



ADMINISTRATIVE COMMUNICATIONS SYSTEM

UNITED STATES DEPARTMENT OF EDUCATION

Office of Management, Executive Office

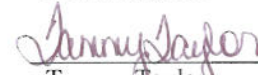
400 Maryland Avenue; Washington, DC 20202

Transmittal Sheet #: 2006-0002 *Date:* March 31, 2006

Distribution: All ED employees

Distribution Approved:

Directives Management Officer:


Tammy Taylor

Action: Pen and Ink Changes

Document Changing: Handbook OCIO-05, *Handbook for Information Technology Security Certification and Accreditation Procedures*, dated 03/06/2006

Pen and Ink Changes: The following pen and ink changes have been made.

<i>Page</i>	<i>Section</i>	<i>Changed</i>	<i>To</i>
All	Dates	03/06/2006	03/31/2006
1	Superseding Information	Information described above	Information described above
D1-D3	Appendix D	Updated links to references in Appendix D.	



ADMINISTRATIVE
COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

Handbook

Handbook OCIO-05

Page 1 of 40 (03/31/2006)

Distribution:

All Department of Education Employees

Approved by: /s/ (03/06/2006)

Michell C. Clark

Acting Assistant Secretary for Management

Handbook for Information Technology Security Certification and Accreditation Procedures

For technical questions concerning information found in this ACS document, please contact Kathy Zheng on (202) 245-6447 or via [e-mail](#).

Supersedes OCIO-05, Handbook for Information Technology Security Certification and Accreditation Procedures dated 03/06/2006.

**U.S. DEPARTMENT OF EDUCATION
INFORMATION TECHNOLOGY SECURITY**



**Handbook for
Information Technology Security
Certification and Accreditation Procedures**

Version 2.0

March 31, 2006

TABLE OF CONTENTS

1.	INTRODUCTION.....	1
1.1	<i>Purpose.....</i>	1
1.2	<i>Background.....</i>	1
1.3	<i>Scope.....</i>	1
1.4	<i>Document Structure.....</i>	2
1.5	<i>Exceptions.....</i>	2
2.	CERTIFICATION & ACCREDITATION OVERVIEW	3
2.1	<i>What is Certification and Accreditation (C&A)?.....</i>	3
2.2	<i>Why is C&A Important?.....</i>	3
2.3	<i>How Does C&A Map to the Lifecycle Management?.....</i>	3
2.4	<i>Who is Involved in the C&A Process?.....</i>	4
2.5	<i>What are the Types of Certification Recommendations?.....</i>	5
2.6	<i>What are the Types of Accreditation Decisions?.....</i>	6
2.7	<i>How is C&A Level of Effort Determined?.....</i>	6
2.7.1	<i>Step 1: Determine Mission Criticality.....</i>	7
2.7.2	<i>Step 2: Determine Information Sensitivity.....</i>	7
2.7.3	<i>Step 3: Determine Level of C&A Effort.....</i>	8
3.	CERTIFICATION & ACCREDITATION PROCESS	10
3.1	<i>Initiation Phase.....</i>	11
3.1.1	<i>Task 1: Establish the C&A Boundary.....</i>	11
3.1.2	<i>Task 2: Determine System Categorization.....</i>	11
3.1.3	<i>Task 3: Develop System Security Documentation.....</i>	12
3.1.4	<i>Task 4: Verify System Security Documentation.....</i>	13
3.2	<i>Certification Phase.....</i>	14
3.2.1	<i>Task 1: Review and Update System Security Documentation.....</i>	14
3.2.2	<i>Task 2: Develop and Finalize Methods and Techniques.....</i>	14
3.2.3	<i>Task 3: Perform Security Control Assessment.....</i>	14
3.2.4	<i>Task 4: Assemble Certification Documentation.....</i>	15
3.2.5	<i>Task 5: Determine Certification Recommendation.....</i>	15
3.3	<i>Accreditation Phase.....</i>	16
3.3.1	<i>Task 1: Assemble Accreditation Documentation.....</i>	16
3.3.2	<i>Task 2: Determine Accreditation Decision.....</i>	16
3.4	<i>Continuous Monitoring Phase.....</i>	17
3.4.1	<i>Task 1: Configuration Management and Change Control.....</i>	17
3.4.2	<i>Task 2: On-Going Security Control Monitoring.....</i>	17
3.4.3	<i>Task 3: Status Reporting and Documentation.....</i>	18
3.4.4	<i>Task 4: Re-certification and Re-accreditation.....</i>	18
4.	SUMMARY	19
APPENDIX A. INTERIM AUTHORIZATION TO OPERATE (IATO).....		A-1
APPENDIX B. GLOSSARY OF TERMS		B-1

APPENDIX C. ACRONYMS C-1

APPENDIX D. REFERENCES D-1

APPENDIX E. DETERMINE CERTIFICATION TIER EXAMPLE E-1

APPENDIX F. ACCREDITATION RECOMMENDATION MEMO F-1

APPENDIX G. ACCREDITATION DECISION LETTER G-1

1. INTRODUCTION

1.1 Purpose

This *Handbook for Information Technology Security Certification and Accreditation Procedures* document is intended to provide a comprehensive and uniform approach to the certification and accreditation (C&A) process. This document is developed in accordance with the Department's Handbook for Information Assurance Security Policy, Office of Management and Budget (OMB) Circular A-130, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 and 800-53 and the Federal Information Security Management Act (FISMA).

1.2 Background

Title III of the E-Government Act (Public Law 107-347), entitled FISMA, requires that all Federal agencies develop, document, and implement a comprehensive information security program to safeguard information and information systems of the respective agency. OMB Circular A-130, Appendix III, also mandates that security must be developed at both the programmatic and system levels. As stated in OMB Circular A-130, at a minimum, agency information security programs shall include the following controls in their general support systems and major applications:

a. Controls for general support systems...

"Authorize Processing¹. Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years..."

b. Controls for major applications...

"Authorize Processing. Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application."

1.3 Scope

This Handbook is for the use of all personnel including contractors who are responsible for or involved in preparing the C&A of the Department's general support systems and major applications. This document is intended to assist the C&A team² members in determining and applying the applicable security standards to their systems and applications.

¹ 'Authorize Processing' synonymous with the term accreditation.

² The C&A team comprises of at least a system manager, system security officer, computer security officer, and user representative. Other Department personnel or contractors may be assigned as part of the team to assist in performing the C&A activities. See Section 2.4 for an overview of the roles and responsibilities of the C&A key participants.

1.4 Document Structure

The remainder of this document is organized as follows:

- **Section 2** describes the fundamentals of C&A to include types of accreditation decisions and necessary documentation and supporting materials.
- **Section 3** provides an overview of the four interrelated phases of the C&A process and includes appropriate references to supporting policies, standards and guidelines:
 - Initiation
 - Certification
 - Accreditation
 - Continuous Monitoring
- **Section 4** provides a summary.

This Handbook contains nine appendices that provide useful references including a C&A checklist and memo templates.

1.5 Exceptions

If compliance with any process in this document is not feasible, technically possible, or the cost of the control does not provide a commensurate level of protection, an exemption from that requirement may be provided. Exceptions shall be a decision made between the system security officer/system manager and the Designated Approving Authority (DAA), in coordination with the Department's Chief Information Security Officer. Written authorization from the Department's Chief Information Security Officer or the DAA is required to allow such an exemption.

2. CERTIFICATION & ACCREDITATION OVERVIEW

2.1 *What is Certification and Accreditation (C&A)?*

Certification is a comprehensive assessment of the management, operational, and technical security controls in a general support system (GSS) or major application (MA) 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. Certification directly supports accreditation by providing authorizing officials with important information necessary to make credible, risk-based decisions on whether to place GSSs/MAs into operation or continue their current operation.

Accreditation is the authorization and approval granted to a GSS/MA to process in an operational environment. The decision is made on the basis of a certification by designated technical personnel, normally the Designated Accreditation Authority (DAA), that the system meets pre-specified management, operational, and technical requirements for achieving adequate security³.

2.2 *Why is C&A Important?*

The C&A process ensures that there are adequate security measures in place to protect the information that resides on the Department's GSSs and MAs. This process is applicable to all Department GSSs/MAs under development and those already in production. In addition, Federal laws and regulations require agencies to perform C&A activities at least every three (3) years or whenever a significant change in the system affects its security. **The Department has determined that mission critical systems should be recertified and reaccredited on an annual basis.** To meet the C&A requirements mandated in Federal laws, the Department has outlined C&A requirements in the *Handbook for Information Assurance Security Policy*.

The C&A process achieves the following:

- Validates security requirements established for a GSS/MA;
- Examines implemented safeguards to determine if they satisfy the Department's security requirements and identifies any inadequacies; and
- Obtains management approval to authorize initial or continued operation of the GSS/MA.

2.3 *How Does C&A Map to the Lifecycle Management?*

The C&A process is a set of methodical processes and activities that must correlate with the development of the system. Table 2.1 shows how C&A activities fit into the lifecycle management (LCM). In accordance with the NIST SP 800-37, new information systems or major upgrades to information systems should begin C&A activities early in the LCM to shape and influence the security capabilities of the system. However, these activities may be performed later in the LCM for operational systems and legacy systems. In either situation, all of the activities should be completed to ensure that:

³ OMB A-130 defines "adequate security" as security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.

- The system has received the necessary attention with regard to security; and
- The DAA explicitly accepts the risk based on the implementation of an agreed-upon set of security controls.

Table 2.1: C&A Activities in the LCM

LCM	Definition	Construction & Validation	Implementation	Support & Improvement	Retirement
C&A Activities	Security Categorization	Self Assessment Risk Assessment	Independent Validation & Verification (IV&V)	Configuration Management and Control	
	Preliminary Risk Assessment	Security Planning Developmental Security Test & Evaluation	Security Test & Evaluation (ST&E) Certification & Accreditation		
C&A Phase	Initiation		Certification & Accreditation	Continuous Monitoring	

2.4 Who is Involved in the C&A Process?

Table 2.2 describes the roles and responsibilities of the C&A key participants involved in the C&A process. Other Department personnel or contractors may be assigned as part of the team to assist in performing the C&A activities.

Table 2.2: C&A Roles and Responsibilities

Roles	Responsibilities
<i>Certifier</i>	<p>The Certifier provides a comprehensive evaluation of the GSS/MA, including technical and non-technical controls, to determine if the GSS/MA is configured with the proper IT security controls. The Certifier provides the DAA with an accreditation recommendation based on the GSS/MA security documentation and the certification recommendation provided by the CRG.</p> <p>The Department’s Chief Information Officer (CIO) is designated as the Certifier, who assumes the role of an independent technical liaison for all stakeholders involved in the C&A process and is an objective third party, independent of the GSS/MA developers.</p> <p>Note: The CIO is not the Certifier for the Office of the Chief Information Officer’s (OCIO) systems. An independent party must be assigned as the Certifier for the OCIO GSSs and MAs.</p>
<i>Certification Review Group</i>	<p>The Certification Review Group (CRG), on behalf of the Certifier, performs independent technical certification activities on all Department systems identified as requiring certification. The CRG is responsible for reviewing and ensuring each GSS/MA’s security documentation is complete and complies with the Department, OMB, and NIST guidance. The CRG is also responsible for conducting ST&E testing as well as automated vulnerability scans and penetration tests. Finally, the CRG provides a certification recommendation and a complete package of associated GSS/MA security documentation to the Certifier.</p>

Roles	Responsibilities
<i>Designated Approving Authority</i>	The DAA (also referred to as the accreditor by the Department) is the authorizing official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations and assets. The DAA determines accreditation based on the certification decision and accreditation recommendation from the Certifier.
<i>Independent Verification and Validation Management Committee</i>	Independent Verification and Validation (IV&V) Management Committee is directly responsible for the capture and review of Corrective Action Plans (CAPs), acceptance and remediation, and the prioritization of the CAP implementation activity and associated schedule.
<i>System Manager</i>	The System Manager (SM) is responsible for ensuring that the GSS/MA is deployed and operated according to the agreed-upon security requirements.
<i>Computer Security Officer</i>	The Computer Security Officer (CSO) manages the efforts of the C&A activities and acts as the managing official for information security of GSSs or MAs within the PO.
<i>System Security Officer</i>	The System Security Officer (SSO) is responsible for ensuring that appropriate operational security posture is maintained for a GSS/MA within the PO. The SSO plays an active role in developing and updating the system security documentation as well as coordinating with the CSO any changes to the system and assessing the security impact of those changes.
<i>User Representative</i>	An individual that represents the operational interests of the user community and serve as liaisons for that community throughout the life cycle of the information system. The user representative assists in the C&A process, when needed, to ensure mission requirements are satisfied while meeting the security requirements and employing the security controls defined in the system security plan.
<i>Department's Chief Information Security Officer/Director of Information Assurance Services (IAS)</i>	The Department's Chief Information Security Officer is the Senior Agency Information Security Officer and the Director of Information Assurance Services (IAS), who is responsible for carrying out the Department's CIO responsibilities under FISMA and ensuring agency compliance with FISMA. The Department's Chief Information Security Officer/Director of IAS will oversee the Department C&A process and maintain the Department's repository for all official documentation required for C&A.

2.5 What are the Types of Certification Recommendations?

After the system security documentation review and testing activities have been completed, the CRG provides the certification findings and recommendation to the Certifier. The Certifier will present the certification recommendation to the DAA based on the certification assessment results and recommendation provided by the CRG. The Certifier can provide one of following certification recommendations.

- **Recommend Accreditation.** If the Certifier finds that the security posture of the system is commensurate with the security requirements, the Certifier will recommend full accreditation to the DAA. In the accreditation recommendation memo (see [Appendix F](#)), the Certifier may also include measures to further enhance security of the system.
- **Recommend Interim Authorization to Operate (IATO).** If the Certifier finds that the security posture of the system is not commensurate with the security requirements, but operation of the system is essential to fulfill the mission of the Department, the Certifier may recommend IATO. The Certifier may recommend IATO with the understanding that the system will operate in a limited capacity to mitigate risk, and that an acceptable level

of security will be achieved within a period of time specified by the DAA. The duration established for an IATO should be no longer than six (6) months.

- **Recommend Denial of Authorization to Operate.** If the Certifier finds that the security posture of the system is not adequate and the operation of the system is not in the best interest of the Department, the Certifier may recommend denial of authorization to operate .

2.6 What are the Types of Accreditation Decisions?

Accreditation decisions resulting from C&A processes should be conveyed to the system manager/SSO. There are three (3) types of accreditation decisions that can be rendered by the DAA. See [Appendix G](#) for samples of accreditation decision letters.

- **Authorization to Operate.** If the DAA deems that the risk is acceptable, an authorization to operate is issued for the system. The system is authorized without any significant restrictions or limitations on its operation. This authorization or accreditation must occur at least every three (3) years, or whenever significant changes are made to the system.⁴
- **Interim Authorization to Operate (IATO).** If the DAA deems that the risk is unacceptable, but operation of the system is essential to fulfill the mission of the Department, an IATO may be granted. The IATO is a limited authorization under specific terms and conditions including corrective actions to be taken and a required timeframe for completion of those actions. The duration established for an IATO should be no longer than six (6) months. See [Appendix A](#) for the requirements for granting an IATO.
- **Denial of Authorization to Operate.** If the DAA deems that risk is unacceptable, it usually indicates that there are major deficiencies in the security controls in the system, the authorization to operate the system is denied. The DAA should work with the responsible individuals to revise the plan of action and milestones (POA&M) to ensure that proactive measures are taken to correct the security deficiencies in the system.

2.7 How is C&A Level of Effort Determined?

The Department has identified a tiered approach to C&A. This approach ensures that the proper level of effort is used to certify and accredit each GSS and MA. As described in the Department's *Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures*, only GSSs and MAs are required to be certified and accredited. To determine if an application qualifies as a MA, the mission criticality and information sensitivity is determined. Based on the results of the determined mission criticality and information sensitivity, the application may then be designed as a MA, if applicable. Information systems are categorized into one of four certification tier levels (Tier 0 -- Tier 3).

⁴ Examples of significant changes to an information system that should be reviewed for possible re-accreditation include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a re-accreditation action.

The level of documentation and testing required for the C&A process depends on the certification tier level determined for each GSS or application. Mission criticality and information sensitivity are two attributes used to determine the certification tier. Although C&A is only required for GSSs and MAs, all applications are considered part of the tier process as the mission criticality and information sensitivity criteria must be determined. The following sections provide descriptions on determining the certification tier for a GSS/MA.

2.7.1 Step 1: Determine Mission Criticality

Mission criticality is determined based on how integral the GSS or application is in carrying out the critical missions of the Department. Each GSS and application is evaluated using the current Department criteria, *Mission Critical (MC)*, *Mission Important (MI)*, and *Mission Supportive (MS)*. A numerical value is assigned to each criticality criteria as follows: MC = 3, MI = 2, and MS = 1. This value will be used to calculate the tier score. As part of the Department's GSS and MA inventory, the SSO/system manager will document the mission criticality of each GSS and application in the GSS and MA Inventory Submission Form. A sample of the inventory form (the Data Sensitivity Worksheet) is provided in appendix A of the *Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures*. In addition, the SSO/system manager will also complete the Department's Critical Infrastructure Protection (CIP) Survey to validate mission criticality. A GSS/MA that is determined to be a Mission-Essential Infrastructure (MEI) Asset through the Critical Infrastructure Protection Survey is automatically considered a Tier 3 system. For detailed information on mission criticality, see the Department's *Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures*.

- **Mission Critical (MC):** Automated information resources whose failure would preclude the Department from accomplishing its core business operations.
- **Mission Important (MI):** Automated information resources whose failure would not preclude the Department from accomplishing core business processes in the short term, but would cause failure in the mid- to long-term (three days to one month).
- **Mission Supportive (MS):** Automated information resources whose failure would not preclude the Department from accomplishing core business operations in the short- to long-term (more than one month), but would have an impact on the effectiveness or efficiency of day-to-day operations.

Source: Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures.

Figure 2.1 Mission Criticality Criteria

2.7.2 Step 2: Determine Information Sensitivity

Information sensitivity of each GSS and application takes into account the *confidentiality*, *integrity*, and *availability*. Figure 2.2 provides a description of each information sensitivity criteria. As a part of the Department's GSS and MA inventory, information sensitivity of each GSS and application is determined. The SSO/system manager documents the information sensitivity of each GSS and application in the GSS and MA Inventory Submission Form. The information sensitivity for each GSS and application must be classified to determine the proper level and type of controls for the system and thus, will help determine the level of effort for certifying and

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and propriety information.
 - **Integrity:** Guarding against improper information modification or destruction, and including ensuring information non-repudiation and authenticity.
 - **Availability:** Ensuring timely and reliable access to and use of information.
- Source: NIST SP 800-37*

Figure 2.2 Information Sensitivity Criteria

accrediting the system.

Each information sensitivity criteria is rated on a scale of High, Medium, or Low and are assigned a numerical value as follows: High = 3, Medium = 2, and Low = 1. This value will be used to calculate the tier score.

To determine the numerical value for information sensitivity, insert the numerical values determined for *confidentiality*, *integrity*, and *availability* into the following formula:

$$\textit{Confidentiality} + \textit{Integrity} + \textit{Availability} = \textit{Information Sensitivity}$$

To calculate the tier score, the numerical scores from Steps 1 and 2 must be inserted into the formula provided below:

$$\begin{array}{c} \textit{Mission Criticality} \\ \textit{(Step 1 Results)} \end{array} + \begin{array}{c} \textit{Information Sensitivity} \\ \textit{(Step 2 Results)} \end{array} = \textit{Tier Score}$$

See [Appendix E](#) for an example on how to determine the certification tier.

2.7.3 Step 3: Determine Level of C&A Effort

As described in the Department's Information Technology Security General Support Systems and Major Applications Inventory Procedures, all GSSs require C&A as they provide the first, basic level of security for all the applications and MAs they host. All MAs⁵ require C&A due to their increased data sensitivity risks and mission criticality, and they require additional security controls beyond those provided by the GSS in which they operate. Applications⁶, due to their low data sensitivity risks and low mission criticality, receive all the appropriate security from the GSS in which they operate. Thus, applications are not required to undergo the C&A process.

The certification tier is determined by identifying the tier score listed in the certification tier scale shown in Table 2.3. The level of effort required for certifying and accrediting the GSS/MA is provided in the appropriate column of the certification tier. Applications that are calculated to have a tier score of 4 or certification tier 0 are not considered MAs and therefore, do not require C&A. However, all GSSs are required to be certified and accredited, and GSSs that are calculated to have a tier score of 4 (certification tier 0) will utilize the C&A effort associated with a certification tier 1 GSS.

⁵ Major application identified as mission critical, mission important, or mission supportive and an information sensitivity category rated as 'Moderate' or 'High'.

⁶ Application identified as mission supportive and all information sensitivity categories rated as 'Low'.

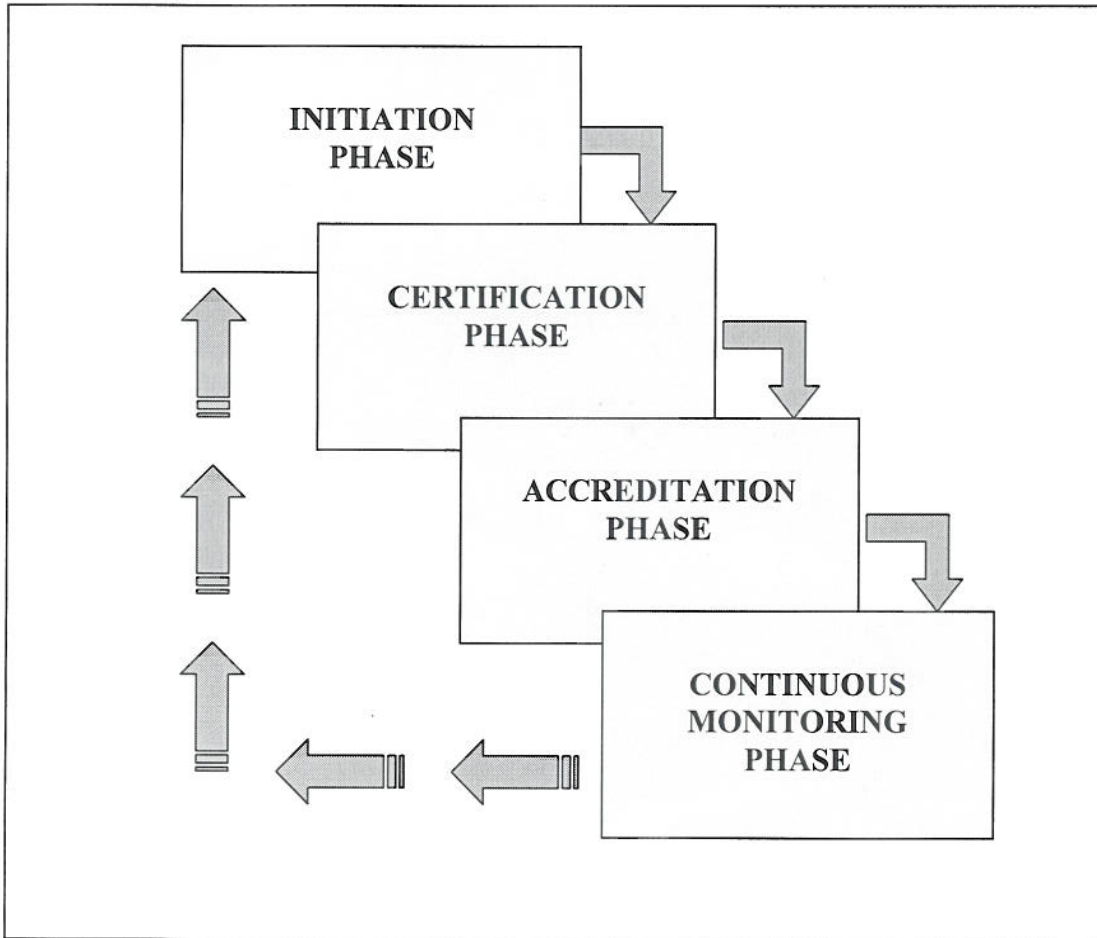
Table 2.3 Certification Tier Scale

Impact Value		Low	Moderate	High
Tier Score	4	5 – 8	9 – 10	11 – 12
C&A Level of Effort Activities	No C&A Required, tier score 4 applications are covered by the GSS/MA in which they operate.	Self Assessment Risk Assessment (Using BLSRs + additional system specific security requirements) System Security Plan* Configuration Management Plan Contingency Plan(Continuity of Support) Security Test & Evaluation (Minimal testing + specific detailed testing, when necessary) Plan of Action & Milestones**	Self Assessment Risk Assessment (Using BLSRs + additional system specific security requirements + vulnerability scanning) System Security Plan* Configuration Management Plan Contingency Plan (Continuity of Support + Disaster Recovery Plan) Security Test & Evaluation (Detailed testing + penetration testing, when necessary) Plan of Action & Milestones**	Self Assessment Risk Assessment (Using BLSRs + additional system specific security requirements + vulnerability scanning) System Security Plan* Configuration Management Plan Contingency Plan(Continuity of Support + Disaster Recovery Plan) Security Test & Evaluation (Detailed testing + penetration testing) Plan of Action & Milestones**
<p>* A system security plan can contain as supporting appendices or as references, other key security-related documents for the system (e.g. a risk assessment, configuration management plan, and contingency plan).</p> <p>Note: Under reasonable and appropriate circumstances, previous assessment results and audits may be incorporated into the certification process.</p>				

3. CERTIFICATION & ACCREDITATION PROCESS

The C&A process consists of four interrelated phases: (1) Initiation, (2) Certification, (3) Accreditation, and (4) Continuous Monitoring. Each phase consists of a set of tasks that are to be carried out by responsible individuals (see Section 2.4). The level of effort applied to the information system undergoing C&A should be commensurate with the FIPS 199 security category of the system and level of risk. Figure 3.1 provides a high-level view of the C&A process.

Figure 3.1: Certification and Accreditation Process



Source: NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004.

3.1 *Initiation Phase*

The purpose of the Initiation Phase is to ensure that the system personnel (e.g., system security officer, system manager, computer security officer) and OCIO/IAS are in agreement with the contents of the system security documentation before the CRG, on behalf of the Certifier, begins the assessment of security controls in the information system.

3.1.1 **Task 1: Establish the C&A Boundary**

The first task in the Initiation Phase is to prepare a description of the C&A boundary (system boundary, facilities, equipment, etc.) and the external interfaces with other equipment or systems. The C&A boundary for the system that is to be accredited needs to be established before the conduct of risk assessment and development of system security plan. The boundary encompasses all those components of the system and excludes separately accredited systems, to which the system is connected. The accreditation boundary should include all facility equipment that is to be addressed in the C&A. The DAA and the Department's Chief Information Security Officer should consult with the prospective SSO and/or system manager when establishing system and security accreditation boundaries.

For large and complex systems, the DAA and the Department's Chief Information Security Officer may define subsystem components with established subsystem boundaries. The decomposition into subsystem components should be reflected in the system security plan for that large and complex system.

3.1.2 **Task 2: Determine System Categorization**

The security category of an information system influences the selection of security controls from NIST SP 800-53. The SSO/system manager should determine the security category of the system in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199 defines security categories for information systems based on potential impact that the loss of confidentiality, integrity, or availability would have on the Department operations or assets. FIPS 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing Federal information and information systems for each of three stated security objectives (confidentiality, integrity, and availability). The Department evaluated the requirements in FIPS 199 and customized the requirements to the Department's environment. The result of an information system (GSS and application) categorization assessment must be documented in the Department's GSS and MA Inventory Submission Form (also called the Data Sensitivity Worksheet). In addition, all GSSs and applications must complete the CIP Survey to determine mission criticality. The resultant data will be considered as the official Department list of mission critical, mission important, and mission supportive GSSs and applications. The Department's *Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures* and FIPS 199 should be considered during the system categorization to help guide the SSO/system manager's selection of controls for the system.

3.1.3 Task 3: Develop System Security Documentation

Once the security category has been determined, the SSOs/system managers must complete the following system security documents in a manner consistent with NIST SP 800-53:

- Risk Assessment
- System Security Plan
- Contingency Plan or Disaster Recovery Plan
- Configuration Management Plan
- Security Testing and Evaluation Procedures

Note: A system security plan can include as supporting appendices or as references, other important security-related documents for the system (e.g., risk assessments, contingency plans, configuration management plans, security configuration checklists).⁷

3.1.3.1 Subtask 3.1: Perform Risk Assessment

A risk assessment (RA) is performed by an independent third party to analyze and interpret risk associated with potential threats and vulnerabilities of a GSS/MA. This analysis is then used as a basis for identifying appropriate and cost-effective remediation measures. All high and medium risks must be mitigated in order for a GSS/MA to be certified. GSSs and MAs are inherently vulnerable to many types of threats. When a threat⁸ is paired with vulnerability, some level of risk is present. It is important to identify the vulnerabilities, what threats are present to exploit the vulnerabilities, the level of risk incurred, and how to reduce that risk to an acceptable level so that it can be controlled. The RA results yield an overall level of risk for the GSS/MA. The result of the risk assessment process is the identification and documentation of the residual risk that the authorizing official (the DAA in the Department) is being asked to accept to authorize the system to process information to satisfy its mission. See the NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, and the Department's *Handbook for Information Technology Security Risk Assessment Procedures* for more detail.

3.1.3.2 Subtask 3.2: Develop System Security Plan

The system security plan (SSP) is developed by providing an overview of the GSS's/MA's security requirements. It describes the controls that are in place or planned for meeting those requirements. The SSP also specifies responsibilities of all individuals who operate or access the GSS/MA. The plan can also contain as supporting appendices or as references, other key security-related documents for the system such as the risk assessment, contingency plan, incident response plan, configuration management plan, security configuration checklists, and any system interconnection agreements. The SSP is a living document—it will be updated throughout the LCM. OMB Circular A-130 requires an individual SSP for all GSSs and MAs. The Department's SSPs must conform to the security controls defined in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* and the standards outlined in NIST SP 800-18, *Procedures for Developing Security Plans for Information Technology Systems*, which provides guidance on how to develop the SSP.

⁷ NIST SP 800-37

⁸ Any circumstance, event, or act that could cause harm to the Department by destroying, disclosing, modifying, or denying service to automated information resources.

3.1.3.3 Subtask 3.3: Develop Contingency Plan or Disaster Recovery Plan

The Contingency Plan (CP) is developed for identifying procedures to enable continuity of business functions in the event of natural or man-made disasters or catastrophes affecting the availability of the GSS/MA. This plan, which always includes a Continuity of Support (COS) and includes a DRP for Certification Tier 2 and 3 systems, **must be tested annually** to ensure the continued effectiveness and adequacy of the plan. For further guidance on developing a CP, refer to the Department's *Handbook for Information Technology Security Contingency Planning Procedures* guide and NIST SP 800-34, *Contingency Planning Procedures for Information Technology Systems*.

3.1.3.4 Subtask 3.4: Develop Configuration Management Plan

The Configuration Management Plan (CMP) is prepared to include procedures on how the GSS/MA changes are managed, with a systematic methodology for applying technical and administrative direction and surveillance throughout its life cycle. The CMP provides assurance that the GSS/MA in operation is the correct version (configuration). If any changes are made, they will be reviewed for security implications before implementing the change. The CMP may be used to ensure that changes take place in an identifiable and controlled environment and do not impact the GSSs or MA's properties negatively, including its security. For further guidance on developing a CMP, refer to the Department's *Handbook for Information Assurance Configuration Management Planning Guide*.

3.1.3.5 Subtask 3.5: Develop Security Test and Evaluation Procedures

Security Test and Evaluation (ST&E) procedures are developed for examining and analyzing the safeguards required to protect a GSS/MA—as they have been applied in an operational environment—to determine the security posture of that GSS/MA. The objective of the ST&E is to assess the technical implementation of the security design and to ascertain that security software, hardware, and firmware features affecting confidentiality, integrity, availability, and accountability have been implemented. ST&E assists in validating the correct implementation of identification and authentication, audit capabilities, access controls, object reuse, trusted recovery, and network connection rule compliance. These procedures will be used by the CRG in Phase 2, Certification, to conduct the ST&E. For further guidance on developing ST&E procedures refer to the Department's *Information Technology Security Testing and Evaluation Guide*.

3.1.4 Task 4: Verify System Security Documentation

The Department's Information Assurance Services (IAS) will serve as a checkpoint to confirm that all system security documentation for the GSS/MA has been completed by the SSO/system manager. IAS will review all required system security documentation (RA, SSP, CP, CMP, and ST&E) developed for the GSS/MA and will determine if the system is ready to be evaluated and tested in Phase 2, Certification. All activities within Phase 1, Initiation, must be completed prior to proceeding with the certification and accreditation phases.

3.2 *Certification Phase*

The purpose of the Certification Phase is to determine the extent to which the security controls for the systems are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The independent third party, CRG, will perform certification activities on behalf of the Certifier.

3.2.1 **Task 1: Review and Update System Security Documentation**

Once the system security documentation has been completed, the IAS will forward them to the CRG for documentation review. The CRG will review all required system security documentation (RA, SSP, CP, CMP, and ST&E) developed for the GSS/MA and determine if they are complete and consistent with the requirements document for the system. If the system security documentation is deemed unacceptable, the system personnel should review the changes recommended by the CRG and update the documentation as needed based on the results of this review. If the system security documentation is deemed acceptable by the CRG, the DAA and the Department's Chief Information Security Officer will accept the security controls document for the system.

3.2.2 **Task 2: Develop and Finalize Methods and Techniques**

The CRG will finalize the ST&E Plan, which will include all testing and evaluation procedures and techniques necessary to evaluate the management, operational, and technical security controls implemented to protect the GSS/MA. Test and evaluation procedures and techniques should be selected according to the management, operational, and technical controls implemented for the GSS/MA and all other standards documented within the Department's *Handbook for Information Assurance Security Policy*; and the system certification Tier level. Only those test procedures and techniques relevant to the system security controls, platform, and configuration should be selected or developed. The scope of ST&E test procedures should be commensurate with the system certification Tier level, in order to use available resources efficiently.

In addition, the CRG will develop the Penetration Test Rules of Engagement that will govern the testing and evaluation activities. Refer to Table 2.3 for determining the system certification tier. The SSO/system manager, the Department's Chief Information Security Officer, and the CRG must agree to the test and evaluation procedures and techniques before proceeding with the next task.

3.2.3 **Task 3: Perform Security Control Assessment**

The security control assessment task is to prepare, conduct, and document the assessment of the security controls in the GSS/MA. The CRG will assess the management, operational, and technical security controls implemented in the system using the testing and evaluation techniques and procedures developed in the ST&E plan. The CRG will also be responsible for conducting ST&E on all Tier 2 and 3 systems, as well as automated vulnerability scans and penetration tests for Tier 3 systems. The CRG will perform penetration tests on Tier 2 systems only if needed. Under appropriate circumstances, the ST&E could be integrated with the risk assessment to avoid duplication of effort. However, all GSSs and MAs are required to perform a security self-

assessment in a manner consistent with NIST SP 800-26. The results of the security assessment, including recommendations for correcting any deficiencies in the security controls, are documented in the preliminary security assessment report.

3.2.4 Task 4: Assemble Certification Documentation

The preliminary security assessment report from the CRG provides the results of the assessment of the security controls in the system and recommendations for correcting deficiencies in the security controls. The SSO/system manager should prepare a POA&Ms and risk analysis forms (RAFs) to correct deficiencies in the security controls for the system. Any finding that is determined to be an acceptable vulnerability, security exposure, or a validated false positive must be fully identified in the RAF and submitted to the Department's Security Office IV&V Management Committee for concurrence. Supporting evidence and adequate justification must always accompany the RAF. All high and moderate risks must be mitigated for the GSS/MA to be certified. The IV&V Management Committee will independently evaluate the corrective actions implemented by SSO/system manager to findings identified for the GSS/MA. The IV&V committee will determine if mitigations are adequate to resolve findings for the system. The CRG will assess any changes made to the security controls in response to corrective actions by the SSO/system manager and develop the final security assessment report, as appropriate. The final security assessment report will be part of the final accreditation package along with all relevant system security documents and supporting materials. The CRG will deliver the C&A related briefings and provide the Certifier with a certification recommendation. Upon successful completion of this phase, the DAA will be able to render an appropriate accreditation decision for the system. The contents of the final accreditation package including the final security assessment report, updated POA&M, and updated system security documentation and supporting materials, should be protected appropriately in accordance with the Department's *Handbook for Information Assurance Security Policy*.

3.2.5 Task 5: Determine Certification Recommendation

After certification assessment, the CRG will provide certification findings and a recommendation to the Certifier. The Certifier will review the certification findings and recommendation and determine the accreditation recommendation based on the acceptable level of residual risk that was determined in the Certification phase. If the residual risk is within the acceptable level, the Certifier may recommend full accreditation. If the Certifier determines that security deficiencies exist, but believes that the short-term operation is within the required acceptable level, the Certifier may recommend IATO. However, if the residual risk is not within the acceptable level, the Certifier may recommend denial of authorization to operate the system and notify the DAA, CRG, and C&A team that the GSS/MA must return to Phase 1, Initiation. When the GSS/MA returns to Phase 1, security controls must be re-evaluated and improved to mitigate risk and minimize residual risk.

After the certification recommendation has been determined, the Certifier prepares the appropriate certification recommendation memo and submits the memo, with the system security documentation, to the DAA. See [Appendix F](#) for samples of accreditation recommendation memo.

3.3 Accreditation Phase

The objective of the Accreditation Phase is to determine if the remaining known vulnerabilities in the GSS/MA (after the implementation of an agreed-upon set of security controls) pose an acceptable level of risk to the Department's operations and assets. Upon successful completion of this phase, the SSO/system manager will have:

- Authorization to operate the system;
- Interim authorization to operate the system; or
- Denial of authorization to operate the system.

3.3.1 Task 1: Assemble Accreditation Documentation

The objective of the accreditation documentation task is to transmit the final accreditation package to the appropriate individuals, and update the system security documentation with the latest information from the accreditation decision. The final accreditation package contains the final security assessment report, accreditation recommendation memo, the final security assessment report, updated POA&M, and all updated system security documentation and supporting materials. The final accreditation package documents the results of the certification assessment and provides the DAA with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the system.

3.3.2 Task 2: Determine Accreditation Decision

The DAA reviews the accreditation recommendation memo along with the system security documentation to determine the accreditation decision based on the business impact of the residual risk and whether the DAA is prepared to accept financial and legal responsibility⁹ for the system. Following a review of the submitted system security documentation and the Certifier's recommendation, the DAA will make one of the following decisions:

- Grant Full Accreditation
- Grant Interim Authorization to Operate
- Deny Accreditation.

If the DAA determines that the system meets all security requirements and accepts financial and legal responsibility for the system, he/she may grant full accreditation. Before the DAA makes a final accreditation decision, he/she must be willing to accept financial and legal responsibility for all residual risk associated with the system. He/She must acknowledge possible legal ramifications (e.g., fines and imprisonment¹⁰) if the system does not meet minimum-security requirements mandated by Federal laws and regulations.

If the DAA determines that the system has deficiencies, but operation of the system is essential to fulfill the mission of the Department, the DAA may grant IATO. If a non-essential system has deficiencies, and imposing restrictions on operations may mitigate the deficiencies, the DAA

⁹ OMB Circular A-123 (Management Accountability and Control) and the Federal Managers' Financial Integrity Act (FMFIA) of 1982 require that the DAA accept financial and legal responsibility for the GSS/MA.

¹⁰ Reference the Computer Fraud and Abuse Act for detailed information on fraud and legal activities associated with the handling of computers and sensitive information.

may grant IATO. If the system is granted IATO, the DAA, Certifier, CRG, and C&A team must develop a POA&M for bringing the system to an acceptable level of security. A maximum length of time for the IATO should be no longer than six (6) months.

If the DAA finds that the security posture of the system is not adequate, and operation of the system is not in the best interest of the Department, the DAA may deny accreditation. When this occurs, the DAA must notify the Certifier, CRG, and the C&A team that the system must return to Phase 1, Initiation. At this point, the C&A team, CRG, Certifier, and the DAA must discuss solutions on how to bring the system to an acceptable level of security. The C&A team and the Certifier must agree before moving to the next step.

After determining the appropriate accreditation decision, the DAA prepares the appropriate accreditation decision memo and submits the memo with the system security documentation and certification recommendation memo to the CIO. See [Appendix G](#) for samples of accreditation decision letters.

3.4 Continuous Monitoring Phase

The objective of the Continuous Monitoring Phase is to provide oversight and monitoring of the security controls in the GSS/MA on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. The activities in this phase are performed continuously throughout the life cycle of the GSS/MA.

3.4.1 Task 1: Configuration Management and Change Control

A system will typically be in a constant state of migration with upgrades to hardware or software and possible modifications to the system environment. Changes to a system can have a significant impact on the security of the system. Documenting system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.

The system personnel shall document and record any relevant information about proposed or actual changes to the system hardware or software, in accordance with the *Handbook for Information Technology Security Configuration Management Planning Procedures*. The system personnel shall also document any changes to the operating environment, including modifications to the physical environment. Prior to making any significant changes to the information system, the SSO/system manager should assess the security impact of such changes. If the results of the security impact analysis indicate that the proposed or actual changes to the GSS/MA will affect or have affected the security of the system, corrective actions should be initiated and the POA&Ms revised.

3.4.2 Task 2: On-Going Security Control Monitoring

On-going security control monitoring enables the system personnel to monitor and identify potential security problems in the system that are not identified during the security impact assessment conducted as part of the configuration management and change controls processes. The continuous monitoring of security controls can be accomplished by performing independent or internal security reviews, self-assessments, ST&E, penetration testing, or audits. The

frequency and intensity with which such evaluations are to be performed should be commensurate with the potential harm to the Department's operations and assets that might result from compromise of the system. For high Tier systems, the selected set of security controls should be evaluated more frequently and more intensive procedures and techniques should be employed. Security controls implemented to protect low Tier systems may be reviewed less often and in a less intensive manner.

3.4.3 Task 3: Status Reporting and Documentation

The objectives of this task are to update the system security documentation to reflect the most recent proposed or actual system changes and the potential security impact associated with each change, and to report the changes and associated security impact to the OCIO/IA.

The SSO/system manager should update the system security documentation to ensure that the documents contain the most current security-related information. The SSO/system manager should prepare and submit status reports to the Department's Chief Information Security Officer, and DAA on a regular basis. The status reports should serve as a basis for the Chief Information Security Officer and DAA to monitor the security status of the system; the progress made to reduce or eliminate vulnerabilities; and to determine when re-accreditation is necessary.

3.4.4 Task 4: Re-certification and Re-accreditation

Re-certification/re-accreditation is necessary to ensure that the Department's information systems continue to operate at an acceptable risk level. The objective of the re-certification/re-accreditation task is to ensure that C&A is not a one-time process, and is managed throughout the life of each GSS/MA.

The Department's Information Security Officer and the DAA should determine when re-accreditation is necessary for a particular system. As required by OMB Circular A-130, all GSSs and MAs must be reaccredited at least once every three (3) years or when significant changes to the system affect system security. **The Department has determined that mission-critical systems should be recertified and reaccredited on an annual basis.**

The re-certification/re-accreditation process should begin at the Initiation Phase. Depending upon the magnitude of changes to the GSS/MS since the previous certification evaluation, the availability of evaluation results and reports, and the system risk level, the resources required for re-accreditation may be substantially less than those required for the original C&A process.

4. SUMMARY

C&A includes technical and non-technical assessments that establish the extent to which the GSS or MA meets a set of specified security requirements for its task and operational environment. The outcome of this process—the accreditation—assures the DAA that the level of security used will protect information and/or processing capabilities.

The C&A process is comprised of four phases: (1) Initiation, (2) Certification, (3) Accreditation, and (4) Continuous Monitoring. Each phase of the process has specific activities that must be completed before the next phase begins. Principal Offices are encouraged to use the process outlined in this document to ensure there is a consistent, seamless C&A program implemented across the Department.

APPENDIX A. INTERIM AUTHORIZATION TO OPERATE (IATO)

Under certain conditions, the Department may issue an Interim Authorization to Operate (IATO). An IATO acknowledges that an information system has significant security deficiencies (as identified by a Department-approved security assessment), but operation of the system or continue its operation is essential to fulfill the mission of the Department, even in light of these security deficiencies.

Note: An IATO is not a replacement for a full accreditation, nor is an IATO to be used to delay corrective action. It is a Federal requirement that all required information systems go through the full certification and accreditation process, and an IATO may only be issued as part of the full certification and accreditation process.

When Should an IATO Be Issued?

Following are some situations in which an IATO may be issued:

- Mission critical systems in the development phase may be issued an IATO before they move into production, and before all required security-control assessments have been completed. For example, completing vulnerability scanning/penetration testing in the development environment may be an inefficient use of the Departmental resources. In such cases, issuing an IATO during the system's development phase—before scans have been completed—may be acceptable, provided the conditions below have been met.
- If, after assessing the results of the security certification, the DAA deems that the level risk is unacceptable, but there is an important mission-related need to place an information system into operation, or continue its operation, even in light of significant security deficiencies, an IATO may be issued.

Requirements for Granting an IATO

An IATO may be issued only after the following requirements have been met:

- There is an overarching mission necessity to place the information system into operation or continue its operation, even in light of the identified security deficiencies.
- A Department-approved security assessment has been performed on the information system, and the results of this assessment have been presented to (and are clearly understood by) relevant system personnel (e.g., system managers, system owners, system security officers), the CRG, Certifier and the DAA. The type of assessment that must be performed depends on the system's criticality.
- A system security plan (and any other required system security documentation) has been reviewed and accepted by the Department's Chief Information Security Officer, the Certifier, and the DAA to ensure that all NIST SP 800-53 recommended security controls are addressed.
- There is a formal plan of action in place to address all findings, with clear milestones, responsibilities, and deadlines. Actions must be taken expeditiously to mitigate those higher levels of risk, moving towards full accreditation and lower levels of risk

- A schedule describing the advancement to the final accreditation has been established. A calendar date (e.g., “by September 2005”) may be used if this is applicable, but frequently the schedule will be event-driven (e.g., completion of software tests or operational security analysis). The schedule must be mutually satisfactory to the system owner and the designated approving authority.
- The IATO has a very specific expiration date.
- The designated approving authority has signed off on the IATO.

Eligible Systems

All systems (both major applications and general support systems) are eligible for an IATO, and granted they meet the conditions stated above.

Operational Restrictions

The system’s normal operational procedures might have to be altered or limited (depending on the identified security deficiencies) until full accreditation is achieved. The IATO is a temporary approval that should be no longer than six months. The limited authorization will remain in effect during that time period as long as: (i) the required security status reports for the system are submitted to this office every three months; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) continued progress is being made in reducing or eliminating vulnerabilities in the information system in accordance with the plan of action and milestones. At the end of the period of limited authorization, the information system must be either authorized to operate or the authorization for further operation will be denied.

Expiration Period

An IATO should be no longer than six (6) months—that is, all security deficiencies ranked as “high” or “moderate” must be fully remediated within six (6) months of the issuance of the IATO. Within six (6) months from the issuance of the original IATO (assuming all “moderate” and “high” findings have been closed), the information system must go through the full certification and accreditation process, including any required assessments for full certification (e.g., vulnerability scan, penetration testing) that were not performed during the IATO process.

Under the most extenuating of circumstances, an IATO may be renewed or extended for an additional six-month period. However, the following conditions must be met before an extension is granted:

- The justification for extending an IATO must be presented both in person and in writing to Department’s Chief Information Security Officer, the Certifier and the DAA. The DAA will make the final decision to either extend the IATO or decommission the application until it is fully certified and accredited.

APPENDIX B. GLOSSARY OF TERMS

Accreditation: The official management decision given by the DAA/Accreditor to authorize operation of a GSS/MA and to explicitly accept the risk to agency operations and assets, based on the implementation of an agreed-upon set of security controls.

Accreditor: See Designated Approving Authority

Availability: Ensuring timely and reliable access to and use of information and information systems.

Baseline Security Requirements (BSRs): A set of security requirements the Department views as the minimal security standards to be upheld by all GSSs and MAs.

Boundary: All components of an information system to be accredited and excluding separately accredited systems, to which the information system is connected.

Certification: The comprehensive assessment of the management, operational, and technical security controls in a GSS/MA, made in support of accreditation, 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.

Certification Review Group (CRG): The CRG, on behalf of the Certifier, performs independent technical certification activities on all Department systems identified as requiring certification. The CRG is responsible for reviewing and ensuring each system security documentation is complete and complies with the Department, OMB, and NIST guidance. The CRG is also responsible for conducting ST&E testing as well as automated vulnerability scans and penetration tests. Finally, the CRG provides a certification recommendation and a complete package of associated system security documentation to the Certifier.

Certification Tier: A GSS or MA may be given a certification tier of 1, 2, or 3. This number (certification tier) represents the level of effort required for certifying and accrediting the GSS/MA

Certifier: Assumes the role of an independent technical liaison for all stakeholders involved in the C&A process and is an objective third party, independent of the GSS/MA developers. The Certifier provides a comprehensive evaluation of the GSS/MA, including technical and non-technical controls, to determine if the GSS/MA is configured with the proper security controls in place. The Certifier provides the DAA/Accreditor with a certification decision and an accreditation recommendation based on the GSS/MA security documentation and the certification recommendation provided by the CRG.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Management Plan (CMP): A plan that describes the management controls involved in all changes and updates made to a system that affects security. The plan includes all

documentation supporting these changes and updates. This plan is maintained throughout the C&A process and updated according to LCM activities.

Contingency Plan (CP): Preventive measures established to assist an organization in their ability to quickly and cost effectively recover critical IT resources.

Continuity of Support (COS): Preventative measures for protecting the IT systems as well as procedures for restoring any system disruption

Designated Approving Authority (DAA): The DAA (or the Accreditor as referred to by the Department) is the authorizing official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations and assets.

Disaster Recovery Plan (DRP): A plan that identifies recovery procedures in the event of natural or man-made disasters or catastrophes affecting the availability of the GSS/MA. This plan is tested annually to ensure the continued effectiveness and adequacy of the plan.

General Support System (GSS): An interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network, including smart terminals that support a branch office; an agency-wide backbone; a communications network; a departmental data processing center, including its operating system and utilities; a tactical radio network; or a shared information processing service organization. See the Department's *Information Technology Security General Support Systems and Major Applications Inventory Procedures* for more details.

Independent Verification and Validation (IV&V): Responsible for the capture and review of CAPs, acceptance and remediation, and the prioritization of the CAP implementation activity and associated schedule.

Information Sensitivity: The formal process of identifying each GSS/MA in terms of its confidentiality, integrity, and availability.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Interim Authorization To Operate (IATO): Provides a limited authorization to operate the system under specific terms and conditions and acknowledges greater risk to the agency for a specified period of time.

Lifecycle Management (LCM): The coordination of activities associated with the implementation of information systems from conception through disposal, which include defining requirements, designing, building, testing, implementing, and disposing of systems.

Major Application (MA): An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. *Note:* All Federal applications require some level of protections, however certain applications—because of the information in them—require

special management oversight and must be treated as major. Adequate security for other applications must be provided by security of the GSS in which they operate. See the Department's *Information Technology Security General Support Systems and Major Applications Inventory Procedures* for additional details.

Mission Critical (MC): Automated information resources whose failure would preclude the Department from accomplishing its core business operations

Mission Criticality: The formal process of identifying each GSS/MA as Mission Critical, Mission Important, or Mission Supportive.

Mission Important (MI): Automated information resources whose failure would not preclude the Department from accomplishing core business processes in the short-term, but would cause failure in the mid-to long-term (3 days to 1 month)

Mission Supportive (MS): Automated information resources whose failure would not preclude the Department from accomplishing core business operations in the short-to long-term (more than 1 month), but would have an impact on the effectiveness or efficiency of day-to-day operations.

Plan of Action and Milestones (POA&M): A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Residual Risk: The portion of risk that remains after security measures have been applied.

Risk Assessment (RA): The process of identifying risks to agency operations, agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

Security Test and Evaluation (ST&E): An evaluation of all hardware, software, and physical security features that are part of a system. This process involves testing these features to determine what threats and vulnerabilities exist for the system. The findings are documented, and recommendations are made that may be included in the RA.

Significant change: Examples of significant changes to an information system that should be reviewed for possible reaccreditation include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.

System Security Plan (SSP): Formal document that provides an overview of the security requirements for the GSS/MA and describes the security controls in place or planned for meeting those requirements. The plan includes system identification, management controls, operational controls, and technical controls. The system security plan outlines responsibilities for all system users and describes the rules of behavior for those users.

APPENDIX C. ACRONYMS

BLSR	Baseline Security Requirements
CAP	Corrective Action Plan
C&A	Certification and Accreditation
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CMP	Configuration Management Plan
COS	Continuity of Support
CP	Contingency Plan
CRG	Certification Review Group
CSO	Computer Security Officer
DAA	Designated Approving Authority
Department	U.S. Department of Education
DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSS	General Support System
IA	Information Assurance
IAS	Information Assurance Services
IATO	Interim Authorization To Operate
IT	Information Technology
IV&V	Independent Verification and Validation
LCM	Lifecycle Management
MA	Major Application
MC	Mission Critical
MEI	Mission-Essential Infrastructure
MI	Mission Important
MS	Mission Supportive
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PO	Principal Office
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SM	System Manager
SP	Special Publication
SSO	System Security Officer
SSP	System Security Plan
ST&E	Security Test and Evaluation

APPENDIX D. REFERENCES

Computer Fraud and Abuse Act

As amended 1994 and 1996, U.S.C. Section 1001 and 1030 Amended Title 18 Crimes and Criminal Procedure.

CMP Procedures

Department's Handbook for Information Technology Security Configuration Management Planning Procedures
(http://wdcrobiis08/doc_img/acs_hb_ocio_11.doc)

GSSs & MAs Inventory Procedures

Department's Handbook for General Support Systems and Major Applications Inventory Procedures (http://wdcrobiis08/doc_img/acs_hb_ocio_9.doc)

IA Security Policy

Department's Handbook for Information Assurance Security Policy
(http://wdcrobiis08/doc_img/acs_hb_ocio_1.doc)

IAPMP

Information Assurance Program Management Plan (IAPMP)

RA Procedures

Department's Handbook for Information Technology Security Risk Assessment Procedures
(http://wdcrobiis08/doc_img/acs_hb_ocio_7.doc)

ST&E Procedures

Department's Information Technology Security Test and Evaluation Guide,
(http://wdcrobiis08/doc_img/ED_STE_Guide_v5.doc)

FFMIA

Federal Managers' Financial Integrity Act (FMFIA) of 1982, P. L. 97-255, September 8, 1982

FISMA

E-Government Act of 2002, Federal Information Security Management Act of 2002

NIST FIPS 199

Standards for Security Categorization of Federal Information and Information Systems, February 2004
(<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>)

FIPS Pub 200

Minimum Security Requirements for Federal Information and Information Systems, March 2006
(<http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>)

**NIST SP 800-18
Revision 1**

Guide for Developing Security Plans for Federal Information Systems
February 2006
(<http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>)

NIST SP 800-26

Security Self-Assessment Guide for Information Technology Systems,
November 2001

- [\(<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>\)](http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf)
- Draft**
NIST SP 800-26
Revision 1 Guide for Information Security Program Assessments and System Reporting Form, August 2005
[\(<http://csrc.nist.gov/publications/drafts/Draft-sp800-26Rev1.pdf>\)](http://csrc.nist.gov/publications/drafts/Draft-sp800-26Rev1.pdf)
- NIST SP 800-30** Risk Management Guide for Information Technology Systems, January 2002
[\(<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>\)](http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)
- NIST SP 800-34** Contingency Planning Procedures for Information Technology Systems June 2002
[\(<http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>\)](http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf)
- NIST SP 800-37** Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004
[\(<http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>\)](http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf)
- NIST SP 800-47** Security Guide for Interconnecting Information Technology Systems August 2002
[\(<http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf>\)](http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf)
- NIST SP 800-50** Building an Information Technology Security Awareness and Training Program, October 2003
[\(<http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>\)](http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf)
- NIST SP 800-53** Recommended Security Controls for Federal Information Systems, February 2005
[\(<http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf>\)](http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf)
- Draft**
NIST SP 800-53A Guide for Assessing the Security Controls in Federal Information Systems, July 15, 2005
[\(<http://csrc.nist.gov/publications/drafts/sp800-53A-ipd.pdf>\)](http://csrc.nist.gov/publications/drafts/sp800-53A-ipd.pdf)
- NIST SP 800-59** Guideline for Identifying an Information System as a National Security System, August 2003
[\(<http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf>\)](http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf)
- NIST SP 800-64** Security Considerations in the Information System Development Life Cycle, October 2003
<http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>
- OMB A-123** Office of Management and Budget (OMB) Management of Federal Information Resources Circular A-123 (Management Accountability and Control), June 21, 1995
[\(<http://www.whitehouse.gov/omb/circulars/a123/a123.html>\)](http://www.whitehouse.gov/omb/circulars/a123/a123.html)
- OMB A-130** Office of Management and Budget (OMB) Management of Federal Information Resources Circular A-130, Appendix III, November 28, 2000

[\(<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>\)](http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)

PDD-63 Presidential Decision Directive (PDD), Critical Infrastructure Protection, May 22, 1998

Privacy Act (<http://www.usdoj.gov/04foia/privstat.htm>)

APPENDIX E. DETERMINE CERTIFICATION TIER EXAMPLE

Given the following information obtained from the GSS and MA Inventory Submission Form completed for the Sample Education System (SES), the certification tier can be determined using the three-step process described in Section 2.7:

GSS/MA Name:		SES
Mission Criticality:		Mission Critical
Information Sensitivity:	Confidentiality	High
	Integrity	High
	Availability	High

Step 1. Mission Criticality

According to the information provided above, mission criticality of SES is Mission Critical (MC). As established in Section 2.7.1, the numerical value for a MC system is **3**.

Step 2. Information Sensitivity

According to the information provided above, each information sensitivity criteria for SES is rated High. As established in Section 2.7.2, the numerical value for information sensitivity criteria rated High is 3.

To determine the numerical value for information sensitivity, the numerical values determined for *Confidentiality*, *Integrity*, and *Availability* must be calculated using the following formula:

$$\begin{array}{ccccccc}
 \textit{Confidentiality} & + & \textit{Integrity} & + & \textit{Availability} & = & \textit{Information Sensitivity} \\
 \boxed{3} & + & \boxed{3} & + & \boxed{3} & = & \boxed{9}
 \end{array}$$

Based on the formula, the numerical value for information sensitivity is **9**.

Step 3. Tier Score

To determine the tier score, the numerical values from Steps 2 and 3 must be calculated using the formula provided below:

$$\begin{array}{ccccccc}
 \textit{Mission Criticality} & + & \textit{Information Sensitivity} & = & \textit{Tier Score} \\
 \boxed{3} & + & \boxed{9} & = & \boxed{12}
 \end{array}$$

The tier score is **12**.

Step 4: Determine Certification Tier

The tier score, as calculated in Step 3, equals 12. Therefore, based on the certification tier scale provided below, SES is a certification Tier 3 GSS. Hence, the level of effort required for certifying and accrediting SES is provided in the certification Tier 3 column.

Certification Tier Scale

Certification Tier	0	1	2	3
Tier Score	4	5 – 8	9 – 10	11 – 12
C&A Level of Effort Activities	No C&A Required, Tier 0 applications are covered by the GSS/MA in which they operate.	Self Assessment Risk Assessment (Using BLSRs + additional system specific security requirements) System Security Plan* Configuration Management Plan Contingency Plan (Continuity of Support) Security Test & Evaluation (Minimal testing + specific detailed testing, when necessary) Plan of Action & Milestones	Self Assessment Risk Assessment (Using BLSRs + additional system specific security requirements + vulnerability scanning) System Security Plan* Configuration Management Plan Contingency Plan(Continuity of Support + Disaster Recovery Plan) Security Test & Evaluation (Detailed testing + penetration testing, when necessary) Plan of Action & Milestones	Self Assessment Risk Assessment (Using BLSRs + additional system specific security requirements + vulnerability scanning) System Security Plan* Configuration Management Plan Contingency Plan (Continuity of Support + Disaster Recovery Plan) Security Test & Evaluation (Detailed testing + penetration testing) Plan of Action & Milestones
<p><i>* A system security plan can contain as supporting appendices or as references, other key security-related documents for the system (e.g. a risk assessment, configuration management plan, and contingency plan).</i></p> <p>Note: Under reasonable and appropriate circumstances, previous assessment results and audits may be incorporated into the certification process.</p>				

APPENDIX F. ACCREDITATION RECOMMENDATION MEMO

Recommend Full Accreditation

To: [DAA NAME]
Principal Officer for [PO NAME]

From: [CERTIFIER NAME]
Assistant Secretary for Management and Chief Information Officer

Subject: Certification Assessment and Accreditation Recommendation for [GSS/MA NAME]

Certification of [PO NAME] [GSS/MA NAME] has been performed in accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; and the Department Certification and Accreditation program. The documented security requirements of the [GSS/MA] have been carefully reviewed and were found to properly reflect the controls required to protect the [GSS/MA] and its information against unauthorized disclosure, alteration, or destruction.

I have reviewed the security measures that have been implemented and planned, and have weighted the remaining residual risks contained in the system against the operational requirements. The remaining residual risks are documented in the attached list of low risks with planned future remediation.

In accordance with the provisions of the Certification and Accreditation program, the [PO NAME] [GSS/MA NAME] **is certified for operation**. I certify that the [GSS/MA] has implemented a level of security commensurate with its criticality. Operation of [PO NAME] [GSS/MA NAME] is in the best interest of the Department of Education and will enable the Department to perform its mission.

I recommend full accreditation of [PO NAME] [GSS/MA NAME] based on your evaluation of the attached certification package.

[Certifier Name]

Date

ATTACHMENT

Recommend Interim Authorization to Operate (IATO)

To: [DAA NAME]
Principal Officer for [PO NAME]

From: [CERTIFIER NAME]
Chief Information Officer

Subject: Certification Assessment and Accreditation Recommendation for [GSS/MA
NAME]

A certification assessment of [PO NAME] [GSS/MA NAME] has been performed in accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; and the Department Certification and Accreditation program. I have reviewed the security measures that have been implemented and planned, and have weighted the remaining residual risks contained in the system against the operational requirement. The remaining residual risks are documented in the list of accepted low risks, as well as the list of low risks with planned future remediations.

In accordance with the provisions of the Certification and Accreditation program, the [GSS/MA NAME] is certified for operation for a period of six months. Analysis of the [PO NAME] [GSS/MA NAME] revealed that it does not meet all of the security requirements and that additional remediation measures are needed to ensure a satisfactory level of security is present.

I recommend an Interim Authorization To Operate (IATO) for [PO NAME] [GSS/MA NAME] based on your evaluation of the security assessment report and supporting documentation. The corrective actions that must be completed to mitigate the risks are described in the security assessment report.

Certifier Signature

Date

Recommend Denial of Authorization to Operate

To: [DAA NAME]
Principal Officer for [PO NAME]

From: [CERTIFIER NAME]
Chief Information Officer

Subject: Certification Assessment and Accreditation Recommendation for [GSS/MA NAME]

Certification of [PO NAME] [GSS/MA NAME] has been performed in accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; and the Department Certification and Accreditation program. The documented security requirements of the [GSS/MA] have been carefully reviewed and were found to properly reflect the controls required to protect the [GSS/MA NAME] and its information against unauthorized disclosure, alteration, or destruction.

I have reviewed the attached system security documentation and recommend *denial of authorization to operate* [PO NAME] [GSS/MA NAME]. This recommendation is based on a review of the [GSS/MA] that indicated a level of security commensurate with its criticality has not been achieved. Operation of [PO NAME] [GSS/MA NAME] is not in the best interest of the Department of Education because an appropriate level of protection does not exist.

Certifier Signature

Date

APPENDIX G. ACCREDITATION DECISION LETTER

Authorization to Operate

To: Chief Information Officer

From: [DAA NAME]
Principal Officer for [PO NAME]

Subject: Accreditation Decision for [GSS/MA NAME]

Certification of [PO NAME] [GSS/MA NAME] has been performed in accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; and the Department Certification and Accreditation (C&A) program. The documented system requirements of [GSS/MA NAME] have been carefully reviewed and were found to properly reflect the controls required to protect [GSS/MA NAME] and its information against unauthorized disclosure, alteration, or destruction. I have reviewed the security measures that have been implemented and planned, and have weighted the remaining residual risks contained in the system against the operational requirement. The remaining residual risks are documented in the attached list of accepted low risks, as well as the attached list of low risks with planned future remediation.

In accordance with the provisions of the Certification and Accreditation program, [PO NAME] [GSS/MA NAME] is **authorized for operation**. This authorization is my formal declaration that appropriate security remediation measures have been properly implemented and that a satisfactory level of security is present.

This authorization is contingent on continued application of the security measures in place, and is valid for a period of three (3) years from the date of this memo, unless a significant change to [PO NAME] [GSS/MA NAME] requires earlier re-certification and re-accreditation. It is the responsibility of the System Manager of the [GSS/MA] to ensure that any change in configuration mode of operation or other modification is analyzed to determine its impact on security, and that appropriate action is taken to maintain a level of security consistent with the requirements for this action.

[DAA name]

Date

Designated Approving Authority

ATTACHMENT

Grant Interim Authorization to Operate (IATO)

To: Chief Information Officer

From: [DAA NAME]
Principal Officer for [PO NAME]

Subject: Accreditation Decision for [GSS/MA NAME]

I have reviewed the results of the security certification for the [PO NAME] [GSS/MA NAME] and the supporting evidence provided in the associated security accreditation package. I have weighed the residual risks and operational requirements and have determined that the risk resulting from the operation of the [GSS/MA] is *not fully* acceptable. However, I have also determined that there is an overarching need to place the [GSS/MA NAME] into operation due to mission necessity. Accordingly, I am issuing an *Interim Authorization to Operate* the [GSS/MA NAME] in its existing operating environment. The [GSS/MA NAME] is *not* considered accredited during the period of limited authorization to operate.

The Certification and Accreditation (C&A) Team will monitor the implementation of the additional security features and notify the Designated Approving Authority (DAA) if deviations from the schedule occur. The corrective actions that must be completed to mitigate the risks are described in the security assessment report. When all additional security measures are implemented and working as proposed, I will fully authorize this [GSS/MA NAME] and remove the operating restrictions.

This interim authorization to operate the [GSS/MA] is valid for six months. The interim authorization will remain in effect during that time period as long as: (i) the required security status reports for the system are submitted to this office every three months until all open actions are completed; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) continued progress is being made in reducing or eliminating vulnerabilities in the information system in accordance with the plan of action and milestones. At the end of the period of limited authorization, the information system must be either authorized to operate or the authorization for further operation will be denied. Renewals or extensions to this IATO will be granted only under the most extenuating of circumstances.

DAA Signature

Date

Deny Accreditation

To: Chief Information Officer

From: [DAA NAME]
Principal Officer for [PO NAME]

Subject: Accreditation Decision for [GSS/MA NAME]

Certification of [PO NAME] [GSS/MA NAME] has been performed in accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; and the Department Certification and Accreditation (C&A) Program. I have examined the accreditation package and certification decision.

After reviewing the security measures that have been implemented and planned, and weighing the remaining residual risks against the operational requirement, I am issuing a *denial of authorization to operate* [PO NAME] [GSS/MA NAME]. My formal declaration is that the [GSS/MA] level of security is not commensurate with its criticality. Operation of [PO NAME] [GSS/MA NAME] is not in the best interest of the Department of Education because an appropriate level of protection does not exist.

Attached is a list of proposed solutions and remediation measures that would provide the level of security required for accreditation.

DAA Signature

Date