



## Table Of Contents

<b>Contracts and Business Case(s)</b> .....	<b>Tab One</b>
Business Case	
Request for Proposals	
Contracts	
Task Orders	
<b>Certification and Accreditation</b> .....	<b>Tab Two</b>
System Security Authorization Agreement	
Configuration Management	
Continuity of Operations Plan	
Disaster Recovery Plan	
Test Plan	
Test Results	
Certification Letter	
Interim Approval To Operate or Accreditation Letter	
<b>Security Plan</b> .....	<b>Tab Three</b>
Security Plan	
System Security Officer Designation Letter	
Service Level Agreements / Memoranda of Understanding	
Rules of Behavior	
<b>Assessments and Audits</b> .....	<b>Tab Four</b>
Inventory Forms	
Risk Assessments	
Corrective Action Plan	
Cost Benefit Analysis	
National Institute of Standards and Technology Self-Assessment	
Inspector General Audits	
Government Accounting Office Audits	
<b>Training</b> .....	<b>Tab Five</b>
Training Schedule	
<b>Clearance and Access Forms</b> .....	<b>Tab Six</b>
Federal Student Aid Employees	
Federal Student Aid Contractors	



## Contracts and Business Cases

This section includes the following:

**Business Cases (BC)** - An FSA business case is used to describe a proposed project to the FSA IRB. The proposal should include estimated budget requirements, FSA system impacts, and security implications, among other areas.

**Request for Proposal's (RFPs)** - An RFP solicits submissions of proposals from contractors that indicate the specifications, both technical and general, for work that the government needs to be out-sourced.

**Contracts** - A formalized agreement between FSA and a contractor to perform work that was advertised in an RFP for a stated period of performance.

**Task Orders (T.O.)** - Individual task orders may be issued as part of a larger contract award.



## Certification and Accreditation (C&A)

This section includes the following:

**System Security Authorization Agreement (SSAA)** - A formal agreement among the Designated Approving Authority (DAA), the Certification Authority, the IT system user representative, and the program manager. It is used throughout the C&A process to guide actions, document decisions, specify security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security. The SSAA should contain the following documents:

**Configuration Management (CM)** - Documented process describing controls of changes made to hardware, software, firmware, documentation, testing, test fixtures, and test documentation throughout the life cycle of an IT system. A CM should include such features as a listing of the members of the CM board, description of the impact analysis process, details of security approval for the change, etc.

**Continuity Of Operations Plan (COOP)** - The COOP focuses on restoring an organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. Standard elements of a COOP include Delegation of Authority statements, Orders of Succession, and Vital Records and Databases. Minor disruptions that do not require relocation to an alternate site are typically not addressed.

**Disaster Recovery Plan (DRP)** - A DRP describes the recovery of critical applications in the event of a major hardware or software failure or destruction of facilities. It applies to major, usually catastrophic, events that deny access to the normal facility for an extended period of time. The DRP scope may overlap that of an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation.

**Test Plan** - The test plan identifies the system to be reviewed and gives a timetable and standards that the system will be tested against.

**Test Results** - The findings from the testing conducted on a system.

**Certification Letter** - A letter establishing the completion of a comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards. The letter, from the Certifier (usually an independent contractor) to the Designated Accrediting Authority (DAA, usually the System Owner) establishes the



## System Security Officer Notebook

### Certification and Accreditation

extent that the system's design and implementation met federal and departmental security requirements.

**Accreditation Letter or Interim Approval To Operate (IATO)** - A letter by the DAA (usually the System Owner) formally declaring that the system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. An IATO is approval for short-term operation of a system within the bounds of acceptable risk, but not a full accreditation. An IATO may be issued with the understanding that deficiencies will be corrected in a time period specified by the DAA.



## Security Plan

This section includes the following:

**Security Plan** - Formal document fully describing the planned security procedures planned or implemented required to meet system security requirements. While every security plan must describe the system's Disaster Recovery Plan, Continuity of Operations Plan, Configuration Management plan, etc., it may not include the actual documents in its appendices. Several of these documents should be included with the System Security Authorization Agreement (SSAA) in the Certification and Accreditation (C&A) section of this notebook.

**System Security Officer Designation Letter** - A letter stating the responsibility of the System Security Officer (SSO) for the security of the system or systems. The letter should be signed by both the SSO and the System Manager.

**Service Level Agreements (SLAs) / Memoranda Of Understanding (MOU)** - A service-level agreement (SLA) is an informal contract between a company and a customer that defines the terms of the company's responsibility to the customer and the type and extent of remuneration if those responsibilities are not met. Memoranda of Understanding are documents that outline specific areas of mutual interest between a company and a partner. Memoranda of Understanding may not commit either company to perform work or to assign, license, or protect ownership of intellectual property. The benefit of an MOU is the foundation of general guidance for pursuing shared interests. The terms of an MOU are agreed upon by all partners and signed.

**Rules Of Behavior (RoB)** - The RoB delineates the responsibilities and expected behavior of all individuals with access to a system. The rules should state the consequences of inconsistent behavior or noncompliance. Included topics are: limits to interconnections, work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges. RoB may be enforced through administrative sanctions specifically related to the system or through more general sanctions. Users should review and sign acknowledgment of the RoB before being authorized access to the system.



## Assessments and Audits

This section includes the following:

**Inventory Forms** – Annual inputs to the Department which define the system as either a General Support System or Major Application, provide an overall description of the system, and describe the Sensitivity (in terms of Confidentiality, Integrity, and Availability) and the Criticality of the system, as per definitions provided by the Department.

**Risk Assessments (RA)** - A risk assessment is the documented analysis of the threats and vulnerabilities of a system, the potential impact that the resulting loss of information or capabilities would have on the organization, and the relative level of risk posed by each threat/vulnerability. The resulting analysis is used as a basis for identifying appropriate and effective countermeasures.

**Corrective Action Plan (CAP)** - The corrective action plan is prepared after a risk assessment or self-assessment. It is composed of the actions and associated timetables required to improve the findings described in the assessments. The CAP should respond to all findings of the assessment; if a risk-based decision is not made to correct a finding, a description of that risk-based decision should be included.

**Cost Benefit Analysis (CBA)** - Cost benefit analysis determines an estimate of all costs, including overhead, installation and operating costs, for options which would correct each finding discovered during an assessment or audit, listing all anticipated benefits resulting from those corrections, and providing recommendations as to which options should be pursued. Options also should include the possibility of leaving the security flaw unchanged, and describing the projected costs and/or consequences.

**National Institute of Standards and Technology (NIST) Self-Assessment** - The NIST Self-Assessment is a questionnaire for agency officials to determine the current status/effectiveness of their security programs and give insight into areas needing improvement. Topics are divided into three main categories: Management Controls, covering risk management, security controls and plan, and life cycle management; Operational Controls, including personnel, physical and environmental security, hardware and software related security issues, and emergency planning matters; and Technical Controls, including authentication, access controls and audit trails.

**Inspector General (IG) Audits** – Independent audits of a system's security programs conducted by the Inspector General of the organization.



## System Security Officer Notebook

### Assessments and Audits

**General Accounting Office (GAO) Audits** – The GAO audits organization’s system security with guidelines found in the Federal Information System Control Audit Manual (FISCAM).



# Training

This section includes the following:

**Training Schedule** - Security/IT courses scheduled within the next year. Governmental training requirements for all employees include annual, security awareness training, and additional security training commensurate to the sensitivity of their job. Track all security-related training here for easy reference. This should include both formal and informal training, seminars, on-line training, etc.



## Clearance and Access Forms

This section includes the following:

**Federal Student Aid (FSA) Employees** - Forms filled out by FSA employees that deal with their clearances and the accesses they have to a system or group of systems.

**Federal Student Aid (FSA) Contractors** - Forms filled out by FSA contractors that deal with their clearances and the accesses they have to a system or group of systems.