

DATE May 21, 2001

REMOTE ACCESS TO COMPUTER SYSTEMS

1. PURPOSE AND SCOPE. This Circular establishes responsibilities and procedures for accessing Bureau of Engraving and Printing (Bureau/BEP) mainframe, servers, or other computer resources from a remote location. It is intended to limit access to Bureau systems to authorized users only, to allow access when required by these users, to protect sensitive information, and to protect Bureau property.

2. POLICY. It is the policy of the Bureau to protect the confidentiality of sensitive information, to ensure that it maintains its integrity and is not changed or manipulated by unauthorized users, and to ensure that those individuals who have a need to access Bureau communication systems, databases, files or documents have the ability to do so in a timely manner without compromising the data or their privacy.

3. DEFINITIONS.

a. Access – Entry into the Bureau Local Area Network, e-mail system, or other computer or communications link associated with the Bureau network or stand-alone computer. Access may be gained through approved methods of connection (e.g. secure modem or Virtual Private Network (VPN)/internet connection).

b. Computers – Only Bureau issued computing devices, which could be laptops, Bureau issued personal computers, or other hardware, may be connected to the Bureau network or other Bureau computers. Additional authorization is required to remove these computers from the Bureau.

c. Portable Electronic Devices (PEDs) – These devices can function as Personal Digital Assistants (PDAs) and connect to the internet to retrieve e-mail. They also have a number of other uses, including web surfing and paging. The policy for use of Portable Electronic Devices is covered in a separate circular.

d. Sensitive Information – This includes any information which the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive information may be (but is not always) marked “Sensitive But Unclassified” (SBU), “For Official Use Only” (FOUO), or “Limited Official Use Only” (LOU).

4. REFERENCES.

BEP Information Security Manual, No. 71-00.42, March 16, 2000.

BEP Security Manual, No. 71-00, February 1, 2001.

Department of the Treasury Security Manual, TD 71-10.

“Electronic and Information Technology – Accessibility”, PL 105-220, Section 508 (29USC 794d), August 7, 1998.

“Protection of Laptop Computers”, Memorandum from James J. Flyzik, Deputy Assistant Secretary (Information Systems) and CIO, Department of the Treasury, March 2001.

Privacy Act of 1974 (5 USC 552a).

Computer Security Act of 1987 (PL 100-235).

“Security of Federal Automated Information Systems”, OMB Circular No. A-130, Appendix III (revised October 2000).

5. RESPONSIBILITIES.

a. The Manager, Information Technology Security Division (ITSD), is responsible for the Bureau’s overall automated information security program. The Manager shall:

- (1) authorize methods of connection for remote access (e.g., secure modem, VPN);
- (2) authorize remote access devices and communications methods (e.g. laptops, PDA’s, analog telephone, wireless, cable or DSL);
- (3) authorize users of remote access devices to connect to the Bureau computing equipment;
- (4) administer VPN configuration and access controls;
- (5) issue secure modems;
- (6) authorize the Systems Support Division (SSD) to install the approved access hardware or software;
- (7) evaluate technologies which ensure secure remote connections and approve devices or software for use;
- (8) maintain records of users who have remote access, including types of access devices, access levels, communications and approving authority; and

CIRCULAR

DATE May 21, 2001

(9) periodically audit use of remote access, assess security of connections, and verify appropriate levels of access.

b. The Manager, Systems Support Division, is responsible for the installation and maintenance of modems, VPNs, and other hardware or software which has been authorized by the appropriate parties. The Manager shall:

(1) ensure that all authorizations have been given before installing remote access devices; and

(2) assign system administrators the responsibility of operational security for devices installed or maintained. The system administrator has the responsibility to alert the Manager, SSD, and the Manager, ITSD, to viruses, attacks, or other security threats, and also to available patches or workarounds for security problems with installed software (if the system administrator is a contractor employee, the COTR for that contract shall be the operational security administrator).

c. Users shall:

(1) apply for authorization to connect to the Bureau mainframe, servers, or other computer resources from remote locations from appropriate authority (at least the Associate Director level for remote connectivity);

(2) provide justification for requiring remote access that is directly related to current job function;

(3) notify the Manager, Information Technology Security Division, if job function or position changes and the need for remote access changes;

(4) understand and agree to abide by rules of use for remote access and for remote access devices. These rules will include, but are not limited to:

(a) identification of the sensitivity of the information to be accessed on the Bureau network or equipment;

- Remote access will be for nonsensitive or sensitive but unclassified information only; if access is required for information which is within a National Security Classification or is otherwise compartmented, contact the Manager, Information Technology Security Division.

- Files which are stored on a remote device will be at the nonsensitive or SBU level only. If information maintained is at the SBU level, the user must consult with the Manager, Information Technology Security Division to ensure that appropriate protection is installed.

(b) connection to Bureau remote devices only as authorized;

- Only Bureau issued equipment that has been approved for remote access may be connected to the Bureau network, mainframe, servers, or other computers.

- Bureau equipment may be connected only through approved devices/software (e.g. encrypted modem or VPN software) issued by the Bureau. VPN connectivity shall be only through connections specifically authorized by the Manager, ITSD. This means that the Manager, ITSD, shall be notified of the type of access available to the laptop or PED; for example, whether it is analog telephone, wireless, cable or DSL, or other. In certain circumstances, a Bureau employee may be authorized to use a Bureau issued personal computer from a remote location. Connectivity restrictions for these computers are the same as for laptops.

- Devices not specifically authorized by the IT Security Division shall not be connected to Bureau networks or computers. This means that non-Bureau issued personal computers, PDAs, etc. shall not be connected to the Bureau network.

- No Bureau device shall be connected to any non-Government network or to any other non-Government device. For Bureau VPN users, this means that any internet connectivity must be through the Bureau approved ISP.

- A personal firewall and virus scanning software must be used for all connections.

(c) protecting the information on the remote device from unauthorized disclosure. This includes ensuring that access to information on the laptop or PED is password protected. The password shall be chosen and changed as required by Bureau password policy and shall not be provided to any other individual. It also includes not using or leaving the laptop or PED in a public place where information may be viewed or retrieved by others;

(d) reporting the loss of any Bureau owned remote access equipment. Also reporting the potential loss or compromise of any sensitive information contained on a remote device; and

(e) reporting attacks on Bureau equipment or networks and reporting viruses or other malicious code to the Manager, ITSD.

CIRCULAR

No.10-08.23

DATE May 21, 2001

d. Office Chiefs, through their Associate Directors, retain the responsibility for the appropriate and secure use of remote technologies by the employees who they have authorized to have access. They shall:

(1) Prepare requests for remote access for users if the access is justified in supporting a business need and related to the employee's job functions;

(2) Provide access requests with recommendations to the appropriate Associate Director for final approval;

(3) monitor usage and act to remove access when Bureau policy is violated;

(4) maintain records of authorized users and government owned equipment furnished to employees. Ensure accountability of issued assets and integrity of Bureau networks, systems and information; and

(5) notify the Manager, Information Technology Security Division, if functions or positions change and the need for remote access changes.

6. OFFICE OF PRIMARY RESPONSIBILITY. Associate Director (Chief Information Officer).

<SIGNED>

Ronald W. Falter

Associate Director (Chief Information Officer)

DISTRIBUTION: Office Chiefs