GSA Office of Governmentwide Policy

Information Technology and Telecommunications Guidelines for Federal Telework and Other Alternative Workplace Arrangement Programs

Purpose: This bulletin establishes guidelines for implementing and operating telework and other alternative workplace arrangement (AWA) programs through the efficient and effective use of information technology and telecommunications.

Expiration Date: This bulletin will remain in effect indefinitely until specifically cancelled.

Guidelines for IT and Telecommunications for Federal Telework and Other AWA Programs

I. Basic Equipment Recommendations

a. An agency may provide employees with computer equipment, associated peripheral equipment (*e.g.*, printer, copier, scanner, facsimile), telecommunications, and associated technical support for the implementation and expansion of telework in the Federal Government. The agency may provide the level and configuration of these resources that it deems necessary for mission accomplishment. To make this determination, an agency may consider factors such as the teleworker's job requirements, frequency of telework, and other work-related parameters. In addition, the agency is advised to review the 2006 Telework Technology Cost Study, which concluded that the One Computer Model is advantageous from both a value added cost perspective and from a multi-purpose perspective. The 2006 Telework Technology Cost Study is located in the GSA Telework Library at **www.gsa.gov/telework.**

b. An agency may establish a policy that provides that teleworkers utilize their respective alternative worksite equipment and associated technical support for continuity of operations (COOP) purposes. In addition to facilitating COOP responsiveness, this dual-purpose use of telework resources can (1) increase the agency's return on investment for the cost of those resources, as well as (2) reduce agency COOP costs. The NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, provides instructions, recommendations, and considerations for government IT contingency planning (see **csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf**), and NIST Special Publication 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, provides additional recommendations and related information (see **csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf**).

c. An agency may provide teleworkers with equipment that is no longer needed for its original purposes, such as when equipment is replaced during a refresh cycle. This strategy can maximize the value of federal IT investments through the 're-use' or 're-purposing' of equipment to help implement or expand an agency telework program. In accordance with 41 C.F.R. §§§ 102-36.30 and 102-36.35, even though equipment may no longer be used for its original purpose, employee, or location, the agency must determine if the equipment can serve other agency uses, such as in alternative worksites. The equipment officially does not become excess until the agency determines that the agency has no further use for the equipment, including use in main or alternative worksites.

II. Telecommunications and Internet Services

a. Public Law 104-52, § 620, 31 U.S.C. § 1348 note, authorizes agencies to use appropriated funds to install telephone lines and necessary equipment, and to pay monthly charges, in any private residence of an employee who has been authorized to work at home in accordance with the guidelines issued by the Office of Personnel Management. The head of the department, division, bureau, or office must certify that adequate safeguards against private misuse exist, and that the service is necessary for direct support of the agency's mission. This authority includes facsimile machines, internet services, broadband access, e-mail services, Voice over Internet Protocol equipment and services, desktop videoconference equipment and services, and, in general, any other telecommunications equipment and services the agency deems needed by individuals working in any authorized alternative worksite**.**

b. As described above, agencies are authorized to provide and/or pay for installation and operation of a dedicated voice line for teleworker use at an alternative worksite. Regardless of whether or not, or the extent to which, an agency provides resources for such a line, a dedicated voice line is recommended so that (1) managers, co-workers, clients, and/or other work-related personnel are not prevented from reaching a teleworker due to the tying up of a teleworker's phone line by online or other data use activity and (2) teleworkers do not put themselves at risk by tying up their personal voice line with business activity. Agencies may carry out this recommendation through the use of landlines and/or cell phones.

c. The authorities described above also authorize agencies to pay equipment costs, usage fees, and service charges for all authorized methods of connectivity (*e.g.*, dial-up, high-speed, wireless, satellite) utilized for official business at alternative worksites.

d. Factors such as teleworker job requirements, telecommunication service availability, and quality and cost of service at the alternative worksite should be used to determine teleworker connectivity. Various types of high-speed telecommunication services are available in many areas and not in others. Speed, performance, reliability, and cost are factors to consider when determining how to meet connectivity requirements. In some instances, for example, in which an analog telephone line is the only available connectivity solution, the resulting dial-up access may be sufficient, depending on the teleworker's job requirements. Agency policies should address the equitable provisioning of these resources. It is recommended that agencies implement more than one type of connectivity because of variations in service availability, teleworker job requirements and modes of operation, and other factors that impact the type of connectivity required.

e. Security and connectivity requirements vary according to whether or not a teleworker's job requires interacting with an agency's centralized IT systems. Teleworkers who do not require interaction with an agency's centralized IT systems may be able to telework successfully using only e-mail and telephone contact with the office, without logging into the agency system. For example, a user who teleworks one or two days per week, and whose job consists largely of writing and document preparation, may never need to log in to agency systems from an alternative worksite. Provided that they are not sensitive or do not contain personally identifiable information, documents can be e-mailed back and forth between the agency system and the user's e-mail account. In this scenario, e-mailing a document from an alternative worksite to the agency system does not require the teleworker to interact with the system. In general, there are many firewall implementations that use an electronic mail proxy to allow access to the files on a protected system without having to directly access that system. Alternatively, the teleworker may physically transport the documents on portable storage media.

When teleworkers need to access the agency's centralized IT systems, it is necessary, at a minimum, to allow for remote logins from the alternative worksite computer. In this case, strong authentication (at least "two factor authentication") is required to minimize the vulnerabilities in providing external access. This solution is sufficient for teleworkers requiring minimal access to internal resources, such as some types of intranet access. NIST provides detailed guidance on this issue in Special Publication 800-63, its document on electronic authentication, and agencies are advised to review and comply with this guidance (see **csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf**).

Some teleworkers, however, may require more involved access to internal resources. In this case, a more secure solution, such as a VPN, should be used. A VPN can provide a high level of security and convenience for the teleworker. Encryption protects all interaction between the offsite computer and the main office, so that in many ways the user's offsite computer is as secure as one on the main office local network. This approach makes it possible to allow offsite users to operate applications such as scheduling, budget analysis, or other complex systems from the alternative worksite. The tradeoff for a VPN is in cost and complexity of administration. Note also that operating a VPN does not guarantee protection from viruses and e-mail worms. The agency Chief Information Officer (CIO), in conjunction with other agency officials (such as telework and/or human resources management policy providers), should examine job requirements and provide policy, guidance, and appropriate secure system access.

f. Agencies should be aware and take advantage of the potential utility and other benefits of audio teleconference and web conference capabilities for their respective telework programs. These capabilities can be excellent tools to facilitate productivity, agency cost savings (from reduced travel expenses, for example), and other benefits for all employees, in general, and for teleworkers, in particular. Agency telework program planners and implementers should be aware of and utilize the relevant telecommunications products, tools, information, and services that are available in their existing contracts and/or from service providers, such as the GSA Global Account Manager (**www.gsa.gov/networksvcs**), or equivalent sources and providers.

III. Security

a. According to an Office of Management and Budget (OMB) memorandum entitled "Protection of Sensitive Agency Information," dated June 23, 2006, which addresses the lack of physical security controls when information is removed from or accessed from outside the agency location, agencies should implement the NIST checklist for protection of remote information (see **www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf**), and:

(1) Encrypt all data on mobile computers and devices that carry agency data, unless the agency determines that the data are non-sensitive;

(2) Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;

(3) Use a "time-out" function requiring user re-authentication after thirty (30) minutes of inactivity for remote access and mobile devices; and

(4) Log all computer-readable data extracts from databases holding sensitive information and verify that each such extract has been erased within ninety (90) days or that its use is still required.

b. FISMA delegates to NIST the responsibility to develop detailed information security standards and guidance for federal information systems, with the exception of national security systems. Agency personnel involved in planning, implementing, and/or operating telework programs should consult the website of NIST's Computer Security Resource Center (see **csrc.nist.gov**) for up-to-date information and guidance on secure computing. Listed below are key documents that can assist in the implementation of secure telework operations.

(1) Security for Telecommuting and Broadband Communications (NIST Special Publication 800-46 (2002)), assists organizations in addressing telework security issues by providing recommendations on securing a variety of applications, protocols, and networking architectures (see **csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf**).

(2) Recommended Security Controls for Federal Information Systems (NIST Special Publication 800-53, Rev. 1 (2006)), provides important guidance on security controls selection and specification, including information on Media Protection, Certification, Accreditation, Security Assessments, Identification and Authentication families, updating security controls, and

the use of external information systems (see **csrc.nist.gov/publications/nistpubs/index.html#sp800-53-Rev1**).

(3) Information Security Handbook: A Guide for Managers (see **csrc.nist.gov/publications/nistpubs/#sp800-100**).

(4) Security Management and Guidance (see **csrc.nist.gov/focus_areas.html#smag**).

c. Agencies should review and comply with applicable controls and guidance, especially sections on portable devices, remote access, and external IT systems set forth in NIST Special Publication 800-53, Rev. 1, when developing telework program implementation guidelines. Listed below are selected controls and guidance from NIST Special Publication 800-53, Rev. 1:

(1) Access Control for Portable and Mobile Devices (*e.g.*, notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations):

i. Establish usage restrictions and implementation guidance for organization-controlled portable and mobile devices;

ii. Authorize, monitor, and control device access to organizational information systems;

iii. Require that portable and mobile device access to organizational information systems be in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (*e.g.*, malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (*e.g.*, wireless, infrared).

(2) Remote Access:

i. Authorize, monitor, and control all methods of remote access to the information system. Remote access controls should be applied to all information systems other than public web servers or systems specifically designed for public access;

ii. Restrict access achieved through dial-up connections (*e.g.*, limit dial-up access based upon source of request) or protect against unauthorized connections or subversion of authorized connections (*e.g.*, using VPN technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication;

iii. Employ automated mechanisms to facilitate the monitoring and control of remote access methods;

iv. Use cryptography to protect the confidentiality and integrity of remote access sessions;

v. Control all remote accesses through a limited number of managed access control points; and

vi. Permit remote access for privileged functions only for compelling operational needs and document the rationale for such access in the security plan for the information system.

(3) Use of External Information Systems Control:

i. Establish terms and conditions for authorized individuals to: (A) access the information system from an external information system; and (B) process, store, and/or transmit organization-controlled information using an external information system. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (*e.g.*, individuals accessing federal information through public interfaces to organizational information systems).

ii. Establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions should address, at a minimum: (A) the types of applications that can be accessed on the organizational information system from the external information system; and (B) the maximum Federal Information Processing Standard 199 security category of information that can be processed, stored, and transmitted on the external information system.

iii. Prohibit authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (A) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (B) has approved information system connection or processing agreements with the organizational entity hosting the external information system.

IV. Privacy

Agencies should review the OMB memorandum entitled "Safeguarding Personally Identifiable Information," dated May 22, 2006, and ensure that their respective telework technology infrastructures, practices and procedures are in compliance with that memorandum and the Privacy Act. The OMB memorandum reemphasizes the many responsibilities under law and policy to safeguard sensitive personally identifiable information appropriately. Among other things, the Privacy Act requires each agency to establish:

Rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance; [and] appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. (5 U.S.C. § 552a(e)(9)-(10))

V. Training

Teleworkers should receive adequate training on the use of IT systems and applications needed for effective job performance. This should include any specialized training associated with (1) effective use of remote access and other resources needed for working remotely, and (2) security awareness and responsibility. In addition, agencies are encouraged to provide opportunities for teleworkers to practice in a telework situation.

VI. Technical Support

a. Agencies should (1) provide adequate and effective Help Desk support for teleworkers, and (2) require Help Desk personnel to possess the skills, procedures, and resources needed for resolving teleworker issues, such as remote access hardware and software issues.

b. Where feasible and applicable, agencies should provide routine systems maintenance via remote transmission procedures such as transmitting ("pushing") software and system upgrades out to the teleworker's alternative worksite as opposed to requiring the teleworker to bring a computer to the agency worksite for maintenance.

VII. Additional References and Resources

a. Office of Management and Budget (see **www.whitehouse.gov/omb/memoranda/m03-18.pdf**).

b. Government Accountability Office (see **www.gao.gov**).

VIII. Commonly Asked Questions

a. *May an employee use his or her own personal computer equipment to conduct official business from an alternative worksite? If so, who is responsible for maintaining an employee's personally-owned equipment that is used for official business?*

Yes, provided certain conditions are met, agencies may permit employees to use personally-owned equipment to conduct official business. If an agency permits the use of personally owned equipment, the employee must agree to allow the agency to (1) configure that equipment with the proper hardware and software necessary for secure and effective job performance, and (2) access the equipment, as needed, to verify compliance with agency policy and procedures. Additional conditions that must be met are set forth in NIST Special Publication 800-53, Rev. 1, on page 64, as follows:

The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.

If the agency allows the use of personally-owned equipment for official business, then the telework agreement should clearly identify the employee's and agency's obligations for appropriate operation, repair, and maintenance of the equipment. While agencies are responsible for Government-owned equipment regardless of location, they are not required to be responsible for employee-owned equipment. At their sole discretion, however, agencies may assume responsibility for employee-owned equipment that is used to conduct official business. For example, agencies may authorize Help Desks or other agency personnel or resources to (1) fix a problem with the employee's personally-owned equipment, (2) help the employee fix the problem, or (3) provide, install, and/or upgrade Government-owned software on employee-owned equipment. If an agency permits the use of personally-owned equipment, the employee must agree to allow the agency to configure that equipment with the proper hardware and software including security, communications and applications.

b. *Are there policies for "limited personal use" of Government e-mail and internet systems?*

Yes. The Office of Management and Budget expects all agencies to establish personal use policies consistent with the recommended guidance developed by the CIO Council in 1999 (see "Personal Use Policies and 'File Sharing' Technology" memorandum at: **www.whitehouse.gov/omb/memoranda/fy04/m04-26.html**). In addition, NIST Special Publication 800-53, Rev. 1, under the section titled Supervision and Review — Access Control, recommends that agencies supervise and review the activities of users with respect to the enforcement and usage of information system access controls. According to this guidance, agencies should review audit records (*e.g.*, user activity logs) for inappropriate activities in accordance with organizational procedures and investigate unusual information system-related activities.

c. *Are there any other Guidelines for Alternative Workplace Arrangements?*

Yes. For additional guidance, see FMR Bulletin 2006-B3, Guidelines for Alternative Workplace Arrangements, Sections I through XV, dated March 17, 2006.

U.S. General Services Administration
GSA Office of Governmentwide Policy
Office of Real Property Management

This is for reference only. The reader should consult www.gsa.gov/fmrbulletin for the complete FMR Bulletin 2007-B1, Information Technology and Telecommunications Guidelines for Federal Telework and Other Alternative Workplace Arrangement Programs.