



District of Columbia Pretrial Services Agency

Policy Statement 5554

Policy Area: Information Technology

Effective Date: April 21, 2005

Management Instruction

Approved: _____

Ronald L. Hickey

Director, OIT

CERTIFICATION, ACCREDITATION, SECURITY AND RISK ASSESSMENT INSTRUCTIONS 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 adhere to certification, accreditation, security, and risk assessment control requirements. The controls are required to be implemented and monitored as described in this Management Instruction, and as mandated and authorized by PSA Policy Statement #5504 *Certification, Accreditation, Security, and Risk Assessment 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

The Federal Information Security Management Act (FISMA) requires that all Federal agencies develop and implement an information security program designed to safeguard business and mission critical systems, information, and related IT assets. Certification, accreditation, security and risk assessments are integral and necessary activities of an information security program before a system can be granted authorization to operate, for supervising interconnected systems, and for continuous monitoring.

Risk assessment is a methodical approach, including an examination of the juxtaposition (i.e., exploit) of vulnerabilities and threats, existing controls, the likelihood of a resulting exploit, and the potential impact to the organization and people in the event of its occurrence. The results of a risk assessment assist an

organization in selecting technical and procedural controls required to achieve adequate security for the system.

IV. PROCEDURES

A. Definitions

This Management Instruction outlines instructions and procedures for adequate certification, accreditation, security, and risk assessment control supported by process and technology.

Certification and Accreditation (C&A) and initial and ongoing security and risk assessments of Federal business and mission critical systems are required by law. The C&A process is a comprehensive, organized, and methodical process mandated by the Office of Management and Budget (OMB) Circular A-130, Appendix III, and guided procedurally by the National Institute of Standards and Technology (NIST). When performed, documented, and reviewed in accordance with the intent of the guidance and with a goal of secure information systems, C&A is an effective top-down approach to achieving the security objectives of business and mission critical systems and instituting a security-minded organizational culture.

Periodic assessments of risk, including evaluation of the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, are required for maintaining and updating security controls.

B. Terms

- **Accreditation** - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
- **Certification** – Detailed analysis of the technical and non-technical security features of a system and appraisal of those security features as to whether they are operating as intended.
- **Certification Agent** - Independent agent (e.g., contractor) performing security tests and evaluations (ST&Es) and supplying report to the Director of the PSA Office of Information Technology.
- **FIPS** – Federal Information Processing Standards are the security standards for Federal Information and Information Systems. These standards involve centralized access control, process verification, real-time transaction auditing

and reporting. FIPS 199 is the standard for determining the security categorization (low, moderate, or high) of a system.

- **Monitoring** – An ongoing activity that checks on systems, users, and environment. Systems should be monitored to detect unauthorized activity, check for deviations from the IT Security Policy, and to verify the effectiveness of the security controls.
- **Risk Assessment** – The process of analyzing vulnerabilities, threats, likelihood, and impact to an information system to determine the risks (i.e. potential for losses), and using the analysis as a basis for identifying appropriate and cost-effective security measures.
- **SDLC** – See System Development Life Cycle. Details of the SDLC can be found in the PSA SDLC Handbook
- **Security Controls** – Measures that are taken to protect information systems. Typically categorized into management, operational, and technical controls. Management and operational controls are also known as administrative, procedural or process controls. Technical controls encompass software, hardware and/or firmware security measures. These sub-types are defined by NIST as follows:
 - **Management Controls** - The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
 - **Operational Controls** - The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
 - **Technical Controls** - The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
- **System** - Components organized to accomplish a specific function or set of functions.
 - **Business Critical System** - IT systems comprised of technology and users within physical and logical boundaries that support organizational mission.
 - **Mission Critical System** - IT systems comprised of technology and users within physical and logical boundaries that support PSA's or other organization's mission(s).
- **Vulnerability** - A weakness in the procedural, mechanical, electronic or other system condition that has the potential to be exploited by a threat.

C. Authority

The Federal Information Security Management Act (FISMA) requires PSA to institute procedures to facilitate the implementation of a Certification, Accreditation, Security, and Risk Assessment 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 certification, accreditation, security and risk assessment control procedures are required to be implemented, practiced, and monitored as described in this Management Instruction, and as mandated and authorized by PSA Policy Statement #5504, *Certification, Accreditation, Security and Risk Assessment Policy for PSA Business and Mission Critical Systems*.

The following technical and process requirements 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., compensating controls, mitigating factors, risk acceptance, resource constraints, etc.) and approval in the system's Security Plan (SSP).

- In support of the certification and accreditation and continuous monitoring process, an assessment of the security controls in the information systems will be conducted at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- All connections from the information system to an information system outside the accreditation boundary will be authorized and monitored/controlled on an ongoing basis.
- Information system interconnection agreements must be reviewed and approved by appropriate PSA officials.
- A security certification will be conducted in support of the Office of Management and Budget (OMB) requirement for accrediting the information system.
 - The security certification will be integrated into and span the System Development Life Cycle (SDLC) of business and mission critical systems.
- A plan of action and milestones (POA&M) for business and mission critical systems will be developed and updated quarterly, documenting

planned, implemented, and evaluated remedial actions to correct any deficiencies noted during assessments of the security controls or as a result of other observations or circumstances (e.g., day-to day operations, incidents, periodic vulnerability scans, etc.) and to reduce or eliminate known vulnerabilities in the system.

- The POA&M will be attached to the System Security Plan and included in the security accreditation package.
- Business and mission critical systems will be authorized (i.e., accredited) for processing.
 - Business and mission critical systems must comply with the requirements of the following regulation and guidance, to complete the activities necessary to receive either an official authorization to operate (ATO) or an interim authorization to operate (IATO).
 - OMB Circular A-130, Appendix III
 - NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and
 - NISP SP 800-64. *Security Considerations in the Information System Development Life Cycle*.
- Accreditation requires the following activities be conducted:
 - Physical and logical boundaries for each business and mission critical system will be established and reviewed annually for any changes.
 - The information system and information stored, processed, and transmitted will be categorized for worst case impact in accordance with FIPS 199, *Security Categorization of Federal Information and Information Systems*. The System Manager will document the security categorization (including supporting rationale) in the system security plan. The security categorizations will be reviewed and approved by designated senior-level officials. Security categorization analyses will include participation of mission support management and PSA Office of Information Technology management.
 - Risk assessments will be conducted to determine the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that support the operations and assets of the agency.
 - Risk assessments will take into account all that is known about vulnerabilities, threat sources, likelihood of exploit, and security controls planned or in place to determine the resulting level of residual risk posed to PSA operations, PSA assets or individuals and the level of impact caused to agency mission and people.

- Risk assessments will be performed annually or whenever there are significant changes to the information system, the facilities where the system resides or other conditions that may impact the security or accreditation status of the system.
 - Security tests and evaluations of the controls identified in the System Security Plans will be performed prior to certification.
 - Certification of the business and mission critical systems will be conducted upon any major change to PSA business and mission critical systems and at least every three years.
- A plan for continuous monitoring will be implemented and maintained.
 - Selection criteria for control monitoring will be established and a subset of the security controls employed within the information system for purposes of continuous monitoring will be selected.
 - Continuous monitoring activities will include comprehensive configuration management activities supported by a plan that controls changes in information system components, includes security impact analyses of changes to the system, ongoing assessment of security controls and status reporting.
 - Specific criteria will be developed and documented for what is considered significant change to each information system.

E. Roles and Responsibilities

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

Table I – Roles and Responsibilities

Role	CA-RA Responsibilities
PSA Executive	<ul style="list-style-type: none"> ● Signs and approves memorandums of understanding; approve interconnection agreements.
Authorizing Official	<ul style="list-style-type: none"> ● Authorizes system operations/processing.
Certification Agent	<ul style="list-style-type: none"> ● Performs security tests and evaluations (ST&Es) and supplying report to the Director of the PSA Office of Information Technology.
Director, PSA Office of Information Technology	<ul style="list-style-type: none"> ● Selects Certification Agent. ● Prepares Accreditation Package. ● Submits POA&M via appropriate OMB reporting channel. ● Manages the continuous monitoring process

<ul style="list-style-type: none">• System Security Officer• System Manager	<ul style="list-style-type: none">• Manage and perform risk assessments.• Ensure SSP and POA&M are current and accurate.• Monitor interconnections.
----------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

F. Authorities and References

- PSA Policy Statement # 5500 *Global Information Technology Security Policy for PSA Business and Mission Critical Systems*
- PSA Policy Statement #5504 *Certification, Accreditation, Security and Risk Assessment Policy for Business and Mission Critical Systems*
- Federal Information Security Management Act of 2002 (FISMA)
- OMB Circular A130, Appendix III
- Federal Information Processing Standards Publication (FIPS 199), Standards for Security Categorization of Federal Information and Information Systems
- Guide for the Security Certification and Accreditation of Federal Information Systems (NIST SP 800-37)
- Recommended Security Controls for Federal Information Systems (NIST SP 800-53)
- Risk Management Guide For Information Technology Systems (NIST SP 800-30)
- An Introduction To Computer Security – The NIST Handbook (NIST SP 800-12)
- Guide For Developing Security Plans For Information Technology Systems (NIST 800-18)
- Security Considerations in the Information System Development Life Cycle (NIST SP 800-64)

G. Attachments

- Security Control Reference Guide