



District of Columbia Pretrial Services Agency

Policy Statement 5552

Policy Area: Information Technology

Effective Date: April 21, 2005

# Management Instruction

Approved:

Ronald L. Hickey

Director, OIT

---

## SECURITY AWARENESS AND TRAINING CONTROL FOR PSA BUSINESS AND MISSION CRITICAL SYSTEMS

### I. MANAGEMENT INSTRUCTION

The District of Columbia Pretrial Services Agency's (PSA) business and mission critical systems must be supported by adequate security awareness and training control. The controls are required to be implemented and monitored as described in this Management Instruction, and as mandated and authorized by PSA Policy Statement #5502, *Security Awareness and Training Policy for PSA Business and Mission Critical Systems*.

### II. COVERAGE

This Management Instruction applies to all permanent and temporary PSA employees, including contractors and interns that use, manage, develop, maintain, or support PSA business and mission critical systems. The term employee as used in this management instruction, collectively refers to all of the aforementioned personnel types.

### III. BACKGROUND

Security awareness and training includes awareness programs that emphasize the importance of security and the adverse consequences of security failure, and training programs that equip personnel with security related roles and responsibilities and with the knowledge and practical application capacities necessary to achieve security objectives.

Security awareness and training is mandated by the Federal Information Security Management Act (FISMA). Federal agencies must provide mandatory, periodic training in computer security awareness and accepted computer security practices for all personnel who are involved with the management, use, support, maintenance, or operation of Federal information systems within or under the supervision of the Federal agency. Awareness training is required prior to

granting access to PSA systems and as ongoing refresher training for maintaining rights and privileges associated with continued access, management, and support of PSA systems.

## IV. PROCEDURES

### A. Definitions

This Management Instruction outlines procedures for adequate security awareness and training supported by process and technology. Security awareness and training gives PSA employees, contractors and interns the required security knowledge and skills to maintain the confidentiality, integrity and availability of the systems and information they work with.

### B. Terms

- **Security Awareness** - Awareness is not training. The purpose of awareness is simply to focus attention on security. Awareness presentations give the audience the ability to recognize IT security concerns and respond accordingly.
- **Security Roles and Responsibilities** - Designation of security control responsibilities to specific individuals who are tasked with specific development, implementation, monitoring, maintenance, and enforcement duties.
- **Security Training** – The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on security issues. Produces relevant and needed security skills and competencies for practitioners of functional specialties other than IT security (e.g., management, systems design and development, system and network administrators, acquisition personnel, auditing).

### C. Authority

FISMA requires PSA to institute procedures to facilitate the implementation of a Security Awareness and Training Policy. The procedures are derived from guidance provided by the National Institute of Standards and Technology Special Publication 800-53, Draft 2, *Recommended Security Controls for Federal Information Systems*.

### D. Requirements

The following security awareness and training procedures are required to be implemented, practiced, and monitored as described in this Management Instruction, and as mandated and authorized by PSA Policy Statement #5502, *Security Awareness and Training Policy for PSA Business and Mission Critical Systems*.

These procedures meet the minimum baseline for systems with a security categorization of *Moderate*. Deviations from or enhancements to these baseline procedures will be documented with rationale (e.g., mitigating factors, risk acceptance, resource constraints, etc.) and approval, in the System's Security Plan (SSP).

- All employees, including managers, senior executives, contractors and other users of business and mission critical systems that support the operations and assets of the organization, will receive security awareness training that informs them of the information security risks associated with their activities and their responsibility to comply with organizational policies and procedures designed to reduce these risks.
- All employees with significant information system security roles and responsibilities will be identified and their roles and responsibilities documented. These employees will be provided with appropriate information system security training to accomplish the goals of all information security policies, management instructions, and associated plans.
- Content of security awareness and training will be based on the following security knowledge requirements:
  - **Executive Management** needs to fully understand directives and laws that form the basis for the security program. They also need to comprehend their leadership roles in ensuring full compliance by users within their units.
  - **Business Owners** must have a broad understanding of security policy and a high degree of understanding of the consequences of impact to operations in the event of system or information compromise.
  - **System Managers** must have a broad understanding of security policy and procedures and a high degree of understanding regarding security controls and requirements applicable to the systems they manage.
  - **System Security Officers** act as expert consultants for their organization and therefore must be well educated on security policy and accepted best practices.
  - **Office of Information Technology Support Personnel, Network and System Administrators** require a high degree of security awareness and training on security controls and rules of behavior for systems they support along with specialized training in operational security controls such as configuration management, access control, disaster recovery, incident response, and other process oriented control areas.

- **Office Directors, Supervisors, and System Users** need a high degree of security awareness and training on security controls and rules of behavior for systems they use to conduct business operations.
- Individual information system security training activities will be documented and monitored including basic security awareness training and specific information system security training using the PSA Training and Development Center’s Learning Management Tool.

**E. Roles and Responsibilities**

A current list of roles and responsibilities will be maintained delineating responsibilities for executing, managing, monitoring and enforcing the procedures in this management instruction.

**Table I – Security Awareness and Training Roles and Responsibilities**

Role	AT Responsibilities
PSA Office of Information Technology	<ul style="list-style-type: none"> <li>● Develop and implement security awareness and training policies and procedures.</li> <li>● Procure or produce in-house required security training.</li> <li>● Coordinate with PSA Training and Career Development Center for security awareness and training logistics and documentation of individual employee participation in security awareness and training.</li> </ul>
PSA Training and Career Development Center	<ul style="list-style-type: none"> <li>● Coordinate with PSA Office of Information Technology for security awareness and training logistics and documentation of individual employee participation in security awareness and training.</li> <li>● Document individual employee completion of security awareness and training.</li> </ul>
CSOSA Office of Information Technology	<ul style="list-style-type: none"> <li>● Produce and deliver security awareness training to all PSA employees.</li> </ul>
<ul style="list-style-type: none"> <li>● Office Directors</li> <li>● Office Deputy Directors</li> <li>● Managers</li> <li>● Supervisors</li> </ul>	<ul style="list-style-type: none"> <li>● Ensure that employees who report to them receive adequate security awareness and training.</li> </ul>
System and IT Administrators	<ul style="list-style-type: none"> <li>● Attend required courses on security awareness and training.</li> </ul>
System Users	<ul style="list-style-type: none"> <li>● Attend required courses on security awareness.</li> </ul>

**F. Authorities and References**

- PSA Policy Statement #5500 *Global Information Technology Security Policy for PSA Business and Mission Critical Systems*

- PSA Policy Statement #5502 *Security Awareness and Training Policy for PSA Business and Mission Critical Systems*
- Federal Information Security Management Act of 2002 (FISMA)
- OMB Circular A130, Appendix III
- Recommended Security Controls for Federal Information Systems (NIST SP 800-53)
- An Introduction To Computer Security – The NIST Handbook (NIST SP 800-12)
- Building an Information Security Awareness and Training Program (NIST SP 800-50)

**G. Attachments**

- Security Control Reference Guide