CHAPTER 10, PART 3
PORTABLE ELECTRONIC DEVICES AND WIRELESS TECHNOLOGY

1 BACKGROUND

Portable Electronic Devices (PED) and Wireless technology have now become part of the evolving business landscape. Cellular telephones, pagers and handheld electronic devices can be seen with greater frequency being used in business meetings, while on business travel and on street corners to communicate with the office, business associates or customers.

A PED is any electronic device that is capable of receiving, storing or transmitting information using any format (i.e., radio, infrared, network or similar connections) without a permanent link to Federal networks. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders. Many of the serious security issues regarding PEDs stem from the manner in which they interact with other computer resources. Typically PEDs communicate wirelessly over limited distances to other devices within and outside USDA. Transmissions using these devices are unprotected, could spread malware to USDA and other networks or they could serve as a back channel through which vulnerabilities are exploited. Users could also use these devices to access a third party Internet Service Provider (ISP) and download applications in violations of security policy. Generally PEDs include but are not limited to: cell phones, pagers, text messaging devices (Blackberries), hand scanners, portable digital assistants, voice recorders, and flash memory. All of these devices can be used to transport data surreptitiously to be read/decoded at a later time.

DR 3300, Telecommunications and Internet Services and Use, defines Wireless Communications as anything that supports communication between mobile, portable, or fixed facilities through the use of the electromagnetic spectrum. Examples include but are not limited to: AM and FM broadcasting, UHF and VHF television, satellite, microwave, citizen's band, paging, cellular service, wireless local area networking technology, infrared and Personal Communications Service (PCS). Wireless technology offers portability, flexibility, increased productivity and lower installation costs. Wireless Local Area Networks allow users to quickly move workstations and laptops to different office locations without the need for wires and loss of network connectivity. Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). Personal Area Networks, such as those enabled by the Bluetooth standard, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections.

However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot. The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks. In addition, immediate concerns include device theft, theft of service and industrial or foreign espionage. To reduce or eliminate these threats, the following policy and procedures have been developed.

2 POLICY

All USDA agencies and staff offices will develop an agency secure approach for the implementation of PEDs and wireless technology. This strategy will consider recommendations contained in the Telecommunications Advisory Sub-Council

(TASC) USDA Wireless Strategy Report dated March 2003, National Institute of Standards and Technology (NIST) Interagency Report 6981 dated April 2003 and Special Publication 800-48, Wireless Network Security.

All implementations of PEDs and Wireless technology require that a formal risk assessment be conducted in the environment where this technology will operate prior to deployment of the PED or wireless technology. Agencies will plan and execute measures to safeguard their systems and lower security risks to a manageable level using the Procedures and Checklists included in this material. Strong encryption and authentication techniques will be used in the transmission and storage of sensitive information, where applicable. Each agency will secure and be accountable for PEDs including establishing password protection to devices, if available, and any built-in or removable flash memory used in such devices. Precautions will be taken to employ management, operational and technical countermeasures that are appropriate for the use of these devices and wireless technology. This policy does not necessarily just apply to Government Furnished Property (GFP), but to any equipment and device used for official purposes. Each agency and staff office will develop a formal PED and Wireless Plan that documents use of this technology and planned implementations. Elements of this plan will also be documented in the Overall Agency Security Plan, including funding levels and countermeasures employed. For additional operational information on PEDs and wireless, please consult DN 3300-12 and DN3300-13.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with a updated timeline for completion**.** CS will monitor all approved exceptions.

3 PROCEDURES

All USDA agencies and staff offices will follow the procedures below for use of PEDs and Wireless technology:

a Encryption techniques, including digital certificates/PKI/Biometrics, that conform to USDA and NIST requirements will be used for Infrared and wireless transmissions and for data storage on PEDs;

b Restrictive security profiles will be established to specifically address device rights, time –of-day usage, server and service access;

c Stringent security controls will be established for PEDs which transmit or store data with a medium or high level of sensitivity or confidentiality;

d Strict physical security standards for PEDs will be implemented to include requirements to hand carry PEDs during travel, powering off device not in use, tracking and tagging of PEDs and contact information in case device is lost or stolen;

e All PEDs, flash memory devices and wireless devices will be provided by the government unless an approved detailed exception has been granted by the CIO;

f PEDs will be screened by the agency or staff office IT Staff at least quarterly for appropriate configurations, viruses, antivirus protection and patch level will be updated, as required;

g Where applicable, Virtual Private Network (VPN) technology is required; split tunneling profiles will be disabled;

h Agencies and staff offices will issue a detailed “Personal Use Policy” for PEDS to include: restrictions on storage of unencrypted SBU data, corporate passwords, Use of Private ISPs, use of Unauthorized software or Copyrighted material, removal of security controls and the use of non-government devices;

i The Personal Use Policy will be signed by all users and kept with the accountable records for PEDs;

j Agencies will develop a specific set of guidelines for mobil users to include: restrictions on use of Private ISPs, specified user locations, disabling of security features and methods of access;

k Standardized configurations will be established for all PEDs to include Operating System software, firmware and authorized applications; modems will be disabled/removed unless specifically required for official duties;

l Security for PEDs and Wireless technology will be coordinated and managed by the Agency Information Systems Security Program Manager (ISSPM);

m Each agency and staff office will be required to conduct PED and Wireless technology risk assessments and complete the appropriate checklists in Tables 1 - 3 to assess the security posture and countermeasures necessary to ensure all security requirements are satisfied; and

n Agencies and staff offices will develop and retain the right to delete or purge data on a PDA in cases of suspected compromise.

4 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Publish and disseminate policy and procedures for PEDs and Wireless Technology;

(2) Provide technical assistance to agencies and staff offices in planning and implementing PEDs and Wireless Technology;

(3) Periodically review agency internal procedures, risk assessments, checklists and formal plans for the use of these devices and technology; make recommendations for the security weaknesses identified;

(4) Research and suggest appropriate security software and security countermeasures for PEDs and Wireless Technology, as required;

(5) Monitor agency implementations to ensure that devices are configured properly, have appropriate antivirus software and system patches;

(6) Collaborate with the OIG and law enforcement in cases of suspected abuse of the personal use policy, as required; and

(7) Review agency exception requests promptly and make security recommendations to the CIO.

b <u>The Associate CIO for Information Resources Management (IRM) will:</u>

Receive, review and coordinate a response with the Associate CIO for Cyber Security to any requests for exceptions to this policy.

c <u>The Associate CIO for Telecommunications Services and Operations (TSO) will:</u>

(1) Ensure that PED and Wireless Technology used by agencies and staff offices is in accordance with the Telecommunications Architecture;

(2) Review the operational support capability of wireless technology and make recommendations for implementation to agencies; and

(3) Review all exceptions, in conjunction with CS, to ensure that PEDs and Wireless Technology complies with TSO operational guidelines.

d <u>Agency Management and Information Technology Officials or Chief Information Officer will:</u>

(1) Implement applications of PEDs and Wireless Technology in accordance with policy and procedures;

(2) Ensure that agency guidelines are developed and implemented to include requirements for technology plans, risk assessments and strict physical accountability;

(3) Require that the appropriate PEDs and Wireless Technology Checklist be completed prior to

installations; strict security controls be employed and standardized configurations be established and monitored;

(4) Ensure that encryption, authentication and VPN Technology is employed, where appropriate;

(5) Require that a Personal Use Policy be developed, executed and maintained for all implementations of PEDs and Wireless Technology and that all other procedures and policy be followed; and

(6) Ensure that formal exceptions are prepared, signed and approved prior to deployment of PEDs or Wireless Technology that does not comply with this policy.

d The agency Information Systems Security Program Managers will:

(1) Coordinate and manage the security control required for PEDs and Wireless Technology;

(2) Assist agency managers in completing the appropriate checklists, as required;

(3) Routinely monitor agency implementation of these devices and technology to ensure that policy and procedures are followed; advise agency managers in cases of lax security controls or improper use;

(4) Assist in developing exception packages, as required;

(5) Participate in the development of technology implementation plans; and

(6) Update the Overall Agency Security Plan to reflect the funding and planned implementation of PEDs and Wireless Technology.

e The agency Systems or Network Administrators will:

(1) Provide appropriate administrative access and permissions for these PEDs and Wireless Technology based job requirements;

(2) Install encryption, VPN Technology and require strong authentication for these devices, especially in cases where Sensitive But Unclassified (SBU) information will be transmitted or stored;

(3) Install standardized configurations, strict security features, profiles and disable modems;

(4) Routinely patch and update PEDs and check devices for unauthorized software or copyrighted material; and

(5) Verify appropriate security controls are in place using the appropriate checklists.

-END-

Table 1: Checklist for Wireless Local Area Networks (LAN)

Agency ____

Description	**Y/N**	**Info New/Updated**	Comments
Management Considerations			
1. Develop an agency security policy that addresses the use of wireless technology, including 802.11. 2. Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology. 3. Perform a risk assessment to understand the value of the assets in the agency that need protection. 4. Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become available (prior to purchase). 5. Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture. 6. Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency. 7. Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers). 8. Complete a site survey to measure and establish the AP coverage for the agency. 9. Take a complete inventory of all APs and 802.11 wireless devices. 10. Ensure that wireless networks are not used until they comply with the agency's security policy. 11. Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate. 12. Place APs in secured areas to prevent unauthorized physical access and user manipulation.			

Technical Considerations			
1. Empirically test AP range boundaries to determine the precise extent of the wireless coverage. **Status** 2. Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends). 3. Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people. 4. Restore the APs to the latest security settings when the reset functions are used. 5. Change the default SSID in the APs. 6. Disable the broadcast SSID feature so that the client SSID must match that of the AP. 7. Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products. 8. Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference. 9. Understand and make sure that all default parameters are changed. ! 10. Disable all insecure and nonessential management protocols on the APs. 11. Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy feature. 12. Ensure that encryption key sizes are at least 128-bits or as large as possible. 13. Make sure that default shared keys are periodically replaced by more secure unique keys. 14. Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs). 15. Install antivirus software on all wireless clients. 16. Install personal firewall software on all wireless clients. 17. Disable file sharing on wireless clients (especially in untrusted environments). 18. Deploy MAC access control lists. 19. Consider installation of Layer 2 switches in lieu of hubs for AP connectivity. 20. Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications. 21. Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers. 22. Fully test and deploy software patches and upgrades on a regular			

basis. 23. Ensure that all APs have strong administrative passwords. ! 24. Ensure that all passwords are being changed regularly. ! 25. Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI. 26. Ensure that the “ad hoc mode” for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor. 27. Use static IP addressing on the network. 28. Disable DHCP. 29. Enable user authentication mechanisms for the management interfaces of the AP. **s** 30. Ensure that management traffic destined for APs is on a dedicated wired subnet. 31. Use SNMPv3 and/or SSL/TLS for Web-based management of APs.			
Operational Considerations			
1. Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended. 2. Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol. 3. Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information. 4. Consider other forms of authentication for the wireless network such as RADIUS and Kerberos. 5. Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity. 6. Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity. 7. Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features. 8. Enable utilization of key-mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys. 9. Fully understand the impacts of deploying any security feature or product prior to deployment. 10. Designate an individual to track the progress of 802.11 security			

products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology. 9. Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features. 10. When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc. 11. If the access point supports logging, turn it on and review the logs on a regular basis.			

Evaluation performed by: ________________________________ Date: ___________________

General comments:

Table 2:
Bluetooth Checklist

Agency ____

Description	Y/N	Info New/Updated	Comments
Management Considerations			
1 Develop an agency security policy that addresses the use of wireless technology including Bluetooth technology. 2 Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology (i.e., Bluetooth). 3 Perform a risk assessment to understand the value of the assets in the agency that need protection. 4 Perform comprehensive security assessments at regular intervals to fully understand the wireless network security posture. 5 Ensure that the wireless "network" is fully understood. With piconets forming scatter-nets with possible connections to 802.11 networks and connections to both wired and wireless wide area networks, an agency must understand the overall connectivity. Note: a device may contain various wireless technologies and interfaces. 6 Ensure external boundary protection is in place around the perimeter of the building or buildings of the agency. 7 Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers). 8 Ensure that handheld or small Bluetooth devices are protected from theft. 9 Ensure that Bluetooth devices are turned off during all hours when they are not used. 10 Take a complete inventory of all Bluetooth-enabled wireless devices. 11 Study and understand all planned Bluetooth-enabled devices to understand any security idiosyncrasies or inadequacies.			

Technical Considerations			
1. Change the default settings of the Bluetooth device to reflect the agency’s security policy. 2. Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the agency. 3. Ensure that the Bluetooth “bonding” environment is secure from eavesdroppers (i.e., the environment has been visually inspected for possible adversaries before the initialization procedures during which key exchanges occur). 4. Choose PIN codes that are sufficiently random and avoid all weak PINs. 5. Choose PIN codes that are sufficiently long (maximal length if possible). 6. Ensure that no Bluetooth device is defaulting to the zero PIN. ! 7. Configure Bluetooth devices to delete PINs after initialization to ensure that PIN entry is required every time and that the PINs are not stored in memory after power removal. 8. Use an alternative protocol for the exchange of PIN codes, e.g., the Diffie-Hellman Key Exchange or Certificate-based key exchange methods at the application layer. Use of such processes simplifies the generation and distribution of longer PIN codes.			
Operational Considerations			
1. Ensure that combination keys are used instead of unit keys. 2. Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e., no Security Mode 1). 3. Ensure that encryption is enabled on every link in the communication chain. 4. Make use of Security Mode 2 in controlled and well-understood environments. 5. Ensure device mutual authentication for all accesses. 6. Enable encryption for all broadcast transmissions (Encryption Mode 3). 7. Configure encryption key sizes to the maximum allowable. 8. Establish a “minimum key size” for any key negotiation process. 9. Ensure that portable devices with Bluetooth interfaces are configured with a password to prevent unauthorized access if lost or stolen. 10. Use application-level (on top of the Bluetooth stack) encryption and authentication for highly sensitive data communication. For example, an			

IPSec-based Virtual Private Network (VPN) technology can be used for highly sensitive transactions. 11. Use smart card technology in the Bluetooth network to provide key management. 12. Install antivirus software on intelligent, Bluetooth-enabled hosts. ! 13. Fully test and deploy software Bluetooth patches and upgrades regularly. 14. Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI. 15. Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity. 16. Fully understand the impacts of deploying any security feature or product prior to deployment. 17. Designate an individual to track the progress of Bluetooth security products and standards (perhaps via the Bluetooth SIG) and the threats and vulnerabilities with the technology. 18. Wait until future releases of Bluetooth technology incorporate fixes to the security features or offer enhanced security features.			

* Requirements added as result of OIG audit

Evaluation performed by: _________________________________ Date: ___________________

General comments:

Table 3:
Personal Electronic Device (PEDS) Assessment Guide

This assessment should be completed by the Agency's ISSPM or designated alternate in conjunction with the Agency Assessment Checklist. Answer all questions. Provide supplemental information as appropriate. All "No" and "Partial" answers must include supplemental information (such as the given reason why the requirement cannot be met) and an action plan that describes how the requirement will be met, as well as a schedule for completion of the plan. Typically, this would be done by developing the action plan in this document and reflecting this in the security plan for the agency.

Agency/System Identification:

Agency (Agency, Office, Bureau, Service, etc.):	
Address	
Date of last Assessment:	

Test Number: **1**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Basic Policy Procedures for Personal Electronic Devices (PED)			
Resources Required:	Local policies for PED systems.		
Personnel Required:	Systems Administrator/Information Security Personnel		
Objectives:	To determine if general policies and procedures are established to control the use of PED systems in the USDA.		
Procedure Description: (Summary)	Verify that policy is in place addressing the use of USDA owned and privately owned PED systems, and to verify that appropriate security measures are taken when connecting PED systems to USDA resources.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Are policies established authorizing personnel to use PED systems?	Written policy establishes policy for personnel to use PED systems to accomplish work related tasks.		
2.	Are policies established to authorize connectivity between PED systems and USDA ADP resources (Remote and direct connect)?	Written policy authorizes personnel to access USDA ADP resources using PED systems.		
3.	Are policies established for requesting access to USDA ADP resources using PED systems?	Written policy addresses procedures for requesting access to USDA ADP resources using PED systems. Procedures should include a systematic process of requesting		
4.	Do policies address functionality and performance standards for PED systems?	Written policy addresses minimum and authorized functionality and		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		performance standards for PED systems (I.E. CPU speed, RAM requirements, storage space, modem requirements, operating system requirements).		
5.	Are adequate PED security standards for both systems administrators maintaining Remote Access Services (RAS) and individual users addressed in USDA policy?	Written policy address adequate security standards used by both systems administrators and users of PED systems.		
6.	Do policies address use of privately owned PED systems to access USDA ADP resources?	Written policy authorizes personnel to use privately owned PED systems to access USDA ADP resources.		
7.	Are training standards established for PED usage and security?	Written training plans address PED usage and security procedures. At a minimum, training programs should address basic security fundamentals, physical security, access procedures, request for use procedures, and course of action plans for lost or stolen PED systems.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
8.	Are written policies established for the accountability, disposal, maintenance, and safeguarding of PED systems?	Written policy addresses procedures for accounting for, disposing of, and maintaining of PED systems.		
9.	Do written policies authorize PED system access to USDA ADP resources through outside internet service providers?	Written policy addresses the use of privately acquired service providers to access USDA ADP resources.		
10.	Do written policies address procedures for personnel to access RAS with PED systems?	Written policy addresses step-by-step procedures for personnel to access USDA ADP resources using remote access.		
11.	Are procedures outlined in the ADP incident response plan for lost or stolen PED systems?	Incident response plans should include immediate steps to take in the event of a reported lost or stolen PED system. At a minimum, the plan of action should include immediate closure of the users account, accessing the amount of information lost with the system, and procedures for obtaining a user incident report.		
12.	Have legal concerns regarding search and seizure of privately owned PED systems been addressed through legal services?	A legal opinion regarding the search and seizure of privately owned PED systems is available.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
13.	Are policies and procedures pertaining to PED systems current?	Policies and procedures are up-to-date.		
14.	Are frequent audits and vulnerability tests conducted to determine the efficiency and effectiveness of wireless and RAS security plans?	Frequent audits and vulnerability tests are conducted to ensure that policies are adhered to. In particular, the following areas should be frequently reviewed: user access, access point vulnerabilities, and equipment functionality.		

Comments:

Action Plan:

Test Number: **2**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Remote Access Services (RAS) (Dial-in, VPN, Wireless, Infrared (IrDA)			
Resources Required:	Established remote access.		
Personnel Required:	Network Administrator		
Objectives:	To determine if remote access points are properly configured. To determine if remote access points meet required security standards.		
Procedure Description: (Summary)	Verify remote access point policies and configurations to ensure efficient and secure access by remote users.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Are dedicated resources selected to support the RAS (access points, servers, firewalls, modems, and routers)?	Dedicated resources should be identified for RAS access. Dedicated equipment will help to reduce security risks to systems used by internal users.		
2.	Are adequate security and architecture standards for the RAS published in the written computer support plan?	Adequate security standards are published in local policy and reflect requirements for end-to-end security.		
3.	Are Systems Administrators knowledgeable of wireless technology?	Systems administrators should have an understanding of wireless functionality to include, but not limited to, Wireless Access Protocol, Wireless Equivalent Privacy, Wireless Markup Language, IEEE 802.xx standards, and “Bluetooth” security.		
4.	Is the RAS designed to provide end-to-end security for wireless communication?	Wireless security sets should be configured for end-to-end security including encryption and decryption		
5.	Do systems supporting the RAS meet established functionality and performance	Computers meet local functionality and performance standards. This		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	standards?	would include items such as minimum CPU operating speed, minimum RAM memory, authorized operating systems, and authorized peripherals.		
6.	Do computer architecture plans for RAS support include segmenting equipment in a secure architecture format such as "DMZ"?	Segmenting equipment dedicated to providing RAS support. Dedicating resources to specific functions in support of the RAS decreases the potential for external attacks on local internal resources.		
7.	Are server systems tasked with handling RAS properly configured for only selected services? SMTP Access Points FTP HTTP HTTPS TELNET	Operating systems are configured per local and manufacturers specifications to provide optimum and secure performance. Systems administrators make frequent checks to ensure that operating systems are up-to-date with new security/ software patches.		
8.	Are appropriate server operating systems selected to support VPN and remote dial-in services?	Software and operating system packages should be selected that will provide optimum		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		service for both client and server.		
9.	Are server software applications properly configured to manage RAS?	Servers and software applications are configured to allow only those services designated for remote access.		
10.	Are firewall security systems properly configured for the RAS?	Remote access servers are protected by firewall security. The firewall is configured to allow only authorized traffic through.		
11.	Are router policies properly configured to provide secure wireless and VPN support?	Routing systems are configured according to local and manufacturers specifications to support remote access. Decisions as to the extent of security provided by router support will dictate the required settings. Routers can be configured to allow pass-by of remote authentication procedures or can be configured to handle a portion of the process (Not Recommended)		
12.	Are configuration rules periodically checked for all systems to ensure they continue to meet local policy, manufacturers	Software applications, servers, firewalls, and routers supporting the VPN should be all		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	specifications, and upgraded changes to support security concerns?	checked periodically for upgrades and patches.		
13.	Do systems supporting the RAS have updated virus scan software with updated signatures?	“Strong virus” protection software with updated signatures is installed. Administrators should pay particular attention to procedures for scanning uploaded files from remote clients.		
14.	Are procedures outlined in the incident response plans in the event of systems failures for equipment supporting the RAS?	Course of action plans are in place to handle disruption of services.		
15.	Do RAS authentication protocols meet local security needs?	Authentication protocols should meet local policy requirements. Recommended use of a RADIUS type authentication protocol for wireless.		
16.	Are passwords established according to local policy as to size, content, and period of availability?	Passwords conform to local policy and procedure. Users and systems administrators are required to frequently change their passwords (min 30 days), and follow specific design guidelines per local regulation.		
17.	Are encryption devices	At a minimum,		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	and keys changed out frequently?	encryption keys should be changed every two weeks. Dynamically created keys are preferred over static keys as they can be changed on a per session basis. Where physical devices such as smart cards are used, best practice recommends bi-weekly to monthly changes.		
18.	Do personnel accessing USDA resources through the RAS authorized in writing?	Request forms should contain at a minimum supervisor, systems administrators, and users signatures.		
19.	Does the system administrator maintain a log of personnel authorized to access the RAS?	Systems administrators maintain a copy of the user request form.		
20.	Are frequent checks made of remote access account logs to ensure that unused or expired accounts are removed?	Expired accounts are removed, and a system is established to ensure that users who have departed the USDA are removed from the RAS access list.		
21.	Are personnel allowed access to only those resources required to meet job requirements?	Personnel are restricted to only those resources required to meet task requirements.		
22.	Are personnel restricted from making multiple “same time” connections	Users should not be allowed multiple login capabilities.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	to the RAS?	An exception would be systems administrators who normally use multiple logins for troubleshooting.		
23.	Are dial-in and VPN access times established?	Where resources and support personnel are limited, access times should be established.		
24.	Has a dial-up protocol been selected that will efficiently and effectively support local dial-in requirements?	A dial-in protocol should be selected that will meet dial-in and security requirements.		
25.	Are modem pools established and configured properly to support dial-in access.	Modem pools are established for remote dial-in service based upon demand.		
26.	Are modem access numbers maintained in a secure area, and are numbers unlisted?	Modem access numbers should be kept in a secure location and periodically changed where possible.		
27.	Do systems administrators maintain audit logs for system performance, intrusion detection, and succeeded and failed login attempts, and user access times?	Systems logs are available for review.		
28.	Are external vulnerability scans conducted to determine weak points?	Vulnerability scans are conducted on a regular schedule basis and at a minimum, when systems changes are made.		
29.	Are intrusion detection	Intrusion detection		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	strategies implemented for the RAS?	procedures for remote services are included in the organizational intrusion detection and response plan.		
30.	Are VPN's used in conjunction with Wired Equivalent Privacy procedures to provide additional security?	VPN's are a sound means for creating encrypted and secure transfer of data from local resources to remote clients.		
31.	Are VPN's configured per manufacturer's and local policy standards to obtain optimum security and efficiency for wireless access?	The VPN architecture and configuration should be per local policy and manufacturer recommendations. A poorly configured VPN can leave local resources extremely vulnerable to outside security breaches.		
32.	Are site VPN's used to allow access to local resources by remote field offices?	If properly configured, a site supporting VPN can be an effective and efficient means to provide outside access by trusted agencies or remote USDA field offices.		
33.	Do policies address the development of site VPN's?	Site VPN's require the same if not greater security measures as private connected VPN services. Policies should address restrictions		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		similar to those required of remote single client users.		
34.	Have VPN protocols been selected based upon the type and level of security required (IPsec, PPTP, L2TP, etc.)?	Protocols have been selected based upon needs.		
35.	Are strict restrictions placed on what resources are available to site VPN's?	As with individual client connections, restrictions should be placed on what areas are offered to site VPN users.		
36.	Does the server/firewall architecture supporting the additional encryption/ decryption for inbound site VPN traffic meet standards to manage additional loads?	The encryption/ decryption process for authenticating and transferring data to and from site VPN's is a demanding process that can diminish the effectiveness of systems being used to support local resources.		
37.	Are coherent addressing schemes developed for both remote and local VPN sites?	Addressing schemes are configured to avoid collision of IP addresses during transfer of data.		
38.	Are VPN's providing site service monitored to ensure that they are operating smoothly?	Systems are monitored to ensure that they are functioning properly per local and manufacturers specifications. Substandard functioning VPN's can create additional drain and flaws in local		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		architecture plans.		

Comments:
Action Plan:

Test Number: **3**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Laptop Systems			
Resources Required:	Access to laptop computer systems.		
Personnel Required:	Systems Administrator/Laptop User		
Objectives:	To determine if laptop computers meet USDA requirements for use and connectivity with local area resources.		
Procedure Description: (Summary)	Verify that procedures are in place for the secure use of laptop computers in both a remote and local area setting.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Do laptop computers meet established functionality and performance standards?	Laptop computers meet local functionality and performance standards. This would include items such as minimum CPU operating speed, minimum RAM memory, authorized operating systems, and authorized peripherals.		
2.	Are unused laptop	Laptop computers		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	systems stored in a secure location?	are stored in a secure location.		
3.	Are strict accountability procedures in place with serialized lists for systems and their peripherals?	Itemized lists available showing complete serialized listings of all peripherals and internal components for all laptop systems.		
4.	Are published laptop checkout procedures followed?	Users have completed the required request form for acquiring laptop systems.		
5.	Are laptop systems "scrubbed" of previous user data prior to turn-in?	Prior to turn-in or checkout, laptop systems should be checked to ensure that user profiles, user data files, and "user unique" software applications are removed.		
6.	Are system/application security features pre-configured for the user?	Applications used to access local resources are properly configured.		
7.	Are systems with dial-in/wireless modems pre-configured using the proper configurations?	Modem software is properly configured.		
8.	Are policies established granting users authorization to add peripherals and software?	Policies are in place defining what peripherals and software users can add to laptop systems.		
9.	Are users restricted from making certain system configuration changes?	Policies have been established restricting users to making only configuration		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		changes necessary to accomplish assigned tasks.		
10.	Are data/file synchronization procedures in place and properly configured?	Systems are properly configured for data synchronization.		
11.	Do users receive training on laptop usage and security requirements?	Verification that the user has been trained in basic functionality and data security requirements.		
12.	Do users understand the RAS requirements and procedures?	The user understands all procedures for the “type” of remote access in use. Identified in a signed statement or training attendance form.		
13.	Do users understand authentication procedures to access local resources?	The user understands the proper authentication procedures for accessing local resources through the RAS.		
14.	Is the user required to enter a password to enter the system BIOS area?	Laptop BIOS areas are password protected.		
15.	Is the user required to enter a password to enter the system boot process?	Prior to boot-up, the user must enter a password. Where applicable, some systems include the added feature of securing the hard drive with a password. If available, this feature should also		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		be activated.		
16.	Is the user required to enter a password prior to accessing the operating system/LAN?	Prior to entering the operating system and logging into LAN resources, the user is required to enter a password.		
17.	Are passwords established according to local policy as to size, content, and period of availability?	Passwords conform to local policy and procedure. Users are required to conform to established policy and change passwords per local regulation.		
18.	Does a locally established "Warning Statement" appear during the boot process?	Laptop systems contain a local established "Warning Statement." Example located at Appendix 1.		
19.	Are individual firewall software applications installed?	For added protection, adding a personal firewall program such as "Black Ice Defender", "Zone Alarm", or "Norton Personal Firewall" will add additional protection.		
20.	Are multiple user accounts properly configured on shared systems?	Laptops checked out for use by multiple personnel should have individual profiles created. Profiles should be configured for individual needs and access rights.		
21.	Are only authorized	Only authorized		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	software applications installed?	software applications are installed.		
22.	Are encryption/decryption procedures used when data is stored on the laptop?	Confidential information is stored in an encrypted state.		
23.	Are at least 128-bit algorithms used for data encryption/decryption?	Systems should be equipped with 128-bit encryption capabilities for data encryption.		
24.	Are data files encrypted on a per record basis?	Systems should decrypt only those records being used. If the system were stolen or lost, a would-be thief will have limited access to only the current working document.		
25.	Are users restricted from disabling encryption settings on a per-application basis?	Users should not be allowed to change encryption settings.		
26.	Are system files/directories tagged as “read only”?	System files are marked as read only.		
27.	Are only authorized and up-to-date software applications installed?	Laptop systems contain only software applications approved by local policy. Frequent checks are made for patches and updates.		
28.	Is the required virus protection software installed with an updated signature file?	Laptop systems have the required virus protection software with an updated signature file.		
29.	Is the system	System		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	screensaver/ password combination process activated?	screensaver/password function is enabled.		
30.	Are authentication procedures established for linking to USDA ADP resources through laptop systems?	Mutual authentication is required prior to obtaining access. This requires a clear acknowledgement of both the RAS system and the client system before access is granted.		
31.	Is the user authorized in writing to access USDA resources through the RAS?	Written authorization allowing the user to access USDA resources is required.		
32.	Are users accessing the RAS authorized access into only certain resources?	Remote access should be limited to only those file areas required to accomplish job related tasks.		
33.	Are there established access hours for remote users?	RAS servers are configured to allow access during only authorized times.		
34.	Are system maintenance/ security/functionality records available?	Systems technicians have updated reports of systems maintenance/ security/functionality checks.		
35.	Are systems properly disposed of per local policy?	Laptop systems found to be inoperative per functionality and performance standards are		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		properly sanitized and disposed of per local policy.		
36.	Are users instructed on procedures to take in cases of lost or stolen laptop system?	Users understand the course of action for reporting lost or stolen systems per local policy.		
37.	Are procedures established for allowing personnel to connect internally (from their own office space) to USDA ADP resources using laptop systems?	Written authorization allowing the user to access resources.		
38.	Do local policies require personnel wishing to connect to USDA ADP resources with privately owned laptop systems to receive prior approval?	Personnel requesting to use privately owned laptop systems to connect to resources require the same prior approval as those personnel using organizational issued laptops.		
39.	Are privately owned systems required to meet the same functionality/performance standards as organizational issued laptops?	Policy addressing requirements for personally owned laptop systems listing the minimum acceptable standards.		
40.	Are privately owned laptops systems checked by IT security personnel prior to being authorized connection into USDA ADP resources?	Privately owned laptops systems are checked for serviceability, unauthorized software, virus protection software, password specifications, and to ensure they meet required		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		configuration settings to connect through local resources or external dial-in/VPN.		
41.	Are owners of privately owned laptop systems informed that their systems are subject to periodic security checks?	Personnel using privately owned laptops should be under the same guidelines as organizational issued laptops with regards to periodic security checks to ensure that conformance standards are being met.		
42.	Are the same security requirements established for organizational issued laptops required for privately owned systems?	Users of privately owned laptop systems should have the same security requirements to connect to local resources. This will include the use of authentication procedures to connect, safeguarding of data, only authorized software systems, virus scanning software, etc.		

Comments:
ACTION PLAN:

Test Number: **4**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Wireless Phones with Internet Capability			
Resources Required:	Cellular phone with access rights to local resources.		
Personnel Required:	System Administrator and Cellular Phone User with Internet connection capabilities.		
Objectives:	To determine if cellular phone systems meet USDA requirements for use and connectivity with local area resources.		
Procedure Description: (Summary)	Verify that procedures are in place for the secure use of cellular phone systems in both a remote and local area setting.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Is there an established functionality and performance standard for cellular phone systems?	Cellular phones used for internet/intranet connectivity to USDA resources meet written functionality and performance standards. This would include items such as minimum CPU operating speed, minimum RAM memory, authorized operating systems, and authorized peripherals.		
2.	Are unused cellular phones stored in a secure location?	Unused cellular phones are stored in a secure location.		
3.	Are strict accountability procedures in place with serialized lists for systems and their peripherals?	Itemized lists are available showing complete serialized listings of all peripherals and		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		internal components for all cellular phones.		
4.	Are published cellular phone checkout procedures followed?	Users have completed the required request form for acquiring cellular phones.		
5.	Are systems "scrubbed" of previous user data prior to turn-in?	Cellular phones with storage capabilities should be scrubbed of all data prior to turn-in. Prior to placing a system back into circulation for reissue, all records/data from previous users should be discarded.		
6.	Is there an operating system password requirement for login?	Prior to entering the operating system and logging into LAN resources, the user is required to enter a password.		
7.	Are passwords established according to local policy as to size, content, and period of availability?	Passwords conform to local policy and procedure. Users are required to conform to established policy and change passwords per local regulation.		
8.	Are mutual authentication procedures established for linking in with USDA resources through cellular systems?	Mutual authentication is required to obtaining approval to access.		
9.	Are 128-bit Advanced Encryption Standard algorithms used for data	Systems should be equipped with 128-bit encryption		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	encryption?	capabilities for data encryption.		
10.	Are only authorized and up-to-date software applications installed?	Cellular systems contain only software applications approved by local policy. Frequent checks are made for patches and updates.		
11.	Is the required virus protection software installed with an up-to-date signature?	Cellular phones have the required virus protection software with updated signature files.		
12.	Are system maintenance/ security/functionality records available?	Systems technicians have updated reports of systems maintenance/ security/functionality checks.		
13.	Are policies established restricting users from making certain configuration changes?	Users are authorized to make only minor adjustments to systems, and only those adjustments necessary to accomplish assigned tasks.		
14.	Are policies established granting users authorization to add peripherals and software?	Restrictions are in place showing what peripherals and software users can add to cellular phones.		
15.	Do users receive training on cellular phone usage and security requirements?	Verification that the user has been trained in basic functionality and data security		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		requirements.		
16.	Are security standards established for cellular phone connectivity to USDA ADP resources?	End-to-end and adequate security measures are established for connectivity to local resources.		
17.	Are cellular phone connections to USDA ADP resources authorized through private domain services (Individual VPN services)?	Access to resources is authorized through private domain services following strict guidelines to accomplish organizational tasks.		
18.	Are data synchronization procedures in place and properly configured?	Systems are properly configured for data synchronization.		
19.	Are user profiles properly configured for docked/un-docked status?	User profiles are configured according to manufacturers and local policy specifications.		
20.	Are there established access hours for cellular phones to connect through to the RAS?	Remote access servers are configured to allow access during only authorized times.		
21.	Are system/application security features pre-configured for the user by an experienced technician?	Software and hardware are both pre-configured		
22.	Are users restricted from disabling encryption settings on a per-application basis?	Users should not be allowed to change encryption settings.		
23.	Do systems provide per record decryption capabilities?	Systems should decrypt only those records being used. If the system were		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		stolen or lost, access would be limited to only the most recent working record.		
24.	Are systems properly disposed of per local policy?	Cellular phones found to be inoperative per functionality and performance standards are properly sanitized and disposed of per local policy.		
25.	Are records available showing prior system security/ functionality checks?	Systems technicians have updated reports of systems maintenance/ security/functionality checks.		
26.	Are organizational cellular phone logs checked for authorized activity?	Logs are checked for unauthorized or suspicious usage.		
27.	Are users instructed on procedures to take in cases of lost or stolen cellular phone?	Users understand the course of action for reporting lost or stolen systems per local policy.		
28.	Are systems properly disposed of per local policy?	Cellular phones found to be inoperative per functionality and performance standards are properly sanitized and disposed of per local policy.		
29.	Do local policies require personnel wishing to connect to USDA ADP resources with privately owned cellular phones to	Personnel requesting to use privately owned cellular phone systems to connect		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	receive prior approval?	to local resources require the same prior approval as those personnel using organizational issued cellular phones to connect to resources.		
30.	Are privately owned cellular phone systems required to meet the same functionality/ performance standards as organizational issued cellular phones?	Policy addressing requirements for personally owned cellular phone systems listing the minimum acceptable standards.		
31.	Are privately owned cellular phone checked by IT security personnel prior to being authorized connection into USDA ADP resources?	Privately owned cellular phone are checked for serviceability, unauthorized software, virus protection software, password specifications, and to ensure they meet required configuration settings to connect through local resources or external dial-in/VPN.		
32.	Are owners of privately owned cellular phone systems informed that their systems are subject to periodic security checks?	Personnel using privately owned cellular phones to access local resources should be under the same guidelines as organizational issued cellular phones with		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		regards to periodic security checks to ensure that conformance standards are being met.		
33.	Are the same security requirements established for organizational issued cellular phones required for privately owned systems?	Users of privately owned cellular phone systems should have the same security requirements to connect to local resources. This will include the use of authentication procedures to connect, safeguarding of data, only authorized software systems, virus scanning software, etc.		

Comments:

Action Plan:

Test Number: **5**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Personal Digital Assistant (PDA)			
Resources Required:	A PDA with authorized access rights to local resources.		
Personnel Required:	Systems Administrator/Authorized PDA user.		
Objectives:	To determine if PDA systems meet USDA requirements for use and connectivity with local area resources.		
Procedure Description: (Summary)	Verify that procedures are in place for the secure use of PDA systems in both a remote and local area setting.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Is there an established functionality and performance standard PDA systems?	PDA's used for internet/intranet connectivity to USDA resources meet written functionality and performance standards. This would include items such as minimum CPU operating speed, minimum RAM memory, authorized operating systems, and authorized peripherals.		
2.	Are unused PDA systems stored in a secure location?	Unused PDA systems are stored in a secure location.		
3.	Are strict accountability procedures in place with serialized lists for systems and their peripherals?	Itemized lists are available showing complete serialized listings of all peripherals and internal		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		components for all PDA systems.		
4.	Are published PDA checkout procedures followed?	Users have completed the required request form for acquiring a PDA system.		
5.	Are systems "scrubbed" of previous user data prior to turn-in?	Prior to turn-in or checkout, PDA systems should be checked to ensure that user profiles, user data files, and "user unique" software applications are removed.		
6.	Is there an operating system password requirement for login?	Prior to entering the operating system and logging into LAN resources, the user is required to enter a password.		
7.	Are passwords established according to local policy as to size, content, and period of availability?	Passwords conform to local policy and procedure. Users are required to conform to established policy and change passwords per local regulation.		
8.	Are individual firewall software applications installed?	For added protection, adding a personal firewall program such as "Black Ice Defender", "Zone Alarm", or "Norton Personal Firewall" will add additional protection.		
9.	Are mutual authentication	Mutual		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	procedures using at least 128-bit encryption standards established for connecting with the RAS?	authentication using 128-bit encryption is the standard requirement.		
10.	Are 128-bit Advanced Encryption Standard algorithms used for data encryption?	Systems should be equipped with 128-bit encryption capabilities for data encryption.		
11.	Is confidential information immediately removed from the system clipboard or memo pad?	Systems should not maintain any confidential information in the clipboard or memo pad.		
12.	Are only authorized and up-to-date software applications installed?	PDA systems contain only software applications approved by local policy. Frequent checks are made for patches and updates.		
13.	Is the required virus protection software installed with an up-to-date signature?	PDA systems have the required virus protection software with updated signature files.		
14.	Are system maintenance/ security/functionality records available?	Systems technicians have updated reports of systems maintenance/ security/functionality checks.		
15.	Are policies established restricting users from making certain configuration changes?	Users are authorized to make only minor adjustments to systems, and only those adjustments		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		necessary to accomplish assigned tasks.		
16.	Are policies established granting users authorization to add peripherals and software?	Restrictions are in place showing what peripherals and software users can add to PDA systems.		
17.	Do users receive training on PDA usage and security requirements?	Verification that the user has been trained in basic functionality and data security requirements.		
18.	Are procedures established for allowing personnel to connect internally (from their own office space) to USDA ADP resources using PDA systems?	Written authorization allowing the user to access resources.		
19.	Are PDA connections authorized through private domain services (Individual VPN services)?	Access to resources is authorized through private domain services following strict guidelines to accomplish organizational tasks.		
20.	Are data synchronization procedures in place and properly configured?	Systems are properly configured for data synchronization.		
21.	Are user profiles properly configured for docked/un-docked systems?	User profiles are configured according to manufacturers and local policy specifications.		
22.	Are systems with wireless modems pre-configured	Software and hardware are both		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	using the proper configurations?	pre-configured		
23.	Are there established access hours for remote PDA users?	RAS servers are configured to allow access during only authorized times.		
24.	Are system/application security features pre-configured for the user by an experienced technician?	Software and hardware are both pre-configured		
25.	Are users restricted from disabling encryption settings on a per-application basis?	Users should not be allowed to change encryption settings.		
26.	Do systems provide per record decryption capabilities?	Systems should decrypt only those records being used. If the system were stolen or lost, access would be limited to only the most recent working record.		
27.	Are systems properly disposed of per local policy?	PDA's found to be inoperative per functionality and performance standards are properly sanitized and disposed of per local policy.		
28.	Are records available showing prior system security/ functionality checks?	Systems technicians have updated reports of systems maintenance/ security/functionality checks.		
29.	Are users instructed on procedures to take in cases of lost or stolen PDA system?	Users understand the course of action for reporting lost or stolen systems per		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		local policy.		
30.	Do local policies require personnel wishing to connect to USDA ADP resources with privately owned PDA systems to receive prior approval?	Personnel requesting to use privately owned PDA systems to connect to USDA ADP resources require the same prior approval as those personnel using organizational issued PDA's.		
31.	Are privately owned PDA systems required to meet the same functionality/ performance standards as organizational issued PDA's?	Policy addressing requirements for using a personally owned PDA with minimum acceptable standards.		
32.	Are privately owned PDA systems checked by IT security personnel prior to being authorized connection into USDA ADP resources?	Privately owned PDA systems are checked for serviceability, unauthorized software, virus protection software, password specifications, and to ensure they meet required configuration settings to connect through resources or external VPN.		
33.	Are owners of privately owned PDA systems informed that their systems are subject to periodic security checks?	Personnel using privately owned PDA's should be under the same guidelines as organizational issued PDA's with regards to periodic		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		security checks to ensure that conformance standards are being met.		
34.	Are the same security requirements established for organizational issued PDA's required for privately owned systems?	Users of privately owned PDA systems should have the same security requirements to connect to local resources. This will include the use of authentication procedures to connect, safeguarding of data, only authorized software systems, virus scanning software, etc.		

Comments:
Action Plan:

SUGGESTED PERSONAL USE POLICY

1. Personal PEDs will not be used for official business unless the CIO grants an approved waiver of this policy and procedures.

2. PEDs will be used for official government business

3. Changes will not be made in official system configurations, operating or antivirus software or remote access arrangements except by the agency IT staff.

4. Modems will remain disabled.

5. In absence of electronic verification or auditing, physical inventories of PEDs will be done on an annual basis.

6. During the annual inventory, storage of information will be checked to confirm only required information is maintained and that SBU data is encrypted.

7. During travel, PEDs will be hand carried to prevent damage or theft.

8. The agency contact person will be contacted immediately in case of loss or theft of the PED.

9. PEDs will be returned to the agency on a regular basis for system updates, patches and accountability reasons.

10. Encryption techniques will be used for infrared and wireless transmissions of SBU information or for storage of SBU data.

11. PEDs will be surrendered to the agency or staff office immediately upon transfer, reassignment, resignation or retirement from federal service.

12. Unauthorized software and unauthorized copyrighted or illegal material will not be loaded or stored on PED.

13. Care will be exercised in discussions of sensitive information using wireless technology to prevent inadvertent disclosure of SBU or violations of the Privacy Act.

14. Floppy disks, CD-ROM, and Flash Memory will not be used to download applications or SBU information in violations of security policy.