U.S. Department of Commerce
Unclassified System Remote Access Security Policy and Minimum Implementation Standards

What is the purpose of this policy?

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 a framework of implementation standards 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.

To whom and to what does this policy apply?

This policy applies to all DOC federal employees and contractors who remotely access unclassified DOC IT systems as well as other authorized government officials, business partners, third party collaborators, and researchers who require remote access to DOC systems. The policy applies to all DOC IT systems, regardless of platform, that allow such access, and it explains the proper configuration and maintenance of the devices used to conduct remote access, including DOC-owned/furnished, personally-owned, and publicly-accessed equipment, and equipment at alternate operation sites used for continuity of operations activities. It explains the security of the communication mechanisms that connect the devices to DOC IT systems.

It does not cover requirements for securing the servers and applications that are remotely accessed, nor does it cover remote access to classified systems. The *DOC IT Security Policy and Minimum Implementation Standards* and the *DOC Security Policy Manual*, currently under development, will address these areas. This policy does not apply to remote access to publicly accessible DOC Web sites, including those sites that support transactions and access to databases, even if that access is in support of the conduct of official Government business. The term "remote access" as used in this policy does not include such Web site access, unless such access includes access to systems and data not publicly available through such Web sites.

This policy is to be applied independent of the size of the IT system and independent of the type of remote access technology. Thus, it includes the following modes of remote access: modems, broadband and wireless connections; third party internet service providers (ISP); public access sites such as kiosks and Internet cafés; and alternate platforms such as personal electronic devices (PED)/personal digital assistants (PDA), and cell phones. It applies to all IT systems used to carry out DOC's mission, located both on and off government property, whether operated by federal employees or contractors.

This policy must be explicitly addressed in all IT procurement activities that involve remote access mechanisms. In addition, before implementing these standards, offices with bargaining units must meet labor relations obligations with those units.

Why does DOC need a remote access security policy?

This policy provides the minimum standards to reduce risks to DOC IT systems and data while enabling DOC staff to continue to remotely access DOC IT systems for official duty purposes. When an individual remotely accesses DOC IT systems, the overall security of those systems may be lowered and the potential for unauthorized access to data. Computers that remotely access DOC IT systems are often not highly maintained with respect to security. The result is that such computers may have been penetrated by hackers or fallen victim to one of thousands of active viruses, trojans, and worms. When these computers remotely access DOC IT systems, hackers, trojans, and worms can circumvent DOC perimeter security mechanisms and cause great damage. This problem is exacerbated when a remote computer is connected to the Internet and to DOC IT systems at the same time (e.g. when using broadband technology). However, remote access is an increasing necessity as more federal workers are carrying portable IT devices (e.g. laptop computers, cell phones, Palm or Windows PDAs, and Blackberries) and using Internet cafés and kiosks to enhance communications and perform DOC mission functions while on travel or teleworking.

Who is responsible for implementing the DOC remote access security policy?

DOC Chief Information Officer (CIO)

The DOC CIO ensures that DOC has a program to protect DOC IT systems and data, approves policy for the IT security of DOC IT systems, adjudicates waiver decision disputes, and ensures that the Department-level IT security compliance monitoring process includes conformance with this policy.

IT Security Program Manager

The DOC IT Security Program Manager maintains and updates DOC IT security policies and monitors operating unit compliance through the conduct of ongoing compliance reviews. The DOC IT Security Program Manager must review and approve or deny waivers to DOC IT security policies.

Director for Human Resources Management

The Director for Human Resources Management addresses issues and questions regarding DOC telework program policy. In addition, the Director assists in determining disciplinary actions available to supervisors of federal employees who violate the requirements of this policy.

Head of Operating Unit and Senior Program Officials

Each DOC Head of Operating Unit and Senior Program Officials (e.g., heads of line offices and major operating unit components) must ensure that system owners implement the mandatory minimum standards of this policy.

Operating Unit CIO

Each operating unit CIO must assist system owners in the implementation of the mandatory minimum standards of this policy, or obtain approved waivers to the requirements. Specifically, operating unit CIOs must:

- Ensure communication of the policy to system owners and system users.
- Establish a program to support the installation, use, and periodic maintenance of antivirus software and personal firewalls on DOC-owned computers used by remote users. Such a program must be consistent with limitations on use of appropriated government resources. It would include providing appropriate information and support, as determined to be necessary by the Operating Unit CIO, to remote users who use personally-owned computers for official business to assist the user in meeting the mandatory minimum standards of this policy, including, at a minimum: facilitating the upgrade of browser software that supports required

encryption; maintaining lists of acceptable antivirus software and personal firewall products from which remote users may choose; assisting in the configuration of personal firewalls; and communicating the release of software security patches to remote users.

- Ensure that operating unit policy and procedures reflect these remote access policies and standards. The operating unit CIO must develop remote access security procedures that supplement this policy to establish specific guidance commensurate with the level of security warranted to meet the operating unit's requirements. Such procedures must be consistent with this policy.

Operating Unit IT Security Officer

Operating unit IT Security Officers (ITSOs) must include monitoring of compliance with this policy as part of their periodic IT security self-assessment program or automated system evaluations. This includes ensuring the maintenance of approved waivers by system owners as part of the documentation for appropriate system security plan(s). In addition, IT Security Officers must:

- Communicate this policy to all remote users within the operating unit.
- Ensure that user IT security awareness and training programs address remote access so that all DOC personnel are aware of this policy.
- Notify and coordinate with the DOC Computer Incident Response Team (DOC CIRT), operating unit CIRT, and the DOC Critical Infrastructure Program Manager regarding computer security incidents resulting from remote access to DOC IT systems.
- Ensure that remote systems are monitored for compliance with this policy (as technically possible).
- Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate the policy.

IT System Owners

System owners must determine the sensitivity of information contained in their systems and allow or deny remote access to these systems. System owners must also ensure that:

- Remote access controls are implemented consistent with the risk and magnitude of harm to the information and the mandatory minimum standards of this policy;
- The relevant system security plans document what types of remote access are acceptable and document the security controls required for that access; and
- The relevant system security plan includes approved waivers of the requirements of this policy.

System and Network Administrators

System/network administrators must support secure remote access services for authorized remote users. Specifically, system/network administrators must:

- Ensure appropriate security controls on remotely accessible systems are set in accordance with the system security plan for the system to which remote access is allowed.
- Follow procedures established for configuring and maintaining approved remote access security technologies (for example, Virtual Private Network servers).
- Install system software patches, including anti-virus software signature files, on DOC-owned computers used for remote access as directed by the system owner or ITSO.
- Terminate remote access privileges within one business day of notification by the manager, supervisor, or COTR that the privileges must be withdrawn.

Help Desk Staff

Help Desk staff, following procedures developed by the Operating Unit CIO that are consistent with this policy, are to provide remote access IT security support to users who are authorized to perform DOC duties remotely, including providing information and assistance in configuring and maintaining remote access hardware and software furnished by DOC, and, to the extent determined by the Operating Unit CIO, provide assistance in supporting personally-owned or public-access hardware or software. Such support must be sufficient to ensure compliance by remote access users with all provisions of this policy.

Managers, Supervisors, and Contracting Officer's Technical Representatives (COTRs)

Managers, supervisors, and COTRs must determine whether federal employees and contractors require remote access in the accomplishment of the DOC mission. Specifically, the manager, supervisor, or COTR must:

- Determine the federal employee's or contractor's need to know before access is granted. Remote access to any DOC IT system must not be authorized for a person who does not have a need for access to the system in the normal performance of his/her official duties.
- Grant remote access privileges to remote users under his/her supervision or oversight and ensure the maintenance of records documenting that remote users are authorized and have read and understand this policy, and notify system owners of new users.
- Ensure that the relevant system security plans allow for the type of remote access granted.
- Review "remote access user security agreements" on an annual basis to verify the continuing need for access, the appropriate level of privileges, and the accuracy of information contained in the agreement (e.g., systems authorized for access and type and version of antivirus software and personal firewall).
- Ensure remote users under his/her supervision or oversight comply with this policy, to the extent practicable, and pursue appropriate disciplinary action when he/she fails to comply with this policy.
- Notify the system owner to revoke remote access privileges when a remote user under his/her supervision or oversight no longer requires remote access privileges or he/she fails to comply with this policy by notifying the system/network administrators within one business day of making such a determination.

Remote Access Users

Because remote users are crucial to effective remote access security, all DOC federal employees and contractors must follow the mandatory minimum standards of this policy. Failure to comply with this policy may result in disciplinary action and/or revocation of remote access privileges as determined by their manager, supervisor, or COTR. Remote users must:

- Complete initial and refresher IT security awareness training as required by DOC IT security policy.
- Certify that he/she have read and understand their responsibilities under this policy prior to receiving remote access authorization and authentication credentials. Abide by the terms of signed "remote access user security agreement."
- In accordance with operating unit CIO's remote user assistance program, ensure the computer used for remote access is configured and maintained according to this policy and according to the method of remote access being used.
- Periodically check to determine that all applicable security patches available for the software

used to process DOC information on personally-owned computers have been installed.

- Return DOC-owned computers used for remote access as directed by the responsible system owner, manager, supervisor, COTR, or ITSO so that the security configuration (e.g. patches) of the computer can be checked and enhanced.
- Exercise caution when accessing government information from a public area to prevent compromise of sensitive information.
- Report, within 24 hours of identification, all IT security incidents to their supervisor, to their COTR, to their ITSO, or to the responsible CIRT following DOC incident reporting procedures (http://www.osec.doc.gov/cio/oipr/ITSec/Incihand.htm).

Will there be a transition period for implementing the DOC remote access security policy?

This policy is effective upon issuance. However, a transition period will be allowed for a careful migration to these standards. All DOC operating units must complete and issue supplemental implementation guidance to describe specific practices for implementing this policy and mandatory minimum standards within each operating unit. The guidance must be issued by March 31, 2003, sooner if possible, and a copy submitted to the DOC IT Security Program Manager. In addition, all DOC operating units must notify the DOC IT Security Program Manager in writing by March 31, 2003, that these standards have been fully implemented, or provide a detailed schedule of milestones for completing implementation no later than September 20, 2003. The mandatory minimum standards of this policy must be fully implemented by September 30, 2003, sooner if possible.

How can I obtain a waiver in situations where I cannot comply with this policy?

Operating unit CIOs must identify any proposed deviations from the mandatory minimum standards of this policy and request a waiver in writing from the DOC IT Security Program Manager. Approved waivers must be documented as part of the appropriate system security plan(s) that cover the system(s) applicable to the waiver. Identical systems under the same management authority and covered by one system security plan require only one waiver request.

Requests for a Remote Access Security Waiver must:

- Cite the specific mandatory minimum standard(s) for which the waiver is requested,
- Explain the rationale for the requested waiver, and
- If applicable, describe compensating controls to be in place during the period of the requested waiver, until systems are compliant with this policy, and provide an action plan (including target dates) for compliance.

Operating unit CIOs may appeal the DOC IT Security Program Manager's waiver decision in writing to the DOC Chief Information Officer.

Is all remote access the same?

DOC categorizes remote access into three tiers according to the risk of harm inherent in the nature of the access and the sensitivity of the information accessed. Tier 1 represents low risk because the systems accessed are between the outermost DOC network perimeter or border device, such as the DOC firewall, and outside inner DOC firewalls that protect local area networks. In addition, Tier 1 information is of low sensitivity. Tier 2 represents medium risk because basic user privileges are allowed to access systems processing or storing sensitive-but-unclassified information inside the inner DOC firewalls and internal to the DOC computing environment. Tier 3 represents high risk because administrative (or “super-user”) privileges are allowed to access systems processing or storing sensitive-but-unclassified information that are internal to the DOC computing environment.

How do DOC IT users obtain remote access privileges?

Operating units must implement a mechanism to document and maintain records of "remote access user security agreements" and management approval for Tier 2 and Tier 3 access. A "remote access user security agreement" provides documentation ensuring that:

- The user's manager, supervisor, or COTR has approved the remote access request;
- The user certifies that he/she has received DOC security training within the last year; and
- The user certifies that he/she understands, and will abide by, the terms of the "remote access user security agreement" and this DOC remote access policy.

An example of such an agreement follows; however, the template may be adopted for electronic completion, signature, and storage in accordance with the Government Paperwork Elimination Act (GPEA). The manager, supervisor, or COTR must maintain records of the documented supervisor approval and the user certification in accordance with the Privacy Act. He/she must also notify the system owners, 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.

U.S. Department of Commerce
Unclassified System Remote Access User Security Agreement (Example)

Purpose and Scope: I understand I am being granted permission to remotely access unclassified DOC IT systems as specified below, and that my use of this access may be monitored by DOC for compliance with this policy. I understand this remote access may be allowed in conjunction with a separate approved request for teleworking. I have completed DOC IT security training within the last 12 months, and I hereby attest that I have read and understand the DOC IT Security policies for remote access and password management. I agree to comply with these policies, and I understand that my failure to comply with these policies may result in termination of my remote access privileges and/or disciplinary action. Remote access to the following unclassified systems and web-enabled applications is authorized for official use:

____________________ ________________________ ___________________________
____________________ ________________________ ___________________________

Protection of Data: I hereby affirm and acknowledge my responsibility to ensure the confidentiality, integrity, and availability of all forms of Government information in accordance with DOC IT Security Policy and the DOC Security Manual, in a manner consistent with its sensitivity.

Protection and Maintenance of Equipment (check one):
_______DOC *will* provide and maintain hardware and software for remote access. I will not alter the configuration of government equipment unless authorized in writing to do so. I will protect DOC-owned/furnished resources and submit the equipment for periodic maintenance as required by DOC.
_______DOC *will not* provide hardware for remote access, but may provide software installation disks and support software used to process DOC information as permitted by software license agreements. I will abide by the license agreements for DOC-furnished software. DOC authorizes me to use my personally-owned computer for remote access, and although DOC may provide limited support, it is not required to support maintenance of the hardware or personally-owned software. I will install and maintain the following:

Anti-virus software (required) ______________________________ (specify vendor and version)
Personal firewall (required) ________________________________ (specify vendor and version)

Computer Incidents: I also acknowledge the possibility, however small, that such information could potentially be viewed or downloaded by others than myself as a result of my remote access. I fully understand that it is my duty to exercise due care in protecting this information and to immediately report an unauthorized disclosure or compromise to my supervisor and the *{enter name/phone of the ITSO, the operating unit CIRT or DOC CIRT}* so that appropriate procedures may be initiated. I further understand that, after proper coordination with law enforcement authorities, the Government may temporarily seize the device used to gain remote access for the purposes of forensic examination and sanitizing of compromised information. Additionally, during this process I understand there exists a risk that system files and programs may be erased or damaged, or that unintentional damage may occur to the computer hard drive. I hereby waive any and all claims against the Department of Commerce, the Federal Government, and individual officers, employees, agents and contractors thereof, arising out of necessary security procedures and actions with respect to personally-owned IT equipment and any such damage to, or erasures of personal data.

____________________________	____________________________	__________
Remote User's Printed Name	Signature	Date

I hereby certify that this federal employee/contractor requires remote access as described herein to accomplish the DOC mission:

____________________________	____________________________	__________
Remote User's Supervisor's Printed Name	Signature	Date

What are the minimum standards for protective countermeasures required by DOC?

Remote connectivity to DOC IT systems can be grouped into the three tiers of access as described in the following table.

<table>
<tr><th>Tier</th><th>Category</th><th>Access Description</th><th>Level of Security for Remote User’s System</th><th>Minimum Standard Countermeasures Required</th></tr>
<tr><td>1</td><td>Authenticated services</td><td>For access to DOC IT services through the Internet or by dial-up that must be authenticated, require access only to services outside the DOC firewall, and do not require access to internal DOC systems.</td><td>Low
Unclassified information of low to medium sensitivity relative to availability, confidentiality, and integrity.</td><td>1. Operating units must establish, or participate in, centralized management control of all modem pools and require written authorization for use of modem pools. Call-back features should be enabled.
2. Remote computers used for “authenticated services” must be configured and maintained in a secure manner as described in the following table. Standard countermeasures are identified as either Mandatory (“M”) or Recommended (“R”) depending on the type of device used.
<table>
<tr><th>Standard Countermeasure</th><th>DOC-Owned/ Furnished Equipment</th><th>Personally-Owned Equipment</th><th>Other (Publicly-accessed) Equipment</th></tr>
<tr><td>Configure computers to not "remember" DOC passwords.</td><td>M</td><td>M</td><td>R</td></tr>
<tr><td>Terminate connections to DOC applications when not being used.</td><td>M</td><td>M</td><td>M</td></tr>
<tr><td>Ensure that all passwords to DOC systems meet the DOC <i>Policy on Password Management</i>.</td><td>M</td><td>M</td><td>M</td></tr>
<tr><td>Do not share or reveal DOC usernames and passwords to anyone (including family members) to prevent unauthorized access to DOC IT systems and data.</td><td>M</td><td>M</td><td>M</td></tr>
<tr><td>Ensure encryption of passwords and data using, as a minimum, Advanced Encryption Standard (AES) or Triple Data Encryption Standard (Triple-DES) when transmitted over the Internet (except for one-time passwords). This encryption can be done by the individual applications or provided by DOC servers through an encrypted tunnel to the remote computer. Wireless Encryption Protocol (WEP) is not an acceptable form of encrypting passwords.</td><td>M</td><td>M</td><td>M</td></tr>
<tr><td>Install, regularly update (at least monthly), and run antivirus software on equipment that supports such software.</td><td>M</td><td>R</td><td>R</td></tr>
<tr><td>Install and regularly update (at least monthly) security related patches on devices that can be patched.</td><td>M</td><td>M</td><td>R</td></tr>
<tr><td>Install personal firewalls on all remote access computers connected to the Internet (for which such software is available). Stand-alone firewalls may be used in conjunction with personal firewalls within home networks using broadband technology (e.g. cable modems, digital subscriber lines, and satellite uplinks) or wherever else applicable.</td><td>M</td><td>R</td><td>R</td></tr>
<tr><td>Shield entry of authentication information from “shoulder-surfers,” as though shielding entry of a PIN at an ATM machine.</td><td>M</td><td>M</td><td>M</td></tr>
<tr><td>Clear browser history and cache and close browser when finished with remote access needs. [For example, with Internet Explorer, select the “Tools” menu, then select “Internet Options,” under the “General” tab, select Temporary Internet Files > “Delete Files,” and History > ”Clear History,” then click “OK” and close the browser.]</td><td>R</td><td>M</td><td>R</td></tr>
<tr><td>Do not save Government information and applications to the hard drive of the remote access computer.</td><td>NA</td><td>R</td><td>M</td></tr>
</table>
</td></tr>
</table>

Tier	Category	Access Description	Level of Security for Remote User's System	Minimum Standard Countermeasures Required
2	Authenticated network access	For access to internal DOC systems (i.e., inside the outermost DOC firewall or perimeter gateway). Such a user may then access a variety of DOC IT services that are only available to computers behind the outermost DOC firewalls that protect systems available only to authorized DOC users. This category includes users who authenticate to a DOC gateway and are granted only partial access to the relevant network.	Medium Highly sensitive-but-unclassified information of medium to high sensitivity relative to availability, confidentiality, and integrity. This level of access requires a moderate amount of security to ensure user identification and authentication and user accountability.	Computers used for "authenticated network access" remote access must be configured and maintained in a secure manner. All of the standard countermeasures listed for Tier 1 are incorporated as mandatory standards for Tier 2, PLUS users must meet the following additional mandatory standards: • Approve all remote access in writing by user's supervisor and ensure the user certifies he/she has been trained and understands applicable policies. • Conduct remote access either from DOC-owned/furnished or personally-owned computers under the control of the user, or public-access computers if the user can verify that security mechanisms exist that satisfy this policy. • Use a mechanism for encrypting sessions that meets at a minimum AES or Triple-DES. Examples include using Public-Key Infrastructure (PKI), a Virtual Private Network (VPN) or a CITRIX remote access server. • Authenticate first to a remote access gateway on the DOC network perimeter as well as comply with the system owner's requirements for authentication and identification of the specific internal system or data resource being accessed. All data must pass through an additional access control point (e.g., a firewall, a modem call-back feature, or SecureID tokens) before users are permitted to access internal systems. • Don't use remote access computers as servers (e.g., web servers, private e-mail servers, File Transfer Protocol (ftp) sites, or chat servers), or connect the computer to other networks, including wireless networks, while connected to the DOC network. • Computers must be protected against unauthorized access by using password-protected screensavers when idle for a duration of 15 minutes. • Terminate connections to the DOC network (either initiated by the user or by DOC remotely accessed systems), when idle for more than 30 minutes. • Use of access protocols vulnerable to exploitation (e.g., Telnet, ftp, and rlogin) is prohibited unless transmission is through an encrypted tunnel such as a VPN. • Use of public-access equipment is prohibited.
3	Remote control	For administrative access to a DOC computer, database, or IT resource (e.g., using *PCAnywhere*). This category is usually used for obtaining remote administrator control but it also includes user level control when unrestricted user level access to the underlying operating system is obtained.	High Highly sensitive-but-unclassified information of medium to high sensitivity relative to availability, confidentiality, and integrity. This level of access requires a high amount of security due to the possible penetration of the remotely accessed computers and level of user privileges allowed.	Remote computers used for "remote control" access must be configured and maintained in a secure manner. All of the standard countermeasures listed for Tier 1 and the mandatory standards for Tier 2 are incorporated as mandatory standards for Tier 3. In addition, he/she must meet the following mandatory standards: • Grant remote control access privileges in moderation, and only to those with proper justification. • Allow use of third-party remote control/direct-access software in moderation (e.g., *PCAnywhere* or "*www.gotomypc.com*"), and only to those with proper justification. • Properly configure use of direct-access software, including: – No remote control/direct access software may be permitted to use dial-up connectivity unless transmissions are encrypted in accordance with the standards of this policy. – Dial-up access must be protected by call-back modems programmed to call authorized user numbers. – IP address screening must be used for broadband connections.

How is data protected from loss?

Remote access users must protect government data from loss, destruction, compromise, and leakage to unauthorized parties. Specifically:
For Tier 1, Tier 2, and Tier 3 access:

- Users must not leave an active connection to DOC IT systems unattended.
- Surge protectors should be used on remote access equipment.

For Tier 2 and Tier 3 access:

- Users must ensure that the government data processed on DOC-owned or personally-owned remote access computers is backed-up on a periodic basis, either automatically through the network or remotely with removable drives (such as government-furnished diskettes).
- When sensitive-but-unclassified government information is copied to a removable drive, the media must be properly marked as For Official Use Only or with the proper information category. If possible, the media should be encrypted to prevent unauthorized disclosure.
- Uninterruptible power (UPS) supplies should be in place to protect data rated High availability (i.e., required within 72 hours of interruption).
- When not in use, media should be stored in heavy locked furniture such as a desk or credenza or a safe.

How are portable remote devices protected from loss?

DOC requires that remote access users protect DOC-owned equipment from loss and destruction, and DOC recommends protection of personally-owned equipment used for remote access. The following practices are recommended:

- Physically secure laptops that spend a majority of their time in two or fewer places with a cable lock. Almost all major laptop brands contain a slot to attach a lock cable. Those that do not can have a lock cable glued on.
- Use a non-descript carrying case for portable devices to avoid unwanted attention. A leather briefcase or obvious laptop case can attract attention in public places, especially airports, and while on planes.
- If traveling with sensitive-but-unclassified information, pack information or information backup in separate bag from the portable device in case of theft of the device.
- Identify the portable device with contact information. Decals or markings can be placed on the device that are difficult to remove and if done so, indicate obvious tampering.
- Record the serial number and other identification information about the portable device twice, and keep one copy at home or in the office in case of theft of the device. This information can be helpful to authorities searching for the device if lost or stolen.
- Consider use of advanced security features such as biometric login, motion sensing, and "Lo-Jack" type location tracking. Depending on the nature of the information accessed by and processed on the remote access device, the cost and benefits of advanced controls should be analyzed.

Where can I find more information on remote access security and related topics?

DOC recommends the following sources for additional information on remote access security:

- Department of Commerce *Telework Program*;

- Department of Commerce *Policy on Password Management;*
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 46-3, *Data Encryption Standard (DES);*
- NIST FIPS 197, *Advanced Encryption Standard*;
- NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy;*
- NIST Special Publication 800-45, *Guidelines on Electronic Mail Security*;
- NIST Special Publication 800-46, *Security for Telecommuting and Broadband Communications*;
- NIST Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; and
- Committee on National Security Systems Information Assurance Advisory Number IAA-002-2002, *Updated Personal Electronic Devices Guidance*, issued by the National Security Agency (document For Official Use Only).

What are definitions of key terms used in this policy?

- **Authentication** – The authentication mechanism provides an added level of assurance that the user really is who he/she says he/she is. Authentication consists of something a user knows (such as a password), something the user has (such as a token or smart card), or something the user is (such as a fingerprint). It is the process by which the remote user is identified by entering a valid username and password.

- **Broadband** – Broadband is a type of data transmission in which a single medium (wire) can carry several channels at once (such as Digital Subscriber Lines (DSL) and cable TV/modem, two-way satellite, and other emerging technologies).

- **Computer Security Incident –** A reportable incident consists of any act that violates an explicit or implied security policy within the DOC or its operating units. More specifically, an incident is any adverse event that threatens the security of information resources. Incidents may include, but are not limited to:
  - Compromise of integrity - when a virus, trojan, or worm infects a system or network;
  - Denial of service attack - when an attacker has disabled a system or a network worm or trojan has used all available network bandwidth;
  - Loss of accountability/misuse - when an intruder or insider uses an account or a system for unauthorized or illegal purposes;
  - Damage to any part of the system - when a virus, trojan, worm, or disgruntled federal employee or contractor destroys data; and
  - Compromise of confidentiality/intrusion - when an unauthorized outsider gains access to your IT resources.
- **Dial-up Access** – Remote connectivity using a modem device to "call" another system over a public telephone line. Such access may utilize analog services, Integrated Services Digital Network (ISDN) service, or DSL telephone service.

- **DOC-Owned/Furnished Resources** – DOC-owned/furnished resources is government equipment including computers, other hardware devices, software, and data that are owned by the Department of Commerce and are provided to remote users for use in their official duties.

- **Firewall** – A firewall is a general term for a network perimeter or border router device (may be hardware, software, or both) designed to prevent unauthorized access to or from one networked environment to another networked environment. A computing environment may consist of one or more firewall devices that each protects specific segments of the internal DOC networked environment. The outermost of these devices would face the public Internet. Firewalls can be configured to examine all messages entering or leaving a DOC network and block those messages that are not explicitly allowed by the firewall configuration rules.
- **Forensic Examination** – Forensic examination is the detailed inspection of computer memory and storage media to confirm or deny the occurrence of compromised information and applications, and if compromised, the extent to which information was compromised.
- **Information Sensitivity** – Information sensitivity reflects the relationship between the characteristics of the information processed (e.g., personnel data subject to protection under the Privacy Act) and the mission need to ensure the confidentiality, integrity, and availability of the information (e.g., legal requirements to protect confidentiality of personal data). Sensitivity may vary from low, to medium, to high. During the system risk assessment, the system owner must determine the sensitivity, or reaction, of the agency's mission to compromises of confidentiality, integrity, and availability of the information stored and processed by the system. This determination, along with the likelihood of compromise occurring, establishes the level of security adequate to protect the data as required by OMB Circular A-130, Appendix III. The system owner must identify the management, technical, and operational controls necessary to provide the required protection.
- **IT Resources** – In this policy, information technology (IT) resources consist of computer hardware, software, firmware, electronic data, networks, and support for these assets.
- **IT System** – In this policy, an IT "system" is a generic term used to refer to a networked computing environment, a shared server, or a personal computer (PC) under the management control of a DOC official.
- **Local Area Network (LAN)** – Computer network that spans a relatively small area, such as a single building or group of buildings.
- **Personally-Owned Resources** – Computers, other hardware devices, and software, owned by the remote access user.
- **Public-Access Equipment** – Computers and other hardware devices owned by a party other than the Department of Commerce or the remote user, to which the unrestricted access by the general public is allowed.
- **Remote Access** – Remote access uses telecommunications to enable authorized access to non-public DOC computing services that would otherwise be inaccessible from work locations outside the established DOC local area network or DOC-controlled wide area network computing environment. This includes access to non-public DOC IT systems and

data that are exposed to the public Internet (e.g., web access to electronic mail by the home user or business traveler) as well as modem dial-up and/or Virtual Private Network (VPN) access to internal DOC IT servers and desktop workstations.

- **Remote Location** – A remote location is a work location at which the worker is not able to connect his/her computer directly to the DOC local area network or DOC-controlled wide area network that contains the systems needed for official duties. This includes a worker's home, a traveler's hotel room, or an emergency worker's field location. Work from remote locations requires the use of telecommunications capabilities such as dial-up modems, Internet connectivity, or wireless networks to access DOC IT systems and data for official duty purposes.
- **Remote User** – Any user who requires access to DOC IT systems from a remote location. Users may include DOC federal employees and contractors, employees of other federal agencies who require remote access to DOC systems, and remote researchers processing DOC information.
- **Sanitization** – System sanitization is a process whereby the storage media of a compromised system is "erased" in order to remove all traces of compromise or sensitive government information.
- **Senior Program Officials** – Senior program officials are upper-level managers in charge of line offices who are direct reports to the Operating Unit Head. For example, if the Operating Unit Head is an Under Secretary, then the senior program officials are the assistant secretaries or office directors, as applicable; if the Operating Unit Head is a Director, then the senior program officials are the associate directors.
- **System Owners** – System owners are mid-level managers responsible for day-to-day system operations.
- **Telework/Telecommuting** – Telework occurs when managers and supervisors of DOC employees, or COTRs of DOC contractors, authorize paid employees to carry out all, or a part of, their work away from their normal places of business, usually at home or from an established government telework center.
- **Virtual Private Network (VPN)** – A virtual private network is a private "tunnel" through a public network (i.e., the Internet). For example, there are a number of systems that enable creation of networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
- **Wide Area Network (WAN)** – A wide area network consists of the connection of many LANs over any distance via telephone lines and radio waves.
- **Wireless LAN (WLAN)** – A wireless LAN consists of a network that uses radio waves rather than wires to communicate between nodes.