CHAPTER 5, PART 3
Telework & Remote Access Security

1 BACKGROUND

The existing government-wide telework initiative, formerly called Flexiplace, has been in place since 1990. Flexiplace was established in response to workforce concerns first documented by the Hudson Institute and later by the Department of Labor. The essence of these concerns was the turn-of-the-century drop in the quality of the labor pool and the consequent fear that federal recruitment/retention would not be able to compete with the private sector salaries. The plan was that initiatives such as Flexiplace would help boost the labor market value of a federal government job.

Despite its chronological age, federal telework is still a relatively new program because of its slow evolution in the federal bureaucracy. For purposes of this policy, the terms “telework”, “telecommuting” and Flexiplace are synonymous and interchangeable. Each is defined as a work arrangement in which an employee regularly works at an alternate worksite such as the employee’s home, a telecommuting center, or other alternate worksite. Public Law 106-346, Section 359, requires that each executive agency implement a telework program and establish the goal of 25 percent each year for eligible agency employees to be given the opportunity to telework. 100 percent of eligible employees are to be given the opportunity to telework by the end of 2005. Home-based telework, work at a telecenter or alternate worksite presents unique managerial, organizational, technological and cultural challenges for USDA.

Telecommuting is gaining wide acceptance by all levels of management as a tool with many benefits to the agency. The benefits include: attracting new applicants and retaining current employees; reducing worker’s compensation; reducing sick leave usage and an alternative to relocating employees in crisis or emergency situations. Other benefits include contributing to the community by reducing air pollution and traffic and providing a mechanism to assist employees in balancing work and family life responsibilities. In spite of the many attractive benefits, opening up an organization’s information systems to dial-in and other forms of remote access present significant security risks. One risk is that intruders will be able to access government systems without having to be on site (remote access). Another risk of telecommuting is that government information can be read, and potentially modified, while in transit. Additional risks include the loss of information and resources while they are outside the protective shell of the organization. In a telework environment, USDA needs to implement security controls commensurate with the sensitivity of the information and importance to the mission. Goal One: Introduce no additional risk to the department. Goal Two: Identify remote users adequately; implement the accesses needed to perform official duties and protect USDA IT resources. Goal Three: Identify the Cyber Security Rules of Behavior for managers and employees participating in the Telework Program.

2 POLICY

All USDA agencies and staff offices establishing telework arrangements will review the security issues for each telecommute position in their organization. The Telework Security/IT Checklist Roles and Functions, Table 1, will be used to identify individuals responsible for completing the telework checklist. Each agency will use the Telework Checklist, Table 2, to ensure that they have addressed all relevant Security and Information Technology (IT) issues before any arrangement is finalized. Waivers will be obtained for telework arrangements that do not meet the requirements of this policy. Each job deemed portable will undergo scrutiny to determine the type of information used in the job in terms of mission criticality and sensitivity. Government owned equipment (GOE) will be issued to individuals who work with Sensitive But Unclassified/ Sensitive Security Information (SBU/SSI). SBU/SSI will not be stored on Employee Owned Equipment (EOE) or non-USDA computers used in Telecenters. SBU information may be accessed if required and approved for official duties but will not be saved on these machines. The security requirements of this policy apply to episodic telework arrangements as well.

Policy exception requests must be submitted if EOE will be used in telework arrangements. EOE must be maintained and properly secured by USDA personnel prior to commencement of the arrangement. A waiver will also be submitted if a USDA laptop with SBU is transported into the Telework Center for use during duty hours. Each agency and staff office will ensure that teleworkers have received Computer Security Awareness Training and understand their responsibilities for properly safeguarding GOE. All telework arrangements will be planned in Information Technology (IT) budgets and detailed in the General Support System (GSS) Security Plan used to support the arrangements. Each agency will establish procedures to ensure all US Government property and sensitive but unclassified information residing offsite is retrieved in the event of an employee transfer, resignation, retirement or death.

Agencies and staff offices will establish appropriate remote access arrangements to ensure that access is obtained through secure firewalls/gateways and robust authentication is used. Robust Authentication methods are required for all dial-up connections (dial-in, DSL, Cable Modem) to include PINs or Tokens. Approved authentication procedures for remote users must be established and the remote access service must be located at the outermost perimeter of the USDA De-Militarized Zone (DMZ). SBU/SSI will encrypted using department approved encryption protocols prior to transmission. Secure Socket Layer (SSL) and Virtual Private Network (VPN) tunneling are recommended. Dial-up connections and remote access will be centrally managed by each agency/ mission area to ensure integrity of network security. Individual modems connecting directly to internal networks, systems, or computers are not authorized.

<u>Policy Exception Requirements</u> – 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. <u>Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with an updated timeline for completion</u>. CS will monitor all approved exceptions.

3 RESPONSIBILITIES

a <u>The Associate CIO for Cyber Security</u> will:

(1) Assist agencies and staff offices in the secure implementation of telework and remote access arrangements;

(2) Provide Cyber Security policy and guidance to the Office of Human Capital Management (OHCM) and other activities involved in telework programs; develop checklist tools to assist agencies in security telework and remote access environments;

(3) Review agency and staff office policy exception requests concerning this policy in a timely manner;

(4) Review telework and remote access provisioning in Security Plans for agency General Support Systems and Security Budgets for sufficiency; and

(5) Conduct periodic reviews of agency telework and remote access arrangements to ensure they comply with this policy.

b <u>Agency Chief Information Officer will:</u>

(1) Implement this policy, including use of the checklists, into any agency Telework or Remote Access arrangements;

(2) Ensure that each position identified for telework is screened for information sensitivity and mission criticality;

(3) Plan telework program expenses and needed upgrades as part of the agency IT Budget and System Life Cycle;

(4) Ensure that GSS Security Plans are updated to include all agency Telework and Remote Access arrangements, as appropriate;

(5) Ensure that telework and remote access based Computer Security Awareness Training is provided to employees and managers participating in this program;

(6) Complete and retain a Telework/IT Security Checklist for all agency telework and remote access arrangements;

(7) Ensure that all existing telework and remote access arrangements are reviewed again the Checklist and that security vulnerabilities identified are corrected; and

(8) Take action to request a formal waiver for arrangements that do not comply with this policy.

c Agency Information System Security Program Managers (ISSPM) will:

(1) Support this policy and assist agencies or staff offices in completing the Telework/IT Security Checklist;

(2) Review all existing telework and remote access arrangements periodically and work with the managers to ensure that they are secure;

(3) Assist in the set up of new arrangements to provide security guidance, as required;

(4) Update the GSS and Overall Agency Security Plans to accurately reflect telework and remote access arrangements, as required; and

(5) Assist in the preparation of agency waivers, as required.

-END-

Table 1: Telework Security/IT Checklist Roles & Functions

GROUP	**DESCRIPTION**	**ROLE & FUNCTIONS**
Executives	Senior Mgmt, CIOs	Provide support and Buy-In Remove Telework Barriers Approve IT Funding
Program/Functional Mgrs.	Business Owners/Program Mgrs.	Plan Telework/IT Budget Complete Checklist (Gen.) with supervisor
Security & Investment Managers	Info. Sys. Sec. Prog. Mgrs Investment Managers Budget Analysts	Assist AIS personnel in completing Checklist; train teleworkers & managers; update GSS & Overall Security Plans; estimate security costs; ensure security controls are in place, review final checklist for completeness Update I-TIPS Overall IT Program (Security Costs) Participate in cost development
IRM, Automated Info. Sys. Mgrs.	System Owners System Administrators/Devel. HELP Desk Technicians	Provision hardware, software Configure system Develop security controls with ISSPM Complete Checklist (each arrangement)
End User	Teleworkers	Adhere to telework security requirements; protect information and equipment
Telework Managers	Functional Supervisor	Perform Job Suitability Review Determine Information Sensitivity Brief on Privacy Restrictions Complete Checklist (General) Arrange Security & IT Training

Table 2

TELEWORK SECURITY/IT CHECKLIST

In a Telework Environment, USDA needs to implement Security Controls commensurate with the sensitivity of the information and importance to the mission. Goal One: Introduce no additional risk to the department. Goal Two: Identify remote users adequately; implement the accesses needed to perform official duties and protect USDA IT resources. Goal Three: Identify the Cyber Security Rules of Behavior for managers and employees participating in the Telework Program.

Date:	**General Support System Used:**
Agency or Staff Office Name:	**Cyber Security POC:**

Checklist Questions	**YES**	**NO**	**PENDING or NOT APPLIC.**	**WAIVER RECV'D**	**COMMENTS**
GENERAL					
** **(Job Sensitivity, Privacy, Planning and Budget)**					
• Has the GOE and services for telework been included or planned in the IT Budget? If not is surplus equipment available? Does long range planning include funding to phase out use of employee owned equipment (mandatory requirement)?					
• Has the Security Plan for the General Support System (s) used to support this arrangement and Overall Agency Program Plan been updated to reflect the following? Physical Security, Encryption requirements, Office Automation Support					

Checklist Questions	YES	NO	PENDING or NOT APPLIC.	WAIVER RECV'D	COMMENTS
(setup, maintenance, monitoring) requirements, Software requirements, Identification of Operating System, Connection Type (Dial, DSL, Cable Modem), Protection of Official Files, Identification of system's accessing the USDA Networks					
• Has the Telework Program been integrated in the normal system development life cycle for the agency? Has this program been integrated into the agency's Overall Security Program, including vulnerability assessments? Have the appropriate General Support System (GSS) and Major Applications Security Plans, including risk assessments been updated to include the Teleworkers?					
• Has management reviewed the job duties, responsibilities and authority to determine the level of information sensitivity in the telework assignments? In addition, have Privacy requirements been identified and documented for the arrangement? NOTE: AS A REMINDER DR 3440-2, CONTROL AND PROTECTION OF SENSITIVE SECURITY INFORMATION AND OCIO CYBER SECURITY GUIDANCE (CS-023) REGARDING SENSITIVE BUT UNCLASSIFIED INFORMATION DEFINE SECURITY AND PROTECTION REQUIREMENTS. Jobs involving classified information are not eligible for telework or remote access arrangements.					
• Does the teleworker understand that there is					

Checklist Questions	**YES**	**NO**	**PENDING or NOT APPLIC.**	**WAIVER RECV'D**	**COMMENTS**
neither expectation of nor Right to Privacy on the computer used to perform official functions while they are at their telework location during duty hours? Do they understand that their personal computer can be subject to seizure for inappropriate activities such as Pornography or Copyright Violations that are done during work hours and while connected to USDA's networks? Has the employee been trained to recognize and handle SBU/SSI in a telework environment?					
• Will the teleworker access E-mail? If so, all E-mail access needs to be encrypted.					
• Have all proper software licenses been purchased for the workstation? a. Does the agency have Software Management and Software Use policies? b. Does the agency have a Software Acquisition policy? c. Does the agency have a Software Manager?					
• Does the employee understand that access to USDA's networks can be blocked if there is any indication of intentional or unintentional security breaches that affect the overall security posture of the department? SEE NIST 800-46, APPENDIX A					
Government Owned Equipment Arrangements					

Checklist Questions	**YES**	**NO**	**PENDING or NOT APPLIC.**	**WAIVER RECV'D**	**COMMENTS**
• Has GOE been provided if the employee will work on Sensitive But Unclassified/Sensitive Security Information (SBU/SSI)? NOTE: GOE SHOULD USE APPROVED AUTHENTICATION AND IDENTIFICATION METHODS (i.e., smart cards or MAC addresses).					
• Has the selection of wireless and other home communication technologies been determined after consideration of security requirements? NOTE: Wireless (VOICE and DATA) and other home technologies have been determined to be insecure and represent a threat to the USDA network. Care should be exercised in use of these technologies and assistance should be requested from Cyber Security, if an agency is in doubt concerning security of new technology. Wireless data communication should be encrypted using Wired Equivalent Privacy (WEP), 802.11b or 802.11g encryption standards and additional encryption methods such as Virtual Private Networking (VPN) or Secure Socket Layer (SSL).					
• Will the employee require a dedicated telephone/modem line? Is a direct Internet connection required? If so, then a firewall must be planned for the workstation and the network. (NIST 800-46 recommends both personal and network firewall devices.) Personal firewall features and configurations shall be standardized and documented in the agency Security Plan.					

Checklist Questions	YES	NO	PENDING or NOT APPLIC.	WAIVER RECV'D	COMMENTS
Has the department's Virtual Private Network (VPN) technology been considered for transport of all SBU/SSI information? If not, has encryption software been planned for the workstation?					
• Has a locked file cabinet been identified/provided to secure SBU/SSI files, records, papers or electronic media?					
• Have GOE Operating Systems (OS) been configured to limit vulnerability intrusion? Browser plugins on all telework devices shall be limited to only those required by the teleworker to perform official functions. Persistent cookies should be disabled or selectively removed. Has the operating system been configured to increase security? NOTE: THIS INCLUDES LATEST ANTIVIRUS SOFTWARE AND VIRUS DEFINITION FILES, SPYWARE REMOVAL TOOLS, FIREWALLS, PASSWORD PROTECTION FOR DESKTOP AND SCREENSAVER PASSWORD PROTECTION, ENCRYPTION SOFTWARE (AS APPROPRIATE) AND USDA AUTHORIZED SOFTWARE, NT FILE SYSTEM (NTFS).					
• Have arrangements been made with the agency Office Automation (OA) staff to provide ongoing maintenance, system/security patches/upgrades, repair and replacement of the GOE? Is the teleworker capable and willing to assist the					

Checklist Questions	**YES**	**NO**	**PENDING or NOT APPLIC.**	**WAIVER RECV'D**	**COMMENTS**
OA staff in following instructions for support of the workstation?) Does the agency have a mechanism in place to uniquely identify telework GOE on the network?					
• Does the teleworker understand that GOE is limited to use for "Official USDA Business" only?					
• Has the GOE issued been inventoried and accounted for? If so, has the Teleworker signed an agreement to voluntarily return the GOE upon departure from USDA employment?					
• Has the teleworker(s) been given Security Awareness Training emphasizing the security requirements of their flexible work arrangement? Is that training repeated at least annually? Did the Teleworker sign an acknowledgement document indicating that they understand all requirements and responsibilities? See NIST 800-46, Appendix A					
Employee Owned Equipment Arrangements					
• Has management reviewed and certified that employee duties do not include SBU/SSI information? **EMPLOYEE OWNED EQUIPMENT (EOE) CANNOT BE USED TO STORE SBU/SSI INCLUDING EMAIL**. HOWEVER, THE VIEWING OF EMAIL (AND ATTACHMENTS) AND/OR SBU/SSI INFORMATION MAY OCCUR USING A SSL WEB BROWSER OR APPROVED TERMINAL SERVICES					

Checklist Questions	**YES**	**NO**	**PENDING or NOT APPLIC.**	**WAIVER RECV'D**	**COMMENTS**
SOLUTION WITH ENCRYPTION.					
• Has the cost of supporting the EOE been included in the agency budget? Has the agency installed the latest USDA authorized Antivirus Software, Firewall Software (if necessary)? Has the Operating System been configured to match USDA security options: Have all configurations been verified by the agency IT staff? Note: Windows 95 and Windows 98 is not a suitable operating system for EOE.					
• Has employee's Operating System (OS) been configured to limit vulnerability to intrusion?					
• Is the employee willing and capable of doing installations, maintenance and repair of personal workstation equipment? (Those functions normally handled by the OA staff) Does the agency have a mechanism in place to uniquely identify telework EOE on the network? In the case of employees who are using their own Internet Service Provider, has the agency determined that there is no prohibition by the provider on business use (telework) of this service?					
• Does the employee understand that while E-mail can be access remotely, after Web Browser is optioned for security, no E-mail files can be downloaded and saved to the workstation?					
• Has the employee partitioned space on their workstation for Official Business files that is accessible only to the teleworker. NOTE: THIS REQUIRES NT FILE SYSTEM OR					

Checklist Questions	**YES**	**NO**	**PENDING or NOT APPLIC.**	**WAIVER RECV'D**	**COMMENTS**
EQUIVALENT.					
• Will the employee require a dedicated telephone/modem line? Is a direct Internet connection required? If so, then a firewall must be planned for the workstation and the network. (NIST 800-46 recommends both personal and network firewall devices.) Has the department's Virtual Private Network (VPN) technology been considered for transport of all SBU/SSI information? If not, has encryption software been planned for the workstation?					
• Does the employee have an approved Anti-virus software program running on their computer? If so are the latest virus definitions used?					
• Has the teleworker(s) been given Security Awareness Training emphasizing the security requirements of their flexible work arrangement? Is that training repeated at least annually? Did the Teleworker sign an acknowledgement document indicating that they understand all requirements and responsibilities?					
• Has the system been scanned to detect spyware and parasite software packages? Has a spyware removal tool been installed? Has the teleworker certified in writing that no Peer-to-Peer software is installed on their personal computer? Will the system be made available for periodic scanning as required by DM 3500-2, Vulnerability Scan Procedures?					
• Does the telework agreement include a					

Checklist Questions	**YES**	**NO**	**PENDING or NOT APPLIC.**	**WAIVER RECV'D**	**COMMENTS**
provision for the teleworker to assume liability for misuse of the personal computer used to perform official functions? See NIST 800-46, Appendix A					
Telework Center Arrangements					
In a Telework Center, follow the instructions for set up of GOE in terms of Security considerations, with the following additional questions.					
• Does the teleworker understand the need to delete any SBU/SSI files downloaded to the Center computer at the end of the day? SBU/SSI needs to be guarded from inadvertent disclosure to the next teleworker.					
• Has the teleworker been placed in an area that affords privacy to prevent others from observing information on the worker's screen? This is a mandatory consideration if the work is considered SBU/SSI information.					

CYBER SECURITY REFERENCES

DM3525-002, Chapter 5, Part 2, Internet Use and Copyright Restrictions

DM 3530-004, Chapter 6, Part 4, Firewall Technical Security Standards

DM 3530-005, Chapter 6, Part 5, Security Encryption Standards

DM 3545-001, Chapter 9, Part 1, Computer Security Awareness and Training

DM 3550-002, Chapter 10, Part 2, Sensitive But Unclassified (SBU) Information Protection

DM3565-001, Chapter 14, Part 1, Annual Security Plans for Information Technology (IT) Systems

NIST Special Publication 800-46, Security for Telecommuting and Broadband Communications, August 2002