Commerce Information **CITR-002**
Technology Requirement **June 13, 2008**

Office of the Chief Information Officer

Safeguarding Data on Foreign Travel

1. PURPOSE

The added reach and productivity enabled by mobile devices, such as laptops, Personal Data Assistants (PDA), and portable media devices, makes their use a business imperative. However, these devices extend the boundary of the Commerce infrastructure and inevitably add risk, which must be properly mitigated. One particular area of risk which must be addressed is the exposure of these devices to the myriad of threats prevalent while on foreign travel. In using these devices, due diligence is necessary to protect the Commerce infrastructure and the integrity and confidentiality of information transmitted to and from these devices.

The purpose of this document is to establish policy for the Department of Commerce (DOC) Operating Units (OUs), and Offices and to provide direction and requirements for safeguarding mobile devices while on foreign travel.

2. SCOPE

This policy covers all DOC laptops, PDA, and portable media devices used on foreign travel.

3. APPLICABILITY

The requirements set forth in this policy apply to all DOC employees and staff who use mobile devices, such as laptops, PDAs), and portable media devices to read, store, or process information, or who use these devices for remote access and to read email and other electronically transmitted and stored data.

4. AUTHORITY

The 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 Chief Information Security Officer (CISO) shall ensure that IT security policy and requirements are developed consistent with applicable statutory authority, including the Clinger-Cohen Act and the 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 policy augments existing policy in DOC IT Security Program Policy and Minimum Implementation Standards (2005). Specifically, these requirements provide additional clarity to the following sections:

a. 1720 What is DOC Policy for AC-19 Access Control for Portable and Mobile Devices?
b. 1721 What is the DOC policy for AC-20 Personally Owned Information Systems?
c. 19.19 What is the DOC policy for SC-18 MOBILE CODE?
d. APPENDIX D: Unclassified System Remote Access Security

In addition, this policy complements two Department memoranda stressing the need for protection of sensitive, including the use of encryption.

a. Deputy Secretary of Commerce Memorandum, Safeguarding Personally Identifiable Information, November 6, 2006.
b. CIO Memorandum, Safeguarding Personally Identifiable Information, December 12, 2006.

6. REQUIREMENTS

All DOC Offices and OUs shall comply by creating procedures, or modifying existing procedures, that meet the following requirements:

General:

a. Only DOC-issued mobile devices that meet existing security requirements set forth by the Department and the OUs (e.g., NIST Special Publication 800 -53) are authorized for use on foreign travel.
b. Travelers must ensure physical security of device while in transit (i.e., do not check with luggage) and while on foreign travel and/or foreign duty (i.e., do not leave unattended).
c. OUs shall also make full use of travel briefings provided by the Office of Security (OSY) and threat awareness information in the Office of Executive Support.
d. Report immediately the loss, theft, or compromise of assigned mobile devices while on travel to the DOC and OU Computer Incident Response Team (CIRT), as appropriate.

Personal Data Assistants:

a. The only PDA authorized for use in support of foreign travel is a BlackBerry device without removable memory cards.
b. BlackBerry devices shall configured to use encryption and disallow the down-load of unauthorized software or applications.
c. OUs shall utilize, AutoBerry, the Department's configuration audit and software control tool, to capture and maintain baseline configurations for all BlackBerry devices.
d. OUs shall use AutoBerry to scan all BlackBerrys used before and after each trip.
e. If the DOC provided tool detects high or moderate risks, the device must be wiped, reloaded, and re-baselined before it is returned to its owner. OUs should use their discretion in evaluating and addressing any low risks detected.
f. OU Information Technology Security Officer (ITSO) shall, if possible, ensure the creation of an image copy of all BlackBerry device's found to have high risks before the device is wiped. The OU ITSO shall send these images to the DOC Computer Incident Response Team (DOC CIRT) for further analysis.
g. AutoBerry is restricted for U.S. Government use only. AutoBerry will not be used on any networked device. In addition, AutoBerry will not be taken outside the United States unless a waiver is requested through the Office of the CIO. OU CIOs are responsible for ensuring the software's limited distribution.

h. The OU CIO or the ITSO should send requests for the software or software updates via email to the DOC CISO.

Laptops:

a. Only DOC issued laptops from a loaner pool shall be utilized during foreign travel.
b. Laptops should only be taken on foreign travel, if there is a pressing business need and management-level concurrence is obtained.
c. Laptops should only be taken on foreign travel, if there is a pressing business need and management-level concurrence is obtained.
d. All laptops are required to have full-disk encryption.
e. All laptops will be loaded with a personal firewall.
f. The OU CIO shall assess the risk exposure of the laptop given the travel destination. A risk assessment should be made by consulting the latest threat information from the Office of Executive Support. Given the assessment, CIOs can decide the actions, such as scanning or wiping, that are best suited for the situation. At a minimum, The OU CIOs shall ensure appropriate procedures are in place to scan all laptops assigned to DOC employees before they are reconnected to the Department's networks.
g. The only remote access permitted will be through encrypted DOC Web-based email, preferably with Two Factor Authentication or an authorized, encrypted DOC Virtual Private Network with Two Factor Authentication.
h. No personally-owned laptops shall be used on foreign travel to perform DOC-related work. Any personally owned computer taken to a foreign country for any reason shall not be connected to the DOC infrastructure, physically or via VPN.

Portable Media Controls:

a. Only DOC assigned portable media, including CD-Rom, USB drives, diskettes, etc., that are encrypted with FIPS 140-2 validated encryption should be used while on foreign travel.
b. No portable media provided by non-DOC staff, i.e., foreign officials, shall be used on loaner laptop or interconnected to any DOC computer or system.

7. REFERENCES

a. U.S. Department of Commerce IT Security Program Policy and Minimum Implementation Standards (2005).
b. Deputy Secretary of Commerce Memorandum, Safeguarding Personally Identifiable Information, November 6, 2006.
c. CIO Memorandum, Safeguarding Personally Identifiable Information, December 12, 2006.
d. NIST Special Publication 800-53 rev 1.
e. Title III of the E-Government Act of 2002, the Federal Information Security Management Act (FISMA.)
f. OMB M-07-16 , Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)
g. M-06-16, Protection of Sensitive Agency Information (June 23, 2006)

Chief Information Officer

June 13, 2008