




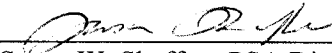
# POLICY STATEMENT

Policy Statement 2011

Policy Area: Information Technology

Effective Date:

Approved:   
Paul A. Quander, Jr., Director

  
Susan W. Shaffer, PSA Director

## NETWORK SECURITY POLICY

### I. COVERAGE

This policy covers all permanent, temporary, and part-time employees of the Court Services and Offender Supervision Agency (CSOSA) and the Pretrial Services Agency (PSA) (hereinafter referred to collectively as the Agency), as well as interns, and contractors, and other non-Agency personnel who access the Agency automated information systems (i.e., email, servers, etc.). The term "employee" as used in this policy covers all of these categories.

### II. BACKGROUND

Securing the Agency's Information Technology (IT) Architecture is an important Agency objective and is required by Federal law. OMB Circular A-130 and Presidential Decision Directive 63 requires the IT organization to secure the infrastructure. Because external networks and Internet sites are not trustworthy, our internal network is vulnerable to misuse and attack. In order to minimize security risk(s), the Agency has implemented firewalls, security policies and other initiatives to secure our automated systems. These initiatives will provide methods for:

- Blocking unwanted/harmful network traffic
- Directing incoming traffic to trustworthy internal systems
- Hiding vulnerable systems which cannot easily be secured from the Internet
- Hiding information such as system names, network topology, network device types, and internal user ID's from the Internet
- Reducing vulnerabilities and threats to Agency automated systems

Network security has been configured to be transparent to internal network users.

### III. POLICY

This policy establishes the rules and guidelines for the Agency's network. All users who require access to the internal (local area network, servers, etc.) and external network (Internet, other agency systems) must do so by using Agency approved software, hardware and Internet gateways. This policy prohibits the use of modems, wireless network communication devices, network tunneling software or any other hardware or software that may be used to circumvent the Agency network security architecture.

#### **IV. AUTHORITIES, SUPERSEDURES, REFERENCES, AND ATTACHMENTS**

##### A. Authorities

OMB Circular No. A-130 Appendix III (Security of Federal Automated Information Resources) [http://www.whitehouse.gov/omb/circulars/a130/a130appendix\\_iii.html](http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html)

Protecting America's Critical Infrastructure – Presidential Decision Directive 63

##### B. Supersedures

None

##### C. Procedural References

Request for Computer Access (CSOSA/IT-0001)  
<http://csosaweb/forms/computeraccess.pdf>

##### D. Attachments

Appendix A. General Procedures

## **APPENDIX A DEFINITIONS**

**Authorized Device** – Any device that has been issued or approved for use by the Agency’s IT organization.

**Firewalls** – A computer or computer software that prevents unauthorized access to private data (on a local area network or Intranet) by outside computer users (i.e., Internet, external entities).

**Non-authorized Device** – Any device that has not been issued or approved for use by the Agency’s IT organization. This includes personal computer equipment.

**Protocols** – A set of conventions governing the treatment and especially the formatting of data in an electronic communications system.

**Virtual Private Network (VPN)** – Provides advanced encryption and tunneling to permit secure, end-to-end, connections over third-party networks, such as the Internet.

**Wireless devices** – Devices that can communicate with a network without being physically connected.

**APPENDIX A  
GENERAL PROCEDURES**

- A. The Agency has blocked access to some external locations/sites (websites, instant messaging, etc.). Employees who have a business need for a particular website or service that is currently blocked, must send a written request through their manager to the Agency Chief Technology Officer.
- B. External locations/sites or protocols that are deemed harmful to the Agency IT environment will be blocked or removed without warning.
- C. Local Area Network connections (LAN drops) will only be active if an authorized device is connected/assigned to that connection.
- D. Employees are prohibited from installing any device on the Agency network. Non-authorized devices connected to or communicating with the Agency network will be removed without warning and the connection disabled. Guidelines for Local Area Network connections are:
  - 1. All LAN connection requests must be made through the Help Desk.
  - 2. Activation will be permitted for authorized equipment only.
  - 3. Connections will be deactivated when a device is removed or relocated.
  - 4. Random and quarterly audits will be performed to ensure that unnecessary connections are not active.
- E. Users are prohibited from operating modems and wireless network devices within the Agency environment. Any requirement for a modem or wireless device must follow the procedure outlined in this policy. Non-authorized devices will be removed without warning and the connection will be disabled. The guidelines for modem/analog and wireless devices are:
  - 1. Request must be made through the Help Desk.
  - 2. IT Security will contact the requestor to gather information on the requirement for the device. IT Security will review all requests. No device can be used or installed unless approved by IT Security.
  - 3. Connections will be removed when a device is removed or relocated.
  - 4. Random and quarterly audits will be performed by the CSOSA Information Security Officer to ensure that unnecessary connections are not active.
- F. Authorized modem/analog connections will be dial-out only.
- G. Systems with modems will not have network connections.

- H. Remote and dial-in access is only allowed via the Office of Information Technology approved secure communication solutions.