Court Services and Offender Supervision Agency
for the District of Columbia

Policy Statement

Policy Statement PS 2036
Policy Area: Office of Information Technology
Effective Date: AUG 17 2005

Approved:
Paul A. Quander, Jr., Director

INFORMATION TECHNOLOGY SECURITY POLICY FOR CSOSA BUSINESS AND MISSION CRITICAL SYSTEMS

I. COVERAGE

This Policy Statement applies to all business and mission critical systems and information of the Court Services and Offender Supervision Agency for the District of Columbia (CSOSA). This Policy Statement also applies to all permanent and temporary CSOSA employees, including contractors and interns, that use, manage, develop, maintain, or support CSOSA business and mission critical systems. For purposes of this policy, the term "employee" includes all of the above-mentioned categories. This policy does not apply to the District of Columbia Pretrial Services Agency (PSA). PSA Employees should reference PSA Policies 5500, 5501, 5502, 5503, 5504, 5505, 5506, 5507, 5508, 5509, 5510, 5511, 5512, 5513, 5514, 5515 and 5516.

II. BACKGROUND

Information Technology Security (IT Security) is an integral component to the overall risk management practices performed by CSOSA in the daily operations that support its mission. CSOSA becomes more effective and efficient each and every year by employing increasingly innovative skills and use of newly available information technology systems. This increased capability is accompanied by an increasing dependence on the more intricate and comprehensive support functions that these business and mission critical systems provide. This in turn presents a greater risk to the agency's ability to support its mission in the event of compromise to these systems.

It is now, more than ever, important to institute an effective information technology security program that incorporates contemporary technology, trained people, and effective and efficient process, to strive to eliminate the uncertainty and reduce the risk associated with information system compromise.

As a Federal agency, CSOSA is required to comply with the Federal Information Security Management Act of 2002 (FISMA). FISMA outlines specific information security and assurance requirements and, through the Office of Management and Budget (OMB), directs Federal agencies to subscribe to the standards instituted by the National Institute of Standards and Technology (NIST), and to utilize the guidance that NIST publishes. NIST has developed a catalog of recommended security controls, which are organized by control family. The control families are listed in Table 1.

Acronym	***Table 1 - NIST Control Families***
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Certification, Accreditation, and Security Assessments*
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment*
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
	* Combined by CSOSA into one Policy Area

With the exception of CA and RA, which were combined into Attachment D for purposes of continuity, CSOSA has developed and disseminated a formal, documented policy statement for each control family. These policy statements are included as attachments to this policy. Each policy addresses purpose, scope, roles and responsibilities. Compliance is addressed in Section III of this Policy Statement 2036. The complete list of CSOSA IT security policy statement attachments is found in Table 2 below.

These policy statement attachments represent executive management's commitment to a general understanding of the varied security requirements of its business and mission critical systems. These policy statement attachments also include a statement of determination to require that these systems employ the comprehensive controls necessary for safeguarding the agency's business and mission critical systems, thereby minimizing adverse impact to its mission, the people who serve the mission, and the people for whom the CSOSA mission serves.

CSOSA business and mission critical systems contain valuable and sometimes sensitive government and personal information, which must be protected to prevent disclosure, unauthorized change, and loss. Each aspect of the system, if not properly secured, can be responsible for the introduction of vulnerabilities to the system as a whole or can diminish the effectiveness of other security controls.

On a larger scale, since CSOSA resources are connected to a wider government network, any system compromise is a potential threat on a grand scale to the Federal Government.

Security is the responsibility of every CSOSA employee.

III. POLICY

Definition
IT security encompasses numerous technical and procedural measures that safeguard the systems and information that CSOSA employees rely on to perform their jobs and support the mission areas they serve. These measures, also known as security controls, protect CSOSA's business and mission critical systems from known and unknown, intentional and unintentional threats.

Scope
All CSOSA business and mission critical systems must have both integral internal and external supporting security capabilities to secure the systems and associated information. These capabilities include adequate technology to perform automated security functions that are supported by effective and efficient process managed, performed and facilitated by people with established, defined, and regularly reviewed security related roles and responsibilities.

Purpose
This IT Security Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the security-related objectives of the Federal Information Security Management Act of 2002 and to adequately protect these systems from compromise to the confidentiality, integrity, and availability of the agency's systems and information.

Procedures
The CSOSA Office of Information Technology, in cooperation with pertinent CSOSA and PSA offices (as required by the associated IT security control family policy statement attachments), will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that uniquely facilitates the implementation of each policy statement attachment and includes instructions supported by procedures for implementing and maintaining the requisite baseline controls recommended by NIST. The Operational Instructions will also include a mechanism that requires accountability and compliance.

Compliance
Compliance with this policy and the IT security Operational Instructions is mandatory. Federal employees, including interns, who violate the provisions of

this policy, either by negligence or intent, may be subject to appropriate disciplinary action, up to and including removal in accordance with the standards of conduct, and/or any disciplinary or termination policies. The Contracting Officers Technical Representative will report contractors who violate the provisions of this policy to their employer, who shall determine the appropriate course of action.

IV. AUTHORITIES, SUPERSEDURES, REFERENCES, AND ATTACHMENTS

A. Authorities

- Federal Information Security Management Act of 2002 (FISMA)
- OMB Circular A-130, Appendix III
- The Clinger-Cohen Act of 1996
- Federal Information Processing Standards Publication (FIPS 199), Standards for Security Categorization of Federal Information and Information Systems
- Federal Information Processing Standards Publication (FIPS 140-2) Security Requirements for Cryptographic Modules
- The Privacy Act of 1974 (5 U.S.C. § 552a)

B. Supersedures

None

C. Procedural References

- 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)
- Building an Information Technology Security Awareness and Training Program (NIST SP 800-50)
- Security Guide for Interconnecting Information Technology Systems (NIST SP 800-47)
- Security Configuration Checklists Program for IT Products (NIST DRAFT SP 800-70)
- Contingency Planning Guide for Information Technology Systems (NIST SP 800-34)
- Electronic Authentication Guideline (NIST SP 800-63)
- Computer Security Incident Handling Guide (NIST SP 800-61)

- CSOSA Memorandum: Standards of Employee Conduct, Effective August 30, 1999
- CSOSA Continuity of Operations Plan
- CSOSA Information Technology Continuity of Operations Plan
- CSOSA Information Technology Disaster Recovery Plan
- CSOSA and PSA Policy Statement 4007: *Release of Defendant/Offender Drug Test Information, Effective July 28, 2004*
- CSOSA Management and Administration Directive #500.2, Safeguarding Sensitive, Unclassified Information
- CSOSA: Standards of Employee Conduct, Effective August 30, 1999
- Security for Telecommuting and Broadband Communications (NIST SP 800-46)
- Guide for Developing Security Plans for Information Technology Systems (NIST SP 800-18)
- CSOSA Policy Statement # 5800, *Personnel Security Program*
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security) (NIST SP 800-27)
- Guide to Information Technology Security Services (NIST SP 800-35)
- Guide to Selecting Information Technology Security Products (NIST SP 800-36)
- Security Considerations in the Information System Development Life Cycle (NIST SP 800-64)
- Recommendation on Key Establishment Schemes (NIST 800-56)
- Recommendation for Key Management (NIST 800-57)

D. Attachments

Appendix	*Table 2 - CSOSA IT Security Policy Statement Attachments*
A	Access Control
B	Awareness and Training
C	Audit and Accountability Control
D	Certification, Accreditation, Risk and Security Assessments*
E	Configuration Management
F	Contingency Planning
G	Identification and Authentication Control
H	Incident Response
I	Maintenance Control
J	Media Protection Control
K	Physical and Environmental Protection
L	Security Planning Control
M	Personnel Security
N	System and Services Acquisition Control
O	System and Communications Protection
P	System and Information Integrity Control
* Combination of Families CA and RA	

Appendix A
Access Control

1. Background

Access control minimizes the extent to which a user can intentionally or unintentionally compromise a system and its information. A confidentiality breach could result in the release of sensitive information to unauthorized persons. An integrity breach could result in an addition, alteration, or deletion of system data. A loss of availability could disrupt a system's ability to support the agency's mission for a potentially extended and damaging period of time. Well-implemented access control can protect a system against these threats by only allowing certain individuals access to certain aspects of the system.

2. Definition

Access control is used to specify what persons or processes have access to a specific system resource and the type of access that is permitted. Access control protects CSOSA's business and mission critical systems from unauthorized access, fraud, or abuse. Access control is achieved using technology supported by organizational process.

3. Scope

All business and mission critical systems must have access control capabilities that include adequate technology, effective process, and defined roles and responsibilities, required for securing these systems and associated information.

4. Purpose

This Access Control Policy Statement establishes management's commitment to require and ensure that CSOSA business and mission critical systems accomplish the access control security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including individual accountability, separation of duties, and protection from unauthorized access.

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies access control capabilities that include process, people, and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will:

- Assign and train individuals with distinct duties and defined responsibilities to ensure that access control technology and processes are functional and effective;
- Establish a formal separation of duties, and/or identification of mitigating controls as resource constraints dictate;
- Ensure that the privacy policy and system use notification are known and accepted by all users; and
- Implement, maintain and monitor the controls required by this policy that minimize the likelihood of unauthorized access.

Appendix B
Awareness and Training

1. 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, with the capacities necessary to achieve security objectives.

Security awareness and training is mandated by the Federal Information Security Management Act of 2002 (FISMA). Federal agencies must provide mandatory, periodic training in computer security awareness and accepted computer security practice 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 the system and through ongoing refresher training for maintaining rights to continued access.

2. Definition

Security awareness and training gives CSOSA 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.

3. Scope

All business and mission critical systems must have supporting security awareness and training capabilities that include adequate technology, effective process, and defined roles and responsibilities, required for securing these systems and associated information.

4. Purpose

This Security Awareness and Training Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the awareness and training security-related objectives of the Federal Information Security Management Act. The objectives include communicating and disseminating security policies, procedures, practices and consequences of non-compliance with all permanent and temporary CSOSA employees, including contractors and interns.

5. Procedures

The CSOSA Office of Information Technology, in cooperation with the CSOSA Office of Human Resources Training and Career Development Center will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies a security awareness and training capability. This capability will incorporate people and process supported by adequate technology and accurate records that contribute to constituting secure information systems and fulfills the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will define and maintain a current list of security related roles and responsibilities, including training requirements (both initial and ongoing) and will work with the Training and Career Development Centers of PSA and CSOSA to develop and or select from an appropriate vendor an initial and yearly training curriculum that will be updated annually to include the most recent updates concerning Security Awareness Training.

The CSOSA Office of Human Resources Training and Career Development Center in conjunction with the Office of Information Technology will train identified employees on their roles and responsibilities as it relates to Information Technology Security as well as initial and ongoing training requirements. Training will be conducted/delivered by subject matter experts from the Office of Information Technology through the means which best meets the needs of the agency. This could include training other than instructor lead training. The Training and Career Development Centers of CSOSA and PSA will ensure that courses are advertised to the agency employees and will document attendance of all employees regardless of the delivery method selected.

Office Directors, Office Deputy Directors, Branch Managers, Supervisory Community Supervision Officers and Supervisors will be responsible for ensuring that the employees who report to them complete the required Security Awareness Training.

Appendix C
Audit and Accountability Control

1. **Background**

Audit trails minimize the extent to which users can avoid accountability for their movements and actions within a system. For example, an authorized user could unintentionally alter or view information stored in the system. Although audit trails cannot prevent this from occurring, they provide a means to record the activity and if necessary, hold users accountable for their actions. Monitoring is a continuous activity required for identification of vulnerabilities, security issues, unusual or suspicious user behavior and/or system activities that may have been, and/or continue to be a source of compromise to any or all of the security objectives of confidentiality, integrity, and availability of CSOSA's business and mission critical systems and information.

2. **Definition**

Audit and accountability control includes the technical capability for accurately capturing information and related event elements combined with an organizational review process to capture changes and events attributable to particular users and/or other entities (e.g., interconnected systems, system processes, or objects). Audit and accountability control achieves both preventive and detective security-related objectives.

3. **Scope**

All business and mission critical systems must have access control capabilities that include adequate technology, effective process, and defined roles and responsibilities, required for securing these systems and associated information.

4. **Purpose**

This Audit and Accountability Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the audit and accountability security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including capturing appropriate information changes, problem identification, reconstruction of events, intrusion detection, and individual accountability.

5. **Procedures**

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies audit and accountability capabilities that include process, people, and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The

Operational Instruction will also include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that audit and accountability control technology and processes are functional and effective; and that the requisite audit and accountability technical capabilities of CSOSA business and mission critical systems are implemented, maintained, and monitored.

Appendix D
Certification, Accreditation, Risk and Security Assessments

1. Background

The Federal Information Security Management Act of 2002 (FISMA) requires Federal agencies to develop and implement an agency-wide information security program designed to safeguard information technology assets that support business and mission critical operations. Certification, accreditation, security, and risk assessment are critical components of an information security program and are required before a system can be granted authorization to operate and repeated no longer than every three years.

2. Definition

Certification and Accreditation (C&A) 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 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.

3. Scope

All business and mission critical systems must be certified and accredited. Periodic and regular security, and risk assessment activity accompanied by technology, process, and defined roles and responsibilities, is required for managing risk for these systems and their associated information.

4. Purpose

It is essential that CSOSA officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems.

This Certification and Accreditation, Security, and Risk Management Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the C&A and security and risk assessment security-related objectives of the Federal Information

Security Management Act of 2002 (FISMA). By understanding the risks inherent to the Agency's information systems, CSOSA management can take the necessary steps to manage the risk and minimize the likelihood of threats to mission impact, prior to authorizing the use of the system.

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies certification, accreditation, security, and risk assessment control capabilities that include process, people, and technology to fulfill the requirements of this policy, FISMA, OMB Circular A-130, Appendix III, and associated standards and procedural guidance provided by the National Institute of Standards and Technology (NIST), including:

- Certification and accreditation of business and mission critical systems;
- Periodic security control and risk assessments;
- Execution of requisite memorandums of understanding (MOU), service level agreements (SLA), and interconnection security agreements (ISA) with entities of all interconnecting systems as identified by formal system boundaries definition and in accordance with the security control requirements dictated by a system's impact category (e.g., security categorization of low, moderate, or high);
- Establishment and maintenance of a formal plan of action and milestones (POA&M) for resolving security deficiencies identified by security and risk assessment or other channels; and
- Establishment of a continuous monitoring plan.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that certification, accreditation, security, and risk assessment controls are performed and implemented for its business and mission critical systems.

Appendix E
Configuration Management

1. Background

Configuration management is the systematic identification, documentation, and control of system elements by recording and reporting change and implementation status. These activities assist in verifying compliance with pre-defined and documented system requirements as well as establishing and maintaining the technical integrity of a system throughout its life cycle. The successful implementation of configuration management activities result in an established and documented system baseline, effective management and tracking of changes made to business and mission critical systems and their related supporting documentation (version control). Configuration management is essential for effective risk management.

2. Definition

Configuration management is the systematic identification, documentation, and control of system elements by recording and reporting change and implementation status. The goal of configuration management is to control the integrity of system changes and prevent unintended or unauthorized activity resulting in changes that could compromise the overall functional and IT security objectives of CSOSA business and mission critical information systems.

3. Scope

All business and mission critical systems will be supported by configuration management capabilities that include adequate technology, effective process, and defined roles and responsibilities, required for securing these systems and their information.

4. Purpose

This Configuration Management Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the configuration management security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including protecting business and mission critical systems from unauthorized, inconsistent and undetectable changes which could compromise system integrity and availability, and affect the agency's ability to perform its mission.

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies configuration management capabilities that include process, people, and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will:

- Assign and train individuals with distinct duties and defined responsibilities to ensure that configuration management is organized and effective;
- Establish a well defined system baseline; and
- Identify an efficient change management process supported by a configuration management plan, that tracks application versions (and system elements within a version), limits access for making changes to appropriate personnel, and allows for efficient implementation of system components when changes are necessary.

Appendix F
Contingency Planning

1. Background

Contingency planning minimizes the risk to CSOSA operations by planning for and proving the capability to recover and reconstitute the agency's business and mission critical systems should a disruption or disaster occur. Loss, disruption, or prevention from access to processing, storage, or communications capacity for an extended duration can be caused by power outage, hardware failure, fire, natural disaster, terrorism, or inadvertent data loss or system malfunction. Planning for recovery and/or reconstitution from these events is essential.

2. Definition

Contingency planning is the identification and appropriation of people, process, and materials required to restore mission support operations provided by CSOSA's business and mission critical systems, infrastructure, and systems support personnel in the event of a disruption or disaster that could debilitate these systems.

3. Scope

All business and mission critical systems must be supported by contingency planning capabilities that include adequate technology, process, and established, defined, and rehearsed, roles and responsibilities required for recovery and/or reconstitution of mission and operational support.

4. Purpose

This Contingency Planning Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the contingency planning security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including ensuring that disruptions to systems do not endure to the extent that the CSOSA mission is compromised or incapacitated.

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies contingency planning capabilities that include process, people, and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance. A detailed Disaster Recovery and Continuity of Support Plan will support this Operational Instruction.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities for:

- Preparing and carrying out contingency plans;
- Coordinating regular training, testing, and review; and
- Monitoring and assessing the appropriateness and effectiveness of contingency plans.

Appendix G
Identification and Authentication Control

1. Background

Identification and authentication control minimizes the extent to which an unauthorized user can access a system and compromise its information and to technically correlate system activity with a particular system user or system process.

2. Definition

Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID. Authentication is the means of establishing the validity of a user's claimed identity to the system. The most common form of authentication is a password.

3. Scope

All business and mission critical systems must include an identification and authentication capability that includes adequate technology, process, and established and defined roles and responsibilities required for instituting, supporting, and maintaining adequate identification and authentication control.

4. Purpose

This Identification and Authentication Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the access control security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including technically equipping business and mission critical systems with identification and authentication control that:

- Requires users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise.
- Correlates Actions to Users. CSOSA business and mission critical systems will internally maintain the identity of all active users and be able to link actions to specific users.
- Includes maintenance of existing and termination of inactive user IDs.
- Is accompanied by authentication using one or a combination of:
  - that which a user knows (i.e., password);
  - that which a user has (e.g., token, smart card); or
  - that which a user is (e.g., via biometric or recognition device).

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies an identification and authentication capability that includes process, people, and technology to constitute secure information systems and fulfills the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that identification and authentication technology and process is functional and effective, and that controls required by Operational Instruction are implemented, maintained, and monitored.

Appendix H
Incident Response

1. 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 these mechanisms. 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.

2. Definition

An effective and efficient incident response and handling capability will enable CSOSA 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.

3. Scope

All business and mission critical systems must be supported by an incident response and handling capability that include adequate technology, effective process, and established and defined roles and responsibilities.

4. Purpose

This Incident Response Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the incident response security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including providing a means to ensure that incidents are handled expeditiously, and that the cause of the incident will be completely reported, investigated, and resolved to prevent potential protracted damage or recurrence.

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies an incident response capability that include process, people, and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance. A detailed Incident Response and Handling Plan that includes a documented communications flow will support this Operational Instruction.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that incident response technology and process is functional and effective and that controls and duties required by Operational Instruction are implemented, maintained, and monitored.

Appendix I
Maintenance Control

1. Background

Adequate maintenance planning and procedures help defend CSOSA business and mission critical systems against known and new security threats. Maintenance control includes monitoring the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of any system changes.

2. Definition

Maintenance control serves to ensure that all maintenance activity and connections supporting CSOSA business and mission critical systems are authorized, monitored, and recorded.

3. Scope

Support of all business and mission critical systems must include a maintenance control capability that includes adequate technology, process, and established and defined roles and responsibilities required for instituting, supporting, and maintaining adequate maintenance control.

4. Purpose

This Maintenance Control Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the maintenance control security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including ensuring that only authorized software is installed on systems; ensuring that changes to the system are tracked; and that only authorized personnel carry out required maintenance activity.

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies maintenance control capabilities that include process, people, and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that maintenance control technology and processes are functional and effective; and that controls required by Operational Instruction are implemented, maintained, and monitored.

Appendix J
Media Protection Control

1. Background

Media protection control is a set of production and input/output controls for the creation, handling, processing, storage, labeling and distribution of information that resides on fixed or removable electronic or hard copy media. These control measures are designed to protect sensitive information stored, handled, transported, or destroyed outside the inherent protective boundaries of the information system.

2. Definition

Media protection control employs processes mandated by formal institutionalized instructions and supported by adequate technology, to protect system data and sensitive information that resides outside of a system's physical and logical boundaries, on electronic or hard copy media. Media protection control also supports the inherent requirement of contingency planning to maintain current electronic copies of system data and documentation and to ensure protection of confidentiality, integrity, and availability of the information and system data.

3. Scope

All business and mission critical systems must have a supporting media protection control capability that includes adequate technology, effective process, and defined roles and responsibilities, required for securing these systems and information.

4. Purpose

This Media Protection Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the media protection security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including safeguarding sensitive information and ensuring that reliable system and data backup media are available to restore the system in the event of a disruption or disaster.

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies media protection capabilities that include process, people, and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that media protection control capabilities are in place. Media protection control required of system users will be detailed in each business and mission critical system's 'rules of behavior' and will support, and be consistent with other Federal and CSOSA policies governing privacy and confidentiality.

Appendix K
Physical and Environmental Protection

1. Background

Physical and environmental controls protect systems and information from both human and environmental threats. Physical and environmental protection controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

2. Definition

Physical and environmental controls are required to protect the facilities that house and support CSOSA's business and mission critical systems. These controls include process and technology, supported by policy and operational instruction, to control physical access and prevent and contain potential damage to information systems and information caused by environmental factors such as temperature, humidity, power outage, fire and other environmental concerns including natural or man-made disasters.

3. Scope

All mission critical systems must be supported by physical and environmental security control capabilities that include adequate technology, process, and defined roles and responsibilities, required for securing these systems and associated information.

4. Purpose

This Physical and Environmental Protection Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the physical and environmental protection security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including protecting business and mission critical systems from damaging physical and environmental threats.

5. Procedures

The CSOSA Office of Information Technology, with support from the CSOSA Office of Facilities, will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies physical and environmental control capabilities that include process, people, equipment and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office of Information Technology, in conjunction with the CSOSA Office of Facilities, will assign and train individuals with distinct duties and defined responsibilities to ensure that physical and environmental protection technology and process is functional and effective; and that required controls are implemented, maintained, and monitored.

Appendix L
Security Planning Control

1. **Background**
Security planning is a core component of an information security program and is integral to understanding the state and effectiveness of the security controls of an information system.

2. **Definition**
Security planning requires the development and maintenance of a system security plan for each of CSOSA's business and mission critical systems. The system security plan documents the control requirements of these systems and includes descriptions of the system's capacity to fulfill those requirements.

3. **Scope**
All business and mission critical systems must be supported with a system security plan that incorporates adequate technology, effective process, and defined roles and responsibilities to develop and maintain the plan and associated rules of behavior and privacy impact requirements.

4. **Purpose**
This Security Planning Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the security planning objectives of the Federal Information Security Management Act of 2002 (FISMA), including ensuring that all business and mission critical security controls and accompanying system rules of behavior and privacy requirements are well documented, and that and all employees are aware of their responsibility to use CSOSA's systems in accordance with the system rules of behavior.

5. **Procedures**
The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies security planning capabilities that include process, people, and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance.

6. **Roles and Responsibilities**
The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that the security planning and updating process is functional and effective; that all system users are

aware of their respective system rules of behavior and privacy responsibilities; and that controls required by Operational Instruction are implemented, maintained, and monitored.

Appendix M
Personnel Security

1. Background

An Introduction to Computer Security: The NIST Handbook, NIST SP 800-12, Chapter 10 Introduction states that:

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relate to how these individuals interact with computers and the access and authorities they need to do their job. No computer system can be secured without properly addressing these security issues.

In order to begin to address these security issues, information technology personnel security controls establish measures that must be taken to determine an individual's suitability for holding authorized access to an agency's information systems.

2. Definition

Information technology personnel security involves procedures that ensure that only vetted employees, contractors and interns who meet stringent background requirements are permitted employment at CSOSA and subsequent access to business and mission critical systems. In addition, information technology personnel security procedures ensure that the professional conduct of personnel meets agency requirements on an ongoing basis. These procedures include:

- Pre-employment background checks;
- Rules of behavior;
- Sanctions for non-compliance with policies and procedures; and
- Transfer and employment termination procedures.

3. Scope

All business and mission critical systems must have supporting information technology personnel security capabilities that include adequate technology, effective process, and defined roles and responsibilities required for securing these systems and associated information.

4. Purpose

This Information Technology Personnel Security Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the access control security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including ensuring that only appropriate personnel have access to the sensitive information contained in business and mission critical systems.

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies information technology personnel security capabilities that include process, people, and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that information technology personnel security capabilities are in place. Information technology personnel security activities will be coordinated with the Office of Human Resources & Strategic Planning, Analysis and Evaluation, and the CSOSA Office of Facilities.

Appendix N
System and Services Acquisition Control

1. Background

System and services acquisition control ensures that security is considered in the acquisition processes surrounding the systems development life cycle (SDLC) of an organization's systems and their constituent components. Security considerations are required to be considered at each phase of the SDLC but can be developed for a system at any phase along the continuum. Security measures can be more effective and cost-effective when incorporated at the beginning of the SDLC.

In planning for system and services acquisition the following must be considered:

- The sensitivity of a system and its data;
- Security requirements for the system (technical features, assurances, operational practices); and
- The capital and operational costs of adequately securing the system.

2. Definition

System and services acquisition control policy sets the stage for incorporating planning for information security throughout the SDLC. This policy ensures that security is an important consideration from requisition to disposal.

3. Scope

Procurements associated with all business and mission critical systems must have supporting system and services acquisition control capabilities that include adequate technology, effective process, and defined roles and responsibilities, required for securing these systems and associated information.

4. Purpose

This System and Services Acquisition Control Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the system and services acquisition security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including ensuring that security is an integral aspect of any software, hardware and services procurement for a business or mission critical system; that proper security design principles are used; that software usage, copyright, and documentation are maintained consistent with applicable laws and regulations; and that third party information service providers who support CSOSA business and mission critical systems employ adequate security controls.

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies a system and services acquisition control capability that identifies process, people, and technology to fulfill the requirements of this policy. The Operational Instruction will include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that system and services acquisition control capabilities are in place. System and services acquisition activities will be coordinated with the CSOSA Office of Finance and Administration.

Appendix O
System and Communications Protection

1. Background

System and communications protection primarily concerns the protection of information security as related to system states (up, down, startup through shutdown) and information flows while contained in an electronic medium. Secure system hardware and boundaries, as well as secure communications between separate components of a system, and/or between the system and external entities, constitute the goal of system and communications protection control.

2. Definition

System and communications control protects information systems and information from compromise by applying technology, technique, and process protection to those components of a system and its communications realm that facilitate information processing, flow, and security.

3. Scope

All mission critical systems must be supported by system and communications protection capabilities that include adequate technology, procedures, and defined roles and responsibilities, required for securing these systems and associated information.

4. Purpose

This System and Communications Protection Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the system and communications protection security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including application partitioning, security function isolation, use of valid Federally approved cryptographic operations/modules, and protection of internal and external communication between systems and external entities.

5. Procedures

The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies system and communications protection capabilities that include process, people, and technology to fulfill the requirements of this policy. The Operational Instruction will include a mechanism that requires accountability and compliance.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that system and communications protection technology and processes are functional and effective; and that required controls are implemented, maintained, and monitored.

Appendix P
System and Information Integrity Control

1. **Background**
System integrity control is used to protect data from unintentional or malicious alteration or destruction, and to provide assurance that the information and the security controls in place to protect information and information systems meet expectations for accuracy and reliability.

2. **Definition**
System integrity control employs technology and process to ensure that flaws and malicious code and/or intrusion activities that could compromise information or security control integrity are discovered and remediated or mitigated in a timely fashion through the use of tools and techniques that make use of sensory and alert mechanisms.

3. **Scope**
All mission critical systems must be supported by system and information integrity capabilities that include adequate technology, procedures, and defined roles and responsibilities required for securing these systems and associated information.

4. **Purpose**
This System and Information Integrity Policy Statement establishes management's commitment to require and ensure that CSOSA's business and mission critical systems accomplish the access control security-related objectives of the Federal Information Security Management Act of 2002 (FISMA), including ensuring that anti-virus software is tracked and updated frequently and that other tools and techniques are used to monitor events, detect attacks, and provide identification of unauthorized use of business and mission critical systems.

5. **Procedures**
The CSOSA Office of Information Technology will develop, disseminate, and periodically review (at least once a year) an Operational Instruction that specifically identifies system integrity control capabilities that include process, people, and technology to constitute secure information systems and fulfill the requirements of this policy, FISMA, and associated standards and guidance provided by the National Institute of Standards and Technology (NIST). The Operational Instruction will also include a mechanism that requires accountability and compliance.

   If the system integrity control capability is provided by a third party service provider, and/or common control area, a service level agreement and interconnection security agreement will be executed in accordance with CSOSA

Policy Statement 5504: Certification, Accreditation, Security and Risk Assessment Policy requirements for interconnected systems.

6. Roles and Responsibilities

The CSOSA Office of Information Technology will assign and train individuals with distinct duties and defined responsibilities to ensure that system and information integrity control technology and process is functional and effective; and that controls required by Operational Instruction are implemented, maintained, and monitored.