



1. PURPOSE

It is the policy of the Department of Commerce (DOC) to ensure that access to Information Technology (IT) systems from remote locations is provided to users in a secure and effective manner. This set of requirements defines the DOC implementation standard intended to protect DOC IT networks and servers from the risks inherent in remote access without significantly impairing the DOC mission or the quality of service to the remote user.

2. BACKGROUND

Given the demands of the modern workforce, the capacity to access computing resources to meet mission requirements, anywhere and anytime, is critical. However, this demand must be balanced with IT security requirements needed to maintain the confidentiality, integrity, and availability of DOC's infrastructure. Accessing the Department's resources from Internet Protocol (IP) addresses not under direct control of the Department essentially expands our perimeter and increases risk.

NIST Special Publication 800-53 defines remote as: "Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet)." DOC further categorizes remote access into four levels according to the risk of harm inherent in the nature of the access and the sensitivity of the information accessed, and requires authentication that is commensurate with that risk.

3. SCOPE

These requirements apply to DOC employees, contractors, or other authorized users using any computing device to access DOC's infrastructure or data from non-DOC Internet Protocol (IP) address space at access level 2, 3, or 4 (defined below, section 6.4). This policy does not apply to access level 1; non-authenticated access (e.g., access to public DOC web sites) is outside the scope of this policy.

4. AUTHORITY

The Department of Commerce (DOC) Chief Information Officer (CIO) has the authority to develop, implement, and manage IT security processes and procedures to protect the availability, confidentiality, and integrity of the Department's IT resources. The DOC Chief Information Security Officer (CISO)/Senior Agency Information Security Officer (SAISO) shall ensure that IT security policy and requirements are developed consistent with applicable statutory authority, including the Clinger-Cohen Act and Federal Information Security Management Act (FISMA); with regulatory requirements and external guidance, including Office of Management and Budget (OMB) policy and Federal Information Processing Standards (FIPS) publications promulgated by the National Institute of Standards and Technology (NIST); and with internal policies and requirements.

5. CANCELLATION/AUGMENTATION OF EXISTING POLICY

This CITR is an addition to the *Department of Commerce IT Security Program Policy (ITSPP)* and replaces *Appendix D: Unclassified System Remote Access Security of the 2005 DOC ITSPP and Minimum Implementation Standards* and *DOC Remote Access Procedures*.

6. POLICY

Operating Units (OUs) have 120 days from the signature date to implement this CITR.

6.1 GENERAL

1. All remote access must be approved by a manager, supervisor, or COTR/COR. This approval must be documented in writing or through an OU electronic-approved mechanism (e.g., digital signature).
2. All remote access users must agree and abide by the terms of the “remote access user security agreement” and this DOC remote access CITR. DOC remote users must practice the same due care as when obtaining access from a DOC facility.
3. Secure remote access must be strictly enforced. Remote access services not explicitly approved by the operating unit CIOs are strictly prohibited.
4. DOC-equipment used to remotely access the DOC IT infrastructure, whether DOC provided or personally owned, must be maintained and configured in a secure manner and meet the minimum requirements set forth in Section 6.2 below.
5. When working from a remote location, only DOC-authorized email accounts must be utilized to conduct official business on behalf of the Department. Personal email accounts (e.g., Hotmail, Yahoo, or Gmail) must not be used to conduct official business.
6. Use of access protocols vulnerable to exploitation (e.g., Telnet, TFTP, FTP, rsh, rcp, rlogin, X Windows, etc.) is prohibited unless transmission is through an encrypted tunnel such as a Virtual Private Network (VPN).
7. Remote access for privileged accounts must only be granted to those with proper justification.
8. Remote access infrastructure must support authentication, authorization, accounting, and auditing and should be designed to decrypt and inspect all traffic, as appropriate, prior to reaching a perimeter or sub-network firewall.

6.2 MINIMUM STANDARDS AND PRACTICES

Remote computers used for Level 2, 3, and 4 access must be configured and maintained in a secure manner as described in the following table. The following table lists the Mandatory (M) and Recommended (R) countermeasures to be implemented depending on the type of device. Although countermeasures in the table below are recommended for personally-owned computers, it is strongly suggested that these requirements be incorporated into the remote access user security agreement. Additionally, remote access initiated from public computers (e.g., kiosks, Internet cafes) should be done sparingly and only when necessary because of the grave risk that these public computers pose.

Standard Countermeasure	DOC/ Contractor - Owned/ Furnished Equipment	Personally- Owned Equipment
Configure computers to not store DOC passwords.	M	R
Terminate connections to DOC remote access when not being used, and users must not leave an active connection to DOC IT systems unattended. Systems must terminate remote connections to the DOC network, when idle for more that 30 minutes.	M	R
Ensure that all passwords comply with DOC policy.	M	R
Ensure encryption of passwords and data, while stored and transmitted, using a FIPS 140-2 validated cryptographic module.	M	R
Install, regularly update (at least daily), and run anti-virus and anti-spyware software on equipment that supports such software.	M	R
Install and regularly update (at least daily) vendor updated and security related patches on devices that can be patched.	M	R
Install personal firewalls on all remote access computers connected to the Internet (for which such software is available).	M	R
Ensure the OU defined baseline of the Federal Desktop Core Configuration is implemented and all unnecessary services are removed or terminated.	M	R

6.3 DOCUMENTATION REQUIREMENT

Operating units must develop and implement a mechanism to document and maintain records of “remote access user security agreements” and management approval for Level 2, 3, and 4 access.

An example of such an agreement follows; however, the template may be adapted for electronic completion, signature, and storage in accordance with the Government Paperwork Elimination Act (GPEA). The manager, supervisor, or COTR/COR must maintain records of the documented supervisor approval. He/she must also notify the system owner, who in turn must provide authorized DOC IT users with the minimum access privileges documented in the agreement that are necessary to accomplish their job duties.

6.4 ACCESS-LEVEL SPECIFIC REQUIREMENTS

DOC categorizes remote access into four levels according to the risk of harm inherent in the nature of the access and the sensitivity of the information accessed. These levels are loosely derived from NIST SP 800-63.

6.4.1 LEVEL 1

Level 1 applies to non-authenticated access external to the DOC network perimeter (e.g., accessing DOC public web sites without establishing a user account and logging in). Level 1 access is outside the scope of this policy.

6.4.2 LEVEL 2

Level 2 access applies to basic user privileges. This category includes users who authenticate to a DOC gateway and are granted only partial access to systems and networks. The countermeasures in section 6.2 apply to Level 2 access. In addition, the following countermeasures must be implemented:

1. Use single-factor passwords that comply with DOC Policy.
2. Access DOC IT resources remotely from DOC-owned/furnished, personally-owned computers under the control of the user, or public-access computers. Due to increasing risk from publicly-accessible computers, remote access from these devices should be used sparingly.

6.4.3 LEVEL 3

Level 3 access applies to non-administrative access to DOC infrastructure using an approved clientless or client-base VPN to access DOC IT resources. All of the countermeasures listed for Level 2 are mandatory for Level 3. In addition, the following countermeasures must be implemented:

1. Two-factor authentication is required.
2. A FIPS 140-2 validated mechanism must be used for encrypting remote access sessions.
3. Personally-owned computers and other non-DOC-provided equipment can be used to gain access to DOC-provided Web Mail and secure Web portals using clientless (e.g., SSL/TLS), providing web access only.
4. Personally-owned computers may not be used for client-based VPN access (e.g., IPsec).
5. DOC-provided equipment must be configured to prevent split-tunneling or dual homing.
6. When not in use, DOC-provided equipment for moderate or high data should be stored in a secure manner.
7. Third-party remote control/direct-access services (e.g., "www.gotomypc.com") used for access to the DOC infrastructure is strictly prohibited.

6.4.4 LEVEL 4

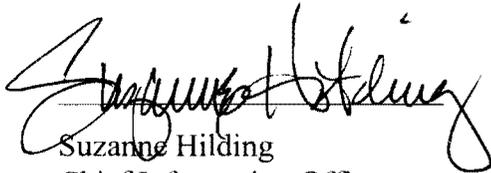
Level 4 represents system administrator access to DOC infrastructure and data. All countermeasures listed for Level 3 are incorporated as mandatory for Level 4. In addition, the following countermeasures must be implemented:

1. Two-factor authentication is required. Three-factor authentication is recommended.
2. Only necessary system administration tasks must be performed while using the root or administrator account.
3. Remote access should be limited by single IP or narrowest IP range possible.
4. The computer performing/initiating remote access must not be a server (e.g., mail, Web).
5. All operating systems installed on multi-boot computers or computers using virtual environments must be configured to meet the requirements in this policy.
6. Logs should be reviewed on the remote host on a weekly basis.

7. REFERENCES

- FIPS 46-3, *Data Encryption Standards (DES)*
- FIPS 140-2, *Security Requirements for Cryptographic Modules*
- FIPS 197, *Advances Encryption Standard*
- NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*
- NIST SP 800-45, *Guidelines on Electronic Mail Security*
- NIST SP 800-46, *Security for Telecommuting and Broadband Communications*
- NIST SP 800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*
- NIST SP 800-63, *Electronic Authentication Guideline*

- Committee on National Security Systems Information Assurance Advisory Number IAA-002-2002
Updated Personal Electronic Devices Guidance, issued by the National Security Agency
- OMB 04-04, *E-Authentication Guidance*
- OMB A-130, *Management of Federal Information Resources*
- OMB 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of*
- CITR-002, *Safeguarding Data on Foreign Travel*
- CITR-005, *Removable Media Devices*


Suzanne Hilding
Chief Information Officer

9/9/09
Approval Date

