



District of Columbia Pretrial Services Agency

Policy Statement 5558

Policy Area: Information Technology

Effective Date: April 21, 2005

# Management Instruction

---

Approved: 

Ronald L. Hickey

Director, OIT

## INCIDENT RESPONSE 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 employ adequate incident response control. The controls – both technical and procedural – are required to be implemented and monitored as described in this Management Instruction, and as mandated and authorized by PSA Policy Statement #5508, *Incident Response 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

A computer security incident is an adverse event in a computer system or network caused by a failure of a security mechanism or an attempted or threatened breach of a security mechanism. Computer security incidents have become more common and their impact far-reaching. When faced with an incident, an organization should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident.

### IV. PROCEDURES

#### A. Definitions

This Management Instruction outlines procedures for adequate incident response supported by process and technology. An effective and efficient incident response and handling capability will enable PSA to respond quickly to

security mechanism failure or breach, thereby minimizing the potential for any ensuing or protracted impact to the confidentiality, integrity and/or availability of its business and mission critical systems and information.

## **B. Terms**

- **Incident Examples** - Unauthorized network scans or probes; successful and unsuccessful system intrusions; unauthorized use of system privileges; and execution of malicious code on an IT resource.
- **Lessons Learned** – Upon review of incident handling, a determination of the effectiveness and efficiencies of measures, roles, responsibilities and other dynamics that could improve the prevention and handling of incidents.
- **Security Incident** – Any event that has resulted in: unauthorized access to, or disclosure of, sensitive information; unauthorized modification or destruction of system data; reduced, interrupted, or terminated data processing capability; introduction of malicious program or virus activity; or the degradation or loss of the system's confidentiality, integrity or availability; or the loss, theft, damage or destruction of an IT resource.
- **Suspicious Activity** - Any activity that is: an abnormal system event occurrence for a given system that cannot be immediately explained, but does not pose an immediate threat; observed recurring activity that possibly indicates attempts are being made to exploit a vulnerability but is countered by security controls in place; sporadic repeated activity that cannot be readily explained by system operations and security staff; activity that, when combined with other factors or anomalous events, indicates a possible cause for concern.
- **Track IT™** - Licensed software tool manufactured by Intuit, used to track help desk, change, inventory, requisition, and other information technology (IT) processes.

## **C. Authority**

The Federal Information Security Management Act (FISMA) requires PSA to institute procedures to facilitate the implementation of an Incident Response 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 incident response procedures are required to be implemented, practiced, and monitored as described in this Management Instruction, and as mandated and authorized by PSA Policy Statement #5508, *Incident Response 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 (mitigating factors, risk acceptance, resource constraints, etc.) and approval, in the system's Security Plan (SSP).

### Technical Requirements

- Automated mechanisms (e.g., PSA's licensed software tool, Track-IT™, configuration of alerts and associated communications methods such as email and pager) will be employed to:
  - o Support the incident handling process.
  - o Support testing of the incident response plan.
  - o Assist in the tracking of security incidents and in the analysis of incident information (e.g., PSA's licensed software tool, Track-IT™).
  - o Assist in the reporting of security incidents.
  - o Ensure the availability of incident response-related information and support.
- These mechanisms will help facilitate a PSA Incident Response Plan

### Process Requirements

- All security incidents for business and mission critical systems will be tracked and documented on an ongoing basis.
- Incident response and handling instructions will be included in the system rules of behavior.
- Users of business and mission critical systems will be trained in appropriate incident handling requirements dictated by the system rules of behavior.
- An Incident Response Plan will be developed and implemented that defines the requirements and delineates the flow of activities and communications required for incident response.
- IT Personnel will be assigned and trained in specific Incident Response Plan roles and responsibilities
- Refresher training will be provided annually.
  - o Simulated events will be incorporated into incident response training, to facilitate effective response by personnel in crisis situations.

- An incident response and handling capability will be implemented for all security incidents. This capability will include preparation, detection, analysis, containment, eradication and recovery.
- The incident response capability for business and mission critical systems will be tested annually to determine the plan’s effectiveness. The results will be documented.
- Lessons learned from ongoing incident handling activities will be incorporated into the Incident Response Plan and new or modified procedures will be implemented accordingly.
- All incident information, consistent with applicable federal laws, directives, policies, regulations, standards and guidance will be promptly reported to appropriate authorities.
- An incident support resource will be designated and provided to offer advice and assistance to users of the business and mission critical systems for the handling and reporting of security incidents.
  - The support resource will be an integral part of the incident response capability.

**E. Roles and Responsibilities**

A current list of roles and responsibilities will be maintained in the Incident Response Plan that delineates responsibilities for executing, managing, monitoring and enforcing the procedures in this management instruction.

**Table I: Incident Response Control Roles and Responsibilities**

<b>Role</b>	<b>IR Responsibilities</b>
PSA Director of Office of Information Technology	<ul style="list-style-type: none"> <li>• Determine appropriate action upon discovery of any suspicious activity or incident.</li> <li>• Inform System Business Owner and executive management, if necessary, of incidents deemed to present risk to mission operations and performance.</li> <li>• Coordinate response activity with CSOSA.</li> </ul>
System Manager	<ul style="list-style-type: none"> <li>• Determine auditable data types and events to correlate and monitor.</li> <li>• Institute automated mechanisms for correlation and reporting.</li> <li>• Report Incidents to Department of Homeland Security’s Incident Response Center</li> </ul>
System Business Owner	<ul style="list-style-type: none"> <li>• Be informed of any incidents or suspicious activity that may impact mission.</li> </ul>
Incident Response and Audit Compliance Manager	<ul style="list-style-type: none"> <li>• Determine auditable data types and events to correlate and monitor.</li> <li>• Execute Incident Response Plan in the event audit trails indicate suspicious activity.</li> <li>• Report all incidents to CSOSA.</li> <li>• Review audit reports for suspicious activity.</li> <li>• Inform System Manager and Business Owner of suspicious activity.</li> </ul>
System Security Officer	<ul style="list-style-type: none"> <li>• Review audit reports for suspicious activity.</li> <li>• Evaluate System Security Plan (SSP) for needed control enhancements to</li> </ul>

	address suspicious activity.
System Administrator	<ul style="list-style-type: none"> <li>Review audit reports for suspicious activity.</li> </ul>
OIT support	<ul style="list-style-type: none"> <li>Investigate audit trails.</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 #5508, *Incident Response Policy for 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 2<sup>nd</sup> Public Draft)
- Risk Management Guide For Information Technology Systems (NIST SP 800-30A)
- An Introduction To Computer Security – The NIST Handbook (NIST SP 800-12)
- Guide For Developing Security Plans For Information Technology Systems (NIST 800-18)
- Computer Security Incident Handling Guide (NIST SP 800-61)

**G. Attachments**

- Security Control Reference Guide