- (4) In an effort to cite the origin of a security requirement (National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA), Treasury, etc.), the origin may be referenced in parenthesis at the end of a requirement; such as (NIST SP 800-153, Sec. 2.1.2), (WIR0020), or (S-PM.1). If the requirement is IRS-defined, then it will be identified as an IRS-defined control, such as (IRS-defined). A complete list of references used as sources for this publication can be found in the Reference exhibit.

10.8.40.1.1
(08-11-2014)
Purpose

- (1) Internal Revenue Manual (IRM) 10.8.40, *Information Technology (IT) Security, Wireless Security Policy* provides policies and guidance to be used by the Internal Revenue Service (IRS) organization to carry out their respective responsibilities in information system security regarding wireless networks and devices.
- (2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.
- (3) To configure less restrictive controls requires a risk-based decision. See the Risk Acceptance and Risk-Based Decisions section within this IRM for additional guidance.

10.8.40.1.2
(08-11-2014)
Authority

- (1) IRM 10.8.1 *Information Technology (IT) Security, Policy and Guidance* establishes the security program and the policy framework for the IRS.

10.8.40.1.3
(08-11-2014)
Scope

- (1) This IRM applies to all IRS-owned wireless devices, services, and networks that store, process, or transmit IRS data or connect to an IRS network or system.
- (2) The provisions in this manual apply to:
 - a. All offices and business, operating, and functional units within the IRS.
 - b. Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing

providers, which use or operate information systems that store, process, or transmit IRS information or connect to an IRS network or system.

- c. All IRS information and information systems. For information systems that store, process, or transmit classified information, please refer to IRM 10.9.1, *National Security Information*, for additional procedures for protecting classified information.

- (3) The IRS shall ensure that the product (e.g., software, hardware) and version selected is in accordance with IRS Enterprise Architecture (EA) Enterprise Standards Profile (ESP) that dictates the official products and versions of software within the IRS.
- (4) The IRS shall ensure the application or system version is a version for which the vendor still offers standardized technical support.
- (5) In the event there is a discrepancy between this policy and IRM 10.8.1, IRM 10.8.1 takes precedence, unless the security controls/requirements within this policy are more restrictive, or otherwise noted.
- (6) This document shall be used in conjunction with appropriate Operating System (OS) IRMs, as well as other IRM-related requirements of any applications, web server, or database accessing the wireless system.
- (7) Organizations may augment the specific security controls within this policy to increase the security levels for a wireless technology implementation if approved by the responsible Authorizing Official (AO).

10.8.40.1.4
(06-23-2016)

Risk Acceptance and Risk-Based Decisions

- (1) Any exception to this policy requires that the Authorizing Official (AO) make a Risk-Based Decision.
- (2) Risk-Based Decision requests shall be submitted in accordance with IRM 10.8.1 and use Form 14201, as described in Risk Acceptance Request and Risk-Based Decision Standard Operating Procedures (SOPs), available on the Enterprise FISMA Compliance SharePoint site via the Risk Acceptance Requests link at <https://portal.ds.irsnet.gov/sites/CyberSRM/SitePages/RiskDecisions.aspx>. Refer to IRM 10.8.1 for additional guidance about risk acceptance.

10.8.40.2
(08-11-2014)

Roles and Responsibilities

- (1) IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*, defines IRS-wide roles and responsibilities related to IRS information and computer security, and is the authoritative source for such information.
- (2) The supplemental requirements provided below are specific to the implementation of IRS wireless security controls and shall be performed in conjunction with the roles and responsibilities defined within other IRMs in the 10.8 series.

10.8.40.2.1
(08-11-2014)

Senior Management/Executives

- (1) Requests to deploy WLAN components for connecting approved end-user devices shall be approved or disapproved by the appropriate AO prior to their deployment.

10.8.40.2.1.1
(10-05-2012)
**Computer Security
Incident Response
Center (CSIRC)**

- (1) The Computer Security Incident Response Center (CSIRC) within the Information Technology (IT) Cybersecurity Organization shall coordinate with UNS, who operates and maintains all Wireless Access Points, to ensure the appropriate Wireless Intrusion Prevention System (IPS) and Wireless Intrusion Detection System (WIDS) technology, for each instance of a wireless network, is instrumented, implemented, and monitored in accordance with System and Information Integrity section of this IRM.

10.8.40.2.1.2
(08-11-2014)
**User and Network
Services (UNS)**

- (1) User and Network Services (UNS) within the IT Organization shall own and operate all IRS enterprise WLAN deployments and wireless access points in accordance with this IRM.

10.8.40.3
(06-23-2016)
IT Security Controls

- (1) The IT security controls within this manual provide a range of safeguards and countermeasures for the IRS and IRS information systems with wireless capabilities.
- (2) Refer to IRM 10.8.1 for the other security control families other than those identified in this IRM.

10.8.40.3.1
(06-23-2016)
Access Control

- (1) The maximum number of consecutive unsuccessful login attempts to a mobile device shall be set in accordance with IRM 10.8.1. (SRG-MPOL-001)
- (2) Usage restrictions shall be established for wireless access. (SRG-MPOL-010)
- (3) IRS Concept of Operations (CONOPS) or site security plan shall include information specifying that Bluetooth devices use only Class 2 or 3 standard radios. (SRG-MPOL-011)
- (4) IRS CONOPS or site security plan shall include guidance requiring that Bluetooth radios must not be modified through signal amplification, antenna configuration, or other techniques that could affect signal detection or interception. (SRG-MPOL-012)
- (5) The IRS shall establish implementation guidance for wireless access. (SRG-MPOL-016)
- (6) Locations where Commercial Mobile Device (CMD) Wi-Fi access is approved or disapproved shall be documented. (SRG-MPOL-018)

Note: Additional information on WiFi access can be found in the appropriate System Security Plan (SSP) and on the WLAN Project sharepoint site <https://organization.ds.irsnet.gov/sites/ITUNSEFO/WLAN/SitePages/Home.aspx>

- (7) The IRS shall establish a wireless access control and security policy to define the administrative procedures and technical requirements to be met prior to being authorized to connect to an IRS information system. (SRG-MPOL-028)
- (8) The IRS shall maintain a list of all AO-approved wireless and non-wireless devices under their control that store, process, or transmit IRS information. (SRG-MPOL-029)
- (9) Each wireless device connecting to an IRS network shall be included in the applicable site security plan or other appropriate SA&A document. (SRG-MPOL-030)

- (10) The IRS shall have a wireless remote access policy signed by the site AO, Director, or other appropriate authority. (SRG-MPOL-031)
- (11) The IRS wireless remote access policy shall address the following security topics: (SRG-MPOL-031)
- Device unlock requirements.
 - Anti-virus application.
 - Personal firewall.
 - Client software patches kept up to date - Internet browsing through enterprise Internet gateway.
 - Device security policy managed by centrally-managed policy manager.
 - Anti-spyware app (recommended).
 - Procedures after client is lost, stolen, or other security incident occurs.
 - Host-based Wireless Intrusion Detection and Prevention System (WIDPS)/monitor WIDPS.
 - Configuration requirements of wireless client - Home WLAN authentication requirements.
 - Home WLAN SSID requirements
 - Separate WLAN access point required for home WLAN.
 - Password length and complexity required for home WLAN.
 - Use of third-party Internet portals (kiosks) (approved or not approved).
 - Use of personally-owned or contractor-owned client devices (approved or not approved).
 - Implementation of health check of client device before connection is allowed.
 - Places where remote access is approved (home, hotels, airport, etc.).
 - Roles and responsibilities:
 - Which users or groups of users are and are not authorized to use organization's WLANs.
 - Which parties are authorized and responsible for installing and configuring APs and other WLAN equipment.
 - WLAN infrastructure security:
 - Physical security requirements for WLANs and WLAN devices, including limitations on the service areas of WLANs.
 - Types of information that may and may not be sent over WLANs, including acceptable use guidelines.
 - WLAN client device security:
 - The conditions under which WLAN client devices are and are not allowed to be used and operated.
 - Standard hardware and software configurations that must be implemented on WLAN client devices to ensure the appropriate level of security.
 - Limitations on how and when WLAN client's device may be used, such as specific locations.
 - Guidelines on reporting losses of WLAN client devices and reporting WLAN security incidents.
 - Guidelines for the protection of WLAN client devices to reduce theft.
- (12) The IRS shall ensure the network access control solution supports wireless clients and solutions if wireless networking is implemented. (SRG-MPOL-035)
- (13) IRS employees shall be responsible to ensure they only use the secured Wi-Fi: (IRS-defined)
- a. Of approved hotels where they are staying; and
 - b. Installed at home

Note: The intent of this requirement is to avoid a situation where the employee is inadvertently using their neighbors Wi-Fi or a nearby hotel.

- 10.8.40.3.2
(06-23-2016)
Security Awareness and Training
- (1) Training materials shall be developed stating Bluetooth must be disabled on all applicable devices unless they employ FIPS 140-2 validated cryptographic modules for data in transit. (SRG-MPOL-019)
- 10.8.40.3.3
(08-11-2014)
Audit and Accountability Policy and Procedures
- (1) Auditable events shall be logged and processed in accordance with IRM 10.8.3 *Information Technology (IT), Security Audit Logging Security Standards*.
- (2) Wireless access point logging shall be enabled. (IRS-defined)
- (3) Audit logs shall be reviewed in accordance with IRM 10.8.1 and IRM 10.8.3. (IRS-defined I)
- 10.8.40.3.4
(06-23-2016)
Security Assessment and Authorization (SA&A)
- (1) IRS Wireless networks and devices transmitting IRS information and/or connecting to an IRS network shall be authorized (i.e., Security Assessment and Authorization (SA&A)) in accordance with IRM 10.8.1.
- (2) IRS wireless systems (including associated peripheral devices, operating systems, applications, network/Personal Computer (PC) connection methods, and services) shall be approved by the AO prior to installation and use for processing IRS information. (DISA STIG ID: WIR0005) (SRG-MPOL-017)
- (3) Wireless devices (e.g., computers, smartphones, tablets) and support enterprise servers (e.g., BlackBerry Enterprise Servers, Good Servers) shall be incorporated into the appropriate security authorization documentation (e.g., System Security Plan) for the IT area that implements the devices within the IRS organization. (DISA STIG ID: WIR0020)
- (4) Wireless remote access equipment, locations, and location types (e.g., site network Wi-Fi, home, hotel, public) approved for usage shall be documented in the appropriate System Security Plan (SSP). (DISA STIG ID: WIR0020)
- 10.8.40.3.5
(06-23-2016)
Configuration Management
- (1) Configuration management procedures shall be developed for wireless devices to incorporate the requirements of IRM 10.8.1 and this IRM.
- (2) In accordance with IRM 10.8.1, the IRS shall:
- a. Establish and maintain baseline configurations and inventories of IRS information systems. (IRS-defined)
- b. Establish and enforce security configuration settings for IT products installed on IRS information systems. (DISA STIG ID: WIR0020)
- c. Monitor and control changes to the baseline configurations of IRS information systems throughout the respective System Development Life Cycle (SDLC) (i.e., IRS Enterprise Lifecycle (ELC)). (DISA STIG ID: WIR0020)
- (3) Laptops with WLAN interfaces shall have the WLAN card radio set to OFF as the default setting. (DISA STIG ID: WIR0180)
- (4) WLAN EAP-TLS implementation shall use certificate-based PKI authentication to connect to IRS networks. (DISA STIG ID: WIR0116)

- (5) WLAN clients shall not be configured to connect to other WLAN devices without the user initiating a request to establish such a connection.(DISA STIG ID: WIR0185)
 - (6) WLAN-capable devices shall not use wireless peer-to-peer networks to connect to other devices.(DISA STIG ID: WIR0165)
 - (7) Security firmware updates and patches to wireless hardware and software components shall be fully tested and deployed as soon as they become available in accordance with IRM 10.8.50, *Information Technology (IT) Security Servicewide Security Patch Management*.
 - (8) A list shall be maintained of all mobile computing devices that are used to store, process, and transmit IRS data in accordance with inventory requirements defined in IRM 10.8.1 , IRM 10.8.26 *Information Technology (IT) Security, Mobile Devices, Mobile Computing Device Management and Bring Your Own Device Security Policy* , and IRM 2.14 *Asset Management* series.
 - (9) The list of approved wireless devices shall: (DISA STIG ID: WIR0015)
 - a. Be stored in a secure location and
 - b. Include, at a minimum, the following:
 - Access point Media Access Control (MAC) address (WLAN only).
 - Access point IP address (WLAN only).
 - Wireless client MAC address.
 - Network DHCP range (WLAN & Wireless Wide Area Network (WWAN) only).
 - Type of encryption enabled.
 - Access point Service Set Identifier (SSID) (WLAN only).
 - Manufacturer, model number, and serial number of wireless equipment.
 - Equipment location or who the device is issued to
 - Assigned users with telephone numbers.
 - (10) The IRS IT organization shall create and document a list of network protocols within a mobile device deemed to be non-secure for remote access into IRS networks. (SRG-MPOL-002)
-
- (1) Identification and Authentication requirements shall be in accordance with IRM 10.8.1.
 - (2) User authentication mechanisms for the management interfaces of wireless access points and devices shall be enabled. (DISA STIG ID:NET 1623)

10.8.40.3.6
(08-11-2014)
Identification and Authentication

- (3) A password shall be enabled for each wireless client that connects to an IRS network or system. Passwords shall comply with IRM 10.8.1. (IRS-defined)
- (4) Passwords shall be created and maintained in accordance with IRM 10.8.1 and the appropriate operating system IRM for the underlying OS where applicable.
 - a. Wireless devices shall have the default manufacturer passwords changed. (DISA STIG ID: NET 240)
- (5) The fallback method for failed wireless authentication (e.g., forgotten passwords and lost smart cards) shall meet the same authentication requirements as the primary method. (IRS-defined)

10.8.40.3.7
(08-11-2014)
Incident Response

- (1) Wireless networks and devices shall be incorporated into IT incident response capabilities and plans in accordance with IRM 10.8.1.

10.8.40.3.8
(08-11-2014)
Maintenance

- (3) Wireless maintenance activities shall be planned and scheduled in accordance with IRM 10.8.1.

10.8.40.3.9
(08-11-2014)
Media Protection

- (1) Media storage and protection controls shall be implemented in accordance with IRM 10.8.1.
- (2) Prior to decommissioning or transferring to another government agency, wireless systems and other devices that will no longer be used by the IRS, all data (including configuration data) shall be sanitized from the host in accordance with IRM 2.14.1 *Information Technology (IT) Asset Management*, IRM 2.7.4 *IT Operations, Magnetic Media Management*, and IRM 10.8.1. (IRS-defined)

10.8.40.3.10
(06-23-2016)
Physical and Environmental Protection

- (1) Physical access controls shall be employed to restrict the entry and exit of unauthorized personnel and prevent the removal or unauthorized modification of wireless devices installed in an IRS facility. (IRS-defined)
- (2) All wireless network devices, such as Wireless Intrusion Detection System (WIDS) and wireless routers, access points, gateways, and controllers shall be: (DISA STIG ID: WIR0025) (SRG-MPOL-084)
 - a. Secured in such a manner to prevent tampering or theft; or
 - b. Located in a secure room with limited access.
- (3) Wireless devices shall not be permitted or operated in areas where sensitive data is stored, processed, or transmitted unless the devices are approved by the appropriate AO and meet the requirements set forth within this IRM and IRM 10.8.1. (DISA STIG ID: WIR0040)

- (4) External boundary protection mechanisms shall be in place around the perimeter of IRS facilities, as necessary and based on a documented risk assessment, to prevent unauthorized access to wireless systems. (IRS-defined)

10.8.40.3.11
(06-23-2016)

Planning

- (1) All users of mobile devices or wireless devices shall sign a user agreement before the mobile or wireless device is issued to the user. (DISA STIG-ID: WIR0030)
- (2) Refer to the Planning section of IRM 10.8.1 for additional guidance.

10.8.40.3.11.1
(08-11-2014)

**System Security
Planning**

- (1) Wireless devices connecting directly or indirectly (e.g., ActiveSync, wireless) to a network shall be included in the appropriate System's SA&A documentation (i.e., System Security Plan (SSP)). (DISA STIG ID: WIR0020)

10.8.40.3.12
(06-23-2016)

Risk Assessment

- (1) Risk assessments of specific versions of wireless technology shall be conducted in accordance with Exhibit 10.8.40-1 Wireless Security :
- (2) Deficiencies in conformance to the security exhibits shall be documented in risk assessment reports and brought to the attention of the system's AO. (DISA STIG ID: WIR0005)
- (3) Wireless solutions shall not be used if they are not compliant with the security compliance levels/thresholds established by Cybersecurity. (DISA STIG ID: WIR0005)
 - a. Refer to the Risk Assessment section of IRM 10.8.1 for additional guidance.
- (4) For wireless networks and devices that include wireless remote access, the risk assessment shall identify any additional risks and mitigation associated with non-government facilities. (DISA STIG ID: WIR0005)

Note: The risk assessment scope includes the types of non-government facilities where wireless remote access might be conducted.

#

- (6) Wireless access point range boundaries shall be tested to measure and establish the precise extent of the wireless coverage. (IRS-defined)

Note: This requirement does not apply to home user or public wireless network equipment.

- (1) Wireless products shall be acquired, accounted for, and inventoried in accordance with IRM 10.8.1. (IRS-defined)
- (2) Wireless devices shall adhere to the IRS Enterprise Lifecycle (ELC) in accordance with IRM 10.8.1. (IRS-defined)
- (3) The IRS shall only procure and deploy WPA2-Enterprise certified WLAN equipment and software for wireless systems that connect directly to IRS networks. (SRG-MPOL-024)

- (1) Refer to Treasury Directive (TD) 86-02, *Radio Frequency Management* and IRM 10.8.1, for detailed telecommunication environment and services requirements.
- (2) Personally owned or contractor owned CMDs shall not be used to transmit, receive, store, or process IRS information or connect to IRS networks without AO authorization. (DISA STIG ID: WIR0010-01)
- (3) Privately owned Ethernet to Wi-Fi converters (e.g., wireless Ethernet bridges, wireless media adapters) shall not be connected to IRS laptops or workstations. (DISA STIG ID: WIR0010-01)
- (4) Printers shall not be connected to an IRS network via a wireless connection. (IRS-defined)
- (5) FIPS 140-2 validated (or later) encryption modules shall be used to encrypt unclassified sensitive data-at-rest on wireless devices (e.g., laptop, smart-phone, tablet). (DISA STIG ID:WIR0190)

- (1) WLAN routers and hubs may be deployed to connect end-user desktop computers and devices only with prior approval from the appropriate AO. (IRS-defined)

[illegible]

10.8.40.3.14.1.1
(08-11-2014)

WLAN Access Point

- (1) Authorized Guest networks (i.e., internet-only traffic) shall utilize perimeter security architecture (e.g., Antivirus, Content Filtering) in accordance with this IRM and IRM 10.8.1. (IRS-defined)

10.8.40.3.14.1.2
(06-23-2016)

WLAN IDS Sensor Scanning

- (1) The IRS shall monitor for unauthorized wireless connections to an information system in accordance with IRM 10.8.55 *Network Security Policy*. (SRG-MPOL-005)
- (2) The AO shall define a time period for monitoring of unauthorized wireless connections to information systems, including scans for unauthorized wireless access points. (SRG-MPOL-006)
- (3) The IRS shall document and take appropriate action if an unauthorized wireless connection is discovered. (SRG-MPOL-007)
- (4) The IRS shall define the appropriate action(s) to be taken if an unauthorized wireless connection is discovered. (SRG-MPOL-008)
- (5) The IRS shall ensure WIDS sensor scan results are saved for at a minimum one (1) year. (SRG-MPOL-049)

10.8.40.3.14.1.3
(06-23-2016)

Wireless Application Servers

- (1) Wireless application servers (e.g., BlackBerry Enterprise Servers or other communication servers that act as a gateway between a server and a wireless client) shall be configured in accordance with IRM 10.8.1, this IRM, and any other applicable IRMs. (IRS-defined)
- (2) Data exchange shall be encrypted in accordance with the encryption standards of this IRM and IRM 10.8.1. (IRS-defined)
- (3) Wireless application servers shall have the latest virus scanning and security patches installed and updated to detect and prevent viruses and other malicious content from infecting the enterprise network. (IRS-defined)

10.8.40.3.14.1.4
(08-11-2014)

Wireless Clients

- (1) IRS-issued/approved wireless desktop, laptop, and clients shall be used and configured in accordance with the security requirements and encryption standards of this IRM and IRM 10.8.1. (IRS-defined)
- (2) Wireless mobile computing devices shall comply with IRM 10.8.26,

#

#

#

a.

#

#

#

Note: The preferred enforcement method is through an automated technical control whenever feasible.

- (5) All network interfaces not authorized for usage (including contingency plans for business continuity, disaster recovery, etc.) shall be disabled. (NIST SP 800-153, Sec. 2.1.2)

- (1) Bluetooth is an open standard for short-range digital radio signals used for creating small wireless networks on an ad hoc basis. The requirements in this section shall apply to Bluetooth technology as well as any other ad hoc network and Wireless Personal Area Network (WPAN) for which this policy does not provide specific guidance (e.g., ZigBee). (IRS-defined)
- (2) Bluetooth communications shall be used for transmission in accordance with the requirements within this IRM and IRM 10.8.1. (IRS-defined)

[illegible]

- 10.8.40.3.14.2

- (6) Mobile OS specific Bluetooth security requirements for can be found in IRM 10.8.26. (IRS-defined)

10.8.40.3.14.2.1
(08-11-2014)

Bluetooth Connectivity

#

- (2) Bluetooth devices shall not be connectable (responsive to incoming connection requests from other Bluetooth devices) unless necessary to establish a connection, at which time the capability shall be turned off. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 2.2.1)

Note: Ideally, devices should not be connectable once the connection is established, or should never be connectable if operationally possible. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 2.2.1)

- (3) Devices shall initiate Bluetooth connections only when necessary to establish a connection, at which time the capability shall be turned off. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 2.2.2)

Note: Ideally, only one device per Bluetooth piconet shall initiate connections to other devices in that piconet.

- (4) Bluetooth devices shall prompt the user to authorize all incoming Bluetooth connection requests before allowing any incoming connection request to proceed. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 3.1)
- (5) Users shall never accept connections, files, or other objects from unexpected, unknown, or untrusted sources. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 3.2)

10.8.40.3.14.2.2
(08-11-2014)

Bluetooth Pairing and Authentication

- (1) During initial Bluetooth connection requests, all Bluetooth devices shall pair (mutually authenticate) and bond (store the resulting link key). (DoD Bluetooth Peripheral Device Security Requirements, Sec. 4.1.1)
- (2) Bluetooth devices shall store link keys securely. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 4.1.2)
- (3) Subsequent to pairing, all Bluetooth devices shall again mutually authenticate each other during all connection requests. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 4.1.3)
- (4) Bluetooth devices shall not delete existing link keys until after a replacement link key is generated successfully. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 4.1.4)

- (5) All Bluetooth pairing shall be done as infrequently as possible, ideally in a secure location (e.g., an indoor non-public area away from windows and behind physical access controls) where attackers cannot realistically observe entry of the passkey or intercept transmitted pairing messages. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 4.1.5)
- (6) Users or administrators shall not enter or confirm pairing passkeys when unexpectedly prompted to do so. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 4.1.6)
- (7) Users or administrators shall immediately remove unused, lost, stolen, or discarded Bluetooth devices from paired device lists. (DoD Bluetooth Peripheral Device Security Requirements, Sec. 4.1.7)

10.8.40.3.14.2.3
(08-11-2014)
**Bluetooth Legacy
Pairing**

10.8.40.3.14.2.4
(08-11-2014)
**Secure Simple Pairing
Security (Security Mode
4)**

10.8.40.3.14.2.5
(08-11-2014)
Bluetooth Encryption

#

10.8.40.3.14.2.6
(08-11-2014)
Bluetooth Headsets

#

Note: The term “headset” is intended to include any device designed to communicate the human voice to and from a cellular telephone or mobile computing device. It includes portable headsets, hands-free devices in vehicles, portable speakerphones, and other devices with no data functionality.

(IRS-defined)

- (2) Acquisition of IRS-procured Bluetooth headsets shall be a Business Unit Expense. (IRS-defined)

#

- (4) Bluetooth headsets shall not have any capabilities beyond voice communication and encryption. (IRS-defined)

- 10.8.40.3.14.3
(08-11-2014)
**Wireless System
Components**

- 10.8.40.3.14.4
(08-11-2014)
**Global Positioning
System (GPS) Devices**

##

- (4) IRS-owned or personally owned GPS devices shall not be connected to an IRS computer.

#

10.8.40.3.14.5
(08-11-2014)

**Radio Frequency
Identification (RFID)**

- (1) The IRS shall provide notice and full disclosure on the use of RFID to those employees using an RFID application or system. (IRS-defined)

10.8.40.3.14.6
(06-23-2016)

Encryption Standards

#

- (2) The information stored or transmitted through a wireless network or device must be assessed to determine the sensitivity of the information and determine the necessary security controls. (IRS-defined)
- (3) Encryption of sensitive files and/or directories contained on mobile computing devices (e.g. laptops, smartphones, tablets)shall be used in accordance with IRM 10.8.26, (IRS-defined)
- (4) The WLAN shall use AES-CCMP to protect data-in-transit.(DISA STIG ID: WIR0125-01)
- (5) The WLAN shall use EAP-TLS.(DISA STIG ID: WIR0115-01)
- (6) See Exhibit 10.8.40-1 for wireless guidance on specific wireless implementations.

10.8.40.3.15
(08-11-2014)

**System and Information
Integrity**

- (1) Wireless system and information integrity protection shall be conducted in accordance with IRM 10.8.1. (IRS-defined)

Exhibit 10.8.40-1 (06-23-2016)**Wireless Security Control Exhibit**

1. The technical requirements for Wireless Security configuration are maintained in an Excel spreadsheet, which is provided on the IRS IT Security SharePoint site at: https://portal.ds.irsnet.gov/sites/CyberSP/tools/IRM_Exhibits/Forms/AllItems.aspx

Exhibit 10.8.40-2 (08-11-2014)
Glossary and Acronym List

Acronym/Abbreviation	Word/Meaning
AAA (RADIUS)	Authentication, Authorization and Accounting
ACIO	Associate Chief Information Officer
ACL	Access Control List
Ad Hoc Mode	A method that allows all wireless devices within range of each other to discover and communicate in peer-to-peer (P2P) fashion without involving central access points.
Advanced Encryption Standard (AES)	A symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers: AES-128, AES-192, and AES-256. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192, and 256 bits, respectively.
AO	Authorizing Official
AP	Access Point
Bluetooth	A proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions) from fixed and mobile devices, creating wireless personal area networks (WPANs) with high levels of security. Created by telecoms vendor Ericsson in 1994,[1] it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization.
CCMP	Counter-mode/CBC-MAC Protocol
CI	Criminal Investigation
Controlled Unclassified Information (CUI)	A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. In the future, the designation CUI will replace Sensitive But Unclassified (SBU).
CMD	Commercial Mobile Device
CSIRC	Computer Security and Incident Response Center
Data Spillage	Data spillage occurs whenever sensitive data becomes accessible (such as via email or document transfer) onto an information system that is not authorized to process, store, or transmit the data.
DHCP	Dynamic Host Configuration Protocol

Exhibit 10.8.40-2 (Cont. 1) (08-11-2014)

Glossary and Acronym List

Acronym/Abbreviation	Word/Meaning
DISA	Defense Information Systems Agency
DoD	Department of Defense
EAP	Extensible Authentication Protocol
ECDH	Elliptic Curve Diffie-Hellman
EEO	Equal Employment Opportunity
ELC	Enterprise Life Cycle
ERAP	Enterprise Remote Access Project
ESP	Enterprise Standards Profile
FIPS	Federal Information Processing Standards
Global Positioning System (GPS)	A system for determining position by comparing radio signals from several satellites.
GMK	Group Master Key
Good Mobile Messaging	An over-the-air solution users can use to synchronize their PIM data with a handheld device. It consists of a client application for managing PIM data, along with server-side software that provides push capability for email systems and supporting tools.
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
In Band Management	Management communications with a managed switch through the networked data ports of the switch.
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISSO	Information System Security Officer
IT	Information Technology
LED	Light Emitting Diode
LR-WPAN	Low-Rate Wireless Personal Area Network
MAC	Media Access Control
Multimedia Messaging Service (MMS)	An accepted standard for messaging that lets users send and receive messages formatted with text, graphics, photographs, audio, and video clips.
NAT	Network Address Translation

Exhibit 10.8.40-2 (Cont. 2) (08-11-2014)**Glossary and Acronym List**

Acronym/Abbreviation	Word/Meaning
Network Out of Band Management (NE OOBM)	Management communications with a managed switch through a dedicated management port (or ports) separate from the data ports
Network Time Protocol (NTP)	A protocol for synchronizing the clocks of computer systems. NTP is used to ensure accurate log file timestamp information. Without synchronized time, accurately correlating information between devices becomes difficult, if not impossible.
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
P2P	Peer-to-Peer
PC	Personal Computer
PGLD	Privacy Governmental Liaison and Disclosure; formerly Privacy, Information Protection and Data Security (PIPDS)
Piconet	An ad hoc network linking a user group of devices using Bluetooth technology protocols to allow one master device to interconnect with up to seven active slave devices (because a three-bit MAC address is used). Up to 255 further slave devices can be inactive, or parked, which the master device can bring into active status at any time. Piconet range varies according to the class of the Bluetooth device. Data transfer rates vary between about 200 and 2100 kilobits per second (kbit/s) at the application.
PII	Personally Identifiable Information
PIM	Personal Information Management
PMK	Pairwise Master Key
Remote Authentication Dial In User Service (RADIUS)	A networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect to a network service.
RFID	Radio Frequency Identification
RSN	Robust Security Network
SA&A	Security Assessment and Authorization
SAR	Security Assessment Report
SAS	Security Assessment Services

Exhibit 10.8.40-2 (Cont. 3) (08-11-2014)

Glossary and Acronym List

Acronym/Abbreviation	Word/Meaning
Sensitive But Unclassified Information (SBU)	Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 U.S.C. § 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.
SCR	Smart Card Reader
SDLC	System Development Life Cycle
Smartphone	A smartphone is a mobile phone built on a mobile computing platform with more advanced computing ability and connectivity than a feature phone. Smartphones combine the functions of a personal digital assistant (PDA), camera, and mobile phone. They also typically include GPS, touchscreens, web-browsing capabilities, and include a mobile operating system (mobile OS) (e.g., Apple iOS, Microsoft Windows Phone, and RIM BlackBerry OS).
SME	Secure Mobile Environment
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedures
Split Tunneling	Split tunneling is a computer networking concept which allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same network connection.
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSP	System Security Plan
STIG	Security Technical Implementation Guide
Tablet	A tablet computer (tablet) is a mobile computer, larger than a mobile phone or mobile computing device, integrated into a flat touchscreen and primarily operated by touching the screen rather than using a physical keyboard. It often uses an onscreen virtual keyboard, a passive stylus pen, or a digital pen. Besides having most PC capabilities, popular typical tablet computers include wireless Internet browsing functions, potential cell phone functions, GPS navigation, and video camera functions.. In many ways, the functions and purposes of laptops, tablets, and smartphones overlap.
TD P	Treasury Directive Publication

Exhibit 10.8.40-2 (Cont. 4) (08-11-2014)**Glossary and Acronym List**

Acronym/Abbreviation	Word/Meaning
Telematics	The integrated use of telecommunications and informatics, also known as ICT (Information and Communications Technology).
TIGTA	Treasury Inspector General for Tax Administration
UMA	Unlicensed Mobile Assess
USB	Universal Serial Bus
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Protection
WIDS	Wireless Intrusion Detection System
Wi-Fi	Wireless Fidelity
Wireless	A technology that enables devices to communicate without physical connections (without requiring network or peripheral cabling).
Wireless Bridge	A device that links two wired networks, generally operating at two different physical locations through wireless communications.
Wireless Client	A system or device that wirelessly accesses an AP or another client directly.
Wireless Mobile Computing Device	A non-stationary wireless client with the capability of recording, storing, and/or transmitting information. Wireless mobile computing devices PEDs include, but are not limited to, cellular phones, tablets, network interface cards, PDAs, keyboards, mice, and Universal Serial Bus (USB) devices that transmit data wirelessly.
Wireless Fidelity (Wi-Fi)	A term describing a wireless local area network that observes the IEEE 802.11 protocol.
Wipe	A command or series of commands that resets the mobile device to its default factory condition and deletes all user data, including user-installed applications, stored on the device
Wireless Local Area Network (WLAN)	A group of wireless APs and associated infrastructure within a limited geographic area, such as an office building or building campus, that is capable of radio communications. WLANs are usually implemented as extensions of existing wired LANs to provide enhanced user mobility.

Exhibit 10.8.40-2 (Cont. 5) (08-11-2014)

Glossary and Acronym List

Acronym/Abbreviation	Word/Meaning
WPA2	WiFi Protected Access (WPA) and WiFi Protected Access II (WPA2) are security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system WEP (Wired Equivalent Privacy). The WPA2 certification mark indicates compliance with the full IEEE 802.11i standard.
WPAN	Wireless Personal Network
WWAN	Wireless Wide Area Network
Zigbee	A specification for a suite of high-level communication protocols using small, low-power digital radios based on the IEEE 802.15.4-2003 standard for Low-Rate Wireless Personal Area Networks (LR-WPANs), such as wireless light switches with lamps, electrical meters with in-home-displays, consumer electronics equipment via short-range radio needing low rates of data transfer. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other WPANs, such as Bluetooth.

Exhibit 10.8.40-3 (10-05-2012)**References****Internal Revenue Service**

IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*

IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*

IRM 10.8.3, *Information Technology (IT) Security, Audit Logging Security Standards*

Defense Information Systems Agency (DISA)

WLAN Client v6r9, Oct 24, 2014

Mobility Policy v2r2, Mar 12, 2013 (Previously General Wireless)

Bluetooth/Zigbee v6r8, Apr 25, 2013

RFID Scanner v6r8, Apr 25, 2013

RFID Workstation v6r8, Apr 25, 2013

Wireless Keyboard and Mouse v6r8, Apr 25, 2013

National Institute of Standards and Technology (NIST)

NIST SP 800-48, Rev 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008

NIST SP 800-57, Rev 3 *Recommendation for Key Management: Part 1: General*, July 2012

NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* February 2007

NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)* February 2012

Other Publications

DoD -*Bluetooth Peripheral Device Security Requirements* April 2011

RFC 2119 - *Key words for use in RFCs to Indicate Requirement Levels*

ISO/IEC Directives, Part 2 – *Rules for the Structure and Drafting of International Standards: Annex H, Verbal Forms for the Expression of Provisions*