Distribution:
All Department of Education Employees

Approved by: /s/
William J. Leidinger
Assistant Secretary for Management

Handbook for Information Technology Security **Risk Assessment Procedures**

Supersedes Handbook OCIO-07 "Handbook for Information Technology Security Risk Assessment Procedures" dated 05/12/2003.

For technical questions relating to this handbook, please contact Jennifer Beale on 202-401-2195 or via e-mail.

DEPARTMENT OF EDUCATION
INFORMATION TECHNOLOGY SECURITY

Information Technology Security Risk Assessment Procedures

December 2003

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose

The *Risk Assessment Procedures* are intended to provide information to the Department of Education (Department) information technology (IT) security professionals (e.g., computer security officers [CSO], system security officers [SSO], network security officers [NSO]) responsible for the security of the Department's general support systems (GSS) and major applications (MA) and the risk analysis of those GSSs and MAs. These procedures are written with the assumption that the reader has some basic knowledge of IT security and the associated disciplines as described by the National Institute of Standards and Technology (NIST). The procedures outline a systematic, flexible, step-by-step approach that can be implemented consistently across the Department. It establishes the parameters and minimum standards required for a Department risk assessment as in accordance with Office of Management and Budget (OMB) Circular A-130, and NIST Special Publication (SP) 800-30. These procedures may be used by a system owner to: 1) perform risk assessments during all stages of the system's life cycle; 2) provide guidance to contractors responsible for developing a system in preparation for an independent risk assessment; and/or 3) understand the risk assessment reports performed by the independent risk assessor.

1.2 Background

Risk is a measure of the degree to which information resources are exposed based on the exploitation of a *vulnerability* by a potential *threat*[1]. Risk is composed of two elements: 1) the **impact** that an exploited vulnerability would have on the organization's mission or operations; and 2) the **likelihood** that such an exploitation would occur. A *risk assessment* is the process of analyzing and then interpreting risk associated with potential threats and vulnerabilities. The risk assessment acts as a means to help evaluate the effectiveness of various security controls in place for each GSS or MA[2].

The *Department of Education Information Technology Security Risk Assessment Procedures* is written to support the Department's risk management based *Department of Education Information Technology Security Policy*, which states that risk assessments must be performed at least every three years or whenever a significant change occurs to the GSS or MA.

1.3 Scope

The scope of these procedures includes what a risk assessment is, why a risk assessment is important, how a risk assessment feeds into the certification and accreditation (C&A) process, and the minimal security requirements for conducting a risk assessment. These procedures are based upon the *Department of Education Information Technology Security Policy*, *Department of Education Information Technology Security Program Management Plan*, NIST SP 800-30, OMB Circular A-130, and other applicable Federal IT security laws and regulations. The

[1] Vulnerability and threat are addressed in Section 2.

[2] According to NIST SP 800-18, Procedures for Developing Security Plans for Information Technology Systems, security controls are categorized into three domains: management, operational, and technical. These domains are discussed in further detail in Section 2.8.

process documented in these procedures will be used in performing risk assessments for all GSSs and MAs throughout the Department[3].

1.4 Structure

These procedures are organized into three major sections.

- Section 1 introduces the risk assessment process.
- Section 2 provides an overview of the major risk assessment concepts as well as how the risk assessment is related to the C&A process.
- Section 3 describes how to conduct a complete and thorough risk assessment (characterize the system, identify threats, identify vulnerabilities, analyze risk, recommend remediation measures, and document results).

Supporting the procedures are nine appendices; these appendices provide useful references (e.g., glossary of terms, acronyms, references, baseline security requirements (BLSRs), points of contact, vulnerability questionnaire, system disposal checklist, risk assessment report format, and risk assessment security action plan letter templates).

[3] The *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures* can be used to help determine if a particular system is a GSS or MA.

2. RISK ASSESSMENT CONCEPTS

2.1 Why Conduct a Risk Assessment?

The *Department of Education Information Technology Security Policy* requires risk assessments be performed on all GSSs and MAs. The purpose of the risk assessment is to quantify the impact of potential threats on a particular vulnerability to a GSS or MA. The benefits of performing a risk assessment include—

- Identifying GSS or MA weaknesses
- Enabling management to make informed decisions regarding implementation of security controls and remediation measures
- Promoting a consistent approach to measuring risk
- Allowing stakeholders to place values on potential losses
- Prioritizing levels of risk based on mission criticality and information sensitivity.

2.2 When Should a Risk Assessment be Conducted?

According to Federal regulations, Principal Officers are required to conduct a risk assessment of all GSSs or MAs at least every 3 years or when there is a major change in the GSS or MA environment, whichever occurs first. Ideally, some form of risk assessment must be performed during each phase of the system development lifecycle (SDLC)[4]. The phase of the SDLC during which the risk assessment is performed determines the level of detail, availability, and sometimes the sources of data. For example, the Baseline Security Requirements, in Appendix D, must be used as a checklist when performing a risk assessment for a GSS or MA in Phase 1 of the SDLC. Note that the System Disposal Checklist, in Appendix F must be utilized to ensure necessary steps have been taken to dispose of the GSS or MA. Table 1 describes the Department's SDLC phases and related risk assessment activities.

Table 1. SDLC Phases and Related Risk Assessment Activities

SDLC Phase	Risk Assessment Activity
Phase 1 – Project Initiation	Risks are identified to ensure security controls are being considered and will be built into the GSS or MA. Conduct a high-level risk assessment using the BLSRs in Appendix D as a checklist to ensure security controls are being considered and will be built into the GSS or MA.
Phase 2 – Requirements Specification	The risks identified during this phase are used to support the development of the systems requirements, including security requirements.
Phase 3 – Design	The risks identified during this phase can be used to support the security analyses of the GSS or MA that may lead to architecture and design trade-offs during the design phase. A GSS or MA Inventory submission form must be submitted to the Office of the Chief Information Officer (OCIO) during this phase. This will assess the anticipated mission criticality and information sensitivity of the system.

[4] It is best to perform a risk assessment early in the cycle to avoid security retrofits. These retrofits are often costly and require significant levels of effort.

SDLC Phase	Risk Assessment Activity
Phase 4 – Build	Examination of the requirements specification phase is performed to ensure that the business case, project plan, and risk management plan are followed.
Phase 5 – Test	Decisions regarding risks identified must be made prior to deployment. During this phase, and before the next phase of deployment, an independent risk assessment that meets the minimum standards of this procedures must be performed.
Phase 6 – Deploy	The risk management process supports the assessment of the GSS or MA implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system maintenance.
Phase 7 – Maintain	It is good practice to perform a risk assessment during the maintenance of the GSS or MA—in anticipation of the occurrence of an event or even after the occurrence of an event—to analyze vulnerabilities and recommend remediation measures.
Phase 8 – Disposal	Risk management activities are performed for GSS or MA components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that migration is conducted in a secure and systematic manner.

2.3 How is the Required Level of Effort for a Risk Assessment Determined?

Department automated information resources[5] (GSSs and applications) are categorized into one of five certification tiers (e.g., Tier 0 through Tier 4) as listed in Table 2. The certification tier of the GSS or MA determines the level of effort required for conducting risk assessments. Mission criticality and information sensitivity are two attributes used to determine the certification tier[6]. Note: A GSS or MA that is determined to be a Mission-Essential Infrastructure (MEI) Asset through the Critical Infrastructure Protection Survey is automatically considered a Tier 4 system.

For example, a risk assessment for a Tier 4 GSS or MA will consist of a fully documented, formal analysis, using the BLSRs and any additional system specific security requirements. In addition, vulnerability scanning is required as part of the risk assessment for a Tier 4 GSS or MA. However, a risk assessment for a Tier 1 system will consist of using the BLSRs as a checklist and a less detailed, documented analysis.

2.3.1 What if the GSS or Application is Categorized as a Tier 0?

Applications that are categorized as a Tier 0 are not considered MAs and therefore, do not require risk assessments. However, all GSSs are required to undergo a risk assessment, those that are categorized as a Tier 0 will utilize the level of effort associated with a Tier 1 GSS.

Table 2. Required Level of Effort for Risk Assessment

[5] Includes both government information and information technology resources.

[6] Refer to the *Department of Education Information Technology Security Certification and Accreditation Procedures* for further details on how the certification tier is determined for the GSS or MA.

Certification Tier	Required Level of Effort for Risk Assessment
0	No risk assessment required
1	Risk assessment (using BLSRs as a checklist)
2	Risk assessment (using BLSRs + additional system specific security requirements)
3	Risk assessment (using BLSRs + additional system specific security requirements + vulnerability scanning recommended)
4	Risk assessment (using BLSRs + additional system specific security requirements + vulnerability scanning)

2.4 How does the Risk Assessment Feed into the C&A Process?

The C&A process is comprised of the following four phases:

- Phase 1: Definition
- Phase 2: Verification
- Phase 3: Validation
- Phase 4: Post Accreditation

Risk assessments are performed as part of Phase 1[7]. The risk assessment is the foundation for developing all other security documents needed for certifying and accrediting the GSS and MA. The System Security Plan (SSP) must adequately address risks identified in the GSS or MA risk assessment report. The Configuration Management Plan (CMP) and the Contingency Plan (CP) further mitigate risks determined during the assessment. The Security Testing and Evaluation (ST&E) procedures will verify that critical risks highlighted in the risk assessment report have been corrected.

The result of the risk assessment yields an overall level of risk for the system. When using a qualitative methodology, risk values are rated as *high*, *medium*, or *low*. These results and other certification documentation are included as part of the C&A documentation provided to the Certifier[8]. Table 3 provides descriptions for each of these values. The risk level descriptions must be used consistently throughout the Department, resulting in a standardized approach to identifying risk levels.

Table 3. Risk Levels

Risk Level	Description
High	It is likely that exploitation of a given vulnerability by a threat will severely and adversely impact the Department, resulting in over one million dollars worth of damage and/or leading to legal ramifications (e.g., potential jail sentence). This rating indicates a strong need for corrective measures and actions.

7 Refer to the *Department of Education Information Technology Security Certification and Accreditation Procedures* for further information on the C&A process.

8 "Certification includes a comprehensive evaluation of the technical and non-technical security features and other IT system safeguards. Certification is performed in support of the accreditation process to establish the extent to which design and implementation of a particular system meet a set of specified security requirements." – *Department of Education Information Technology Security Policy*.

Medium	It is likely that an exploitation of a given vulnerability by a threat will moderately impact the Department, resulting in between 100,000 and one million dollars worth of damage or leading to legal action without the potential of a jail sentence. This rating indicates a strong need for corrective measures and actions.
Low	The given vulnerability may be subject to exploitation by a threat, but the probability of such exploitation is small and/or its impact on the Department's assets and resources would be minor, resulting in less than 100,000 dollars worth of damage or leading to administrative penalties. This rating indicates a need for corrective measures and actions.

2.5 Who is Responsible for Conducting the Risk Assessment?

The Principal Officer is responsible for ensuring that a risk assessment is conducted, for all GSSs and MAs for which he or she is responsible, in accordance with OMB Circular A-130. The risk assessment team must consist of individuals who are experienced in performing risk assessments (e.g., understand and have applied proven risk assessment methodologies). The team must have knowledge of Federal laws and regulations associated with risk assessments and have adequate technical knowledge of systems and networks. Risk assessment team members must be independent thus not having a vested interest in the GSS or MA being assessed. Thus, no individual from the Principal Office (PO) or any individual who supports or maintains the system should perform the risk assessment. The independent risk assessment team must work with the GSS or MA owners and those who administer and support the GSS or MA in order to obtain all the information needed for the assessment.

The primary requirement for the risk assessment team is that at least one member be considered an information security professional. This individual must have a working knowledge of information security controls and must ensure that all information and documentation gathered for the risk assessment is treated appropriately as Department sensitive information.

All of the roles and responsibilities for the risk assessment process are listed in the table below.

Roles	Responsibilities
Chief Information Officer	The Chief Information Officer (CIO) endorses the remediation plan submitted by the Principal Officer following a completed risk assessment.
OCIO Information Assurance Office	The Information Assurance (IA) office within the Office of the Chief Information Officer is responsible for developing Department of Education information technology security risk assessment policy, procedures and guidance. IA is also responsible for incorporating and monitoring completion of remediation actions into the Department of Education's FISMA action plan that is reported to OMB.
Principal Officer	The Principal Officer is responsible for ensuring that a risk assessment is conducted, for all GSSs and MAs for which he or she is responsible, in accordance with OMB Circular A-130. The Principal Officer participates in interviews with the Risk Assessment Team and submits the resulting risk assessment remediation plan to OCIO.

Roles	Responsibilities
Independent Risk Assessment Team	The independent risk assessment team completes the risk analysis of the system and documents the results in the final Risk Assessment Report. This team must work with the GSS or MA owners and those who administer and support the GSS or MA in order to obtain all the information needed for the assessment.
System Manager (SM)[9]	The SM represents the interests of the GSS or MA throughout the SDLC. The SM is responsible for ensuring the GSS or MA is operating in accordance with the security controls outlined in the SSP. The SM participates in interviews with and demonstrations of the system for the Risk Assessment Team. The SM signs off on the resulting risk assessment remediation plan that is submitted to OCIO.
Computer Security Officer (CSO)	The CSO manages the efforts of the C&A activities, including the risk assessment, and acts as the managing official for information security of GSSs or MAs within the PO. The CSO participates in interviews with and demonstrations of the system for the Risk Assessment Team. The CSO signs off on the resulting risk assessment remediation plan that is submitted to OCIO.
System Security Officer (SSO)	The SSO is directly responsible for the information security of a GSS or MA within the PO. The SSO ensures that security is considered at every point in the life-cycle process and manages the integrity of the GSS or MA. The SSO participates in interviews with and demonstrations of the system for the Risk Assessment Team. The SSO prepares the resulting risk assessment remediation plan that is submitted to OCIO.
User Representative	The user representative is responsible for ensuring that the user is able to conduct normal business activities with the particular GSS or MA. The user representative is the spokesperson for the user community representing the operational interests of the user. This representative ensures that user requirements are met during the SDLC allowing the user to perform the tasks defined in their job description. The user representative participates in interviews with and demonstrations of the system for the Risk Assessment Team.

2.6 What is Information Sensitivity and Mission Criticality?

Two very important elements must be considered when performing a risk assessment. *Information sensitivity* and *mission criticality* are key components that will be used to assess risk levels. This section addresses when and how information sensitivity and mission criticality are factored into the risk assessment. The intent of the following two sections is to simply define these two terms. A more thorough discussion of information sensitivity and mission criticality can be found in the *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures*.

[9] The System Manager is also known as the Program Manager.

2.6.1 Information Sensitivity

The criteria used to measure the information sensitivity include: information *confidentiality*, *integrity*, and *availability*. Figure 1 provides a description of each criteria element.

- **Confidentiality**: Protection from unauthorized disclosure.
- **Integrity**: Protection from unauthorized, unanticipated, or unintentional modification.
- **Availability**: Available on a timely basis to meet mission requirements or to avoid substantial losses.

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

Figure 1. Information Sensitivity Criteria

Information that is labeled "For Official Use Only" is confidential and must be protected from unauthorized disclosure. Unauthorized disclosure of this information may result in a tangible and intangible loss to the agency. Confidential information (i.e., information labeled as "For Official Use Only) is sensitive and may contain any of the following types of data—

- Proprietary business information that may not be released to the public under the Freedom of Information Act or other laws
- Personal data that requires protection under the Privacy Act of 1974.
- Source Selection information for contracts
- Deliberative process materials
- Monetary or budgetary information that would permit circumvention of security measures and internal controls

Refer to the *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures* for additional guidance on assigning levels of high, medium, or low for each information sensitivity criteria. This guidance will assist in determining an overall information sensitivity level for the GSS or MA and the data housed on that GSS or MA.

When considering the type of data transmitted, stored, or processed (e.g., privacy data) on the GSS or MA, it is important to note that sensitive information includes, but is not limited to—

- Social security numbers
- Personal addresses
- Credit history

2.6.2 Mission Criticality

In accordance with the *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures*, the criterion used to measure mission criticality is closely related to how integral the system is to supporting the mission of the Department.

Mission criticality may be measured as being either: *mission critical*, *mission important*, or *mission supportive.* Figure 2 provides a brief definition of these mission criticality types.

- **Mission Critical**: Automated information resources whose failure would preclude the Department from accomplishing its core business operations.
- **Mission Important**: 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**: 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. Mission Criticality Criteria

2.7 How are Threat and Vulnerability Defined?

2.7.1 Threat

A *threat* is defined as any circumstance, event, or act that could cause harm to the Department by destroying, disclosing, modifying, or denying service to automated information resources. There are three threat categories: natural, environmental, and human. Table 4 provides examples of threats found in each category.

Table 4. Threat Categories

Natural Disaster			
• Storm damage (e.g., flood, snow, hurricane)	• Fire	• Lightning strikes	• Earthquakes
Environmental Control Failures			
• Long-term power failure	• Chemicals	• Liquid leakage	• Pollution
Human			
• Assault on an employee	• Arson		• Blackmail
• Bomb or terrorism	• Browsing of Privacy Act and proprietary information		• Civil disorder
• Computer abuse	• Corrupted data input		• Falsified data input
• Fraud	• Hacking		• Impersonation
• Interception	• Labor dispute or Strike		• Malicious code
• Negligence or Human error	• Unauthorized disclosure of sensitive information		• Password guessing (e.g., dictionary attack)
• Replay	• Sabotage or Vandalism		• Social engineering
• Spoofing	• System tampering		• Theft

Natural disasters are caused by extreme weather or earthquake, and environmental control failures are caused by utility failures; a threat agent, someone who exploits system vulnerabilities, is the cause of human threats. Examples of human *threat agents* include the following—

- **Insiders**: Disgruntled employees, dishonest employees, and Department system users, both those with general system access and those with increased, privileged access.

- **Contractors and subcontractors**: Cleaning crew, developers, technical support personnel, and computer and telephone service repairmen

- **Former employees**: Employees who retired, resigned, or were fired

- **Unauthorized users**: Computer criminals, terrorists, and intruders (hackers and crackers) who attempt to access the Department's internal network

- **Authorized users**: Any approved user (e.g., government agency employee, contractor, business partner).

2.7.2 Vulnerability

A vulnerability is a condition that has the potential to be exploited by a threat. BLSRs, located in Appendix D, must be the initial security checklist used to determine vulnerabilities. BLSRs are a set of security requirements the Department views as the minimal security standards to be upheld by all GSSs and MAs. BLSRs must be used to determine vulnerabilities. Therefore, BLSRs that are not met must be flagged as vulnerabilities. Appendix E, Vulnerability Questionnaire is used as a supplement to the BLSRs. The questionnaire is provided to initiate probing. It is recommended that each PO amend the questions to reflect appropriate questions for their GSS or MA.

The following list contains sources to consider when identifying vulnerabilities to the GSS and/or MA—

- Previous risk assessments
- Security audits
- Bulletins [Computer Emergency Response Team (CERT), Federal Computer Incident Response Capability (FedCIRC), and Department of Energy's Computer Incident Advisory Capability (CIAC)]
- Vendor advisories
- System development test procedures
- System test results
- System audit logs

Proactive methods that can be used to collect vulnerability information include—

- Automated vulnerability scan
- Network mapping
- Security test and evaluation (ST&E)
- Penetration testing

Figure 3. Vulnerability Sources

Vulnerabilities are identified from information collected from each PO, its GSS or MA, and the environment. This information is collected during site surveys, interviews, network scanning, and documentation. Available industry sources must be used to identify vulnerabilities that may be applicable to specific systems (see Figure 3 for a list of sources). The specific sources of vulnerabilities and the methodology that must be used to identify them vary depending on whether the GSS or MA is in the design phase or has already been implemented.

If the GSS or MA has been neither designed nor implemented, vulnerabilities can be derived by understanding the weaknesses of the network components and operating systems being considered or proposed. If the GSS or MA is in the process of being designed and implemented, the vulnerability identification must be expanded to include more specific information. In this instance, automated tools and databases of known vulnerabilities may be used to identify appropriate GSS or MA security configurations. However, if the GSS or MA is operational, then the vulnerability identification must include an analysis of whether the security controls implemented were determined to be correct and effective.

2.7.3 Relationship Between Threat and Vulnerability

A vulnerability cannot be exploited unless there is a potential threat and associated threat agent. The threat agent must have the means, opportunity, and motivation to exploit a potential vulnerability. Based on this description, it is evident that threats and vulnerabilities are closely aligned when assessing risk. What might constitute a minor threat has the potential to become a greater threat, or a more frequent threat, because of a vulnerability.

2.8 Which Security Domains Should be Assessed?

The risk assessment must cover three security domains: *management*, *operational*, and *technical* controls. Table 5 defines the security areas as identified by NIST SP 800-26.

Table 5. Security Domains

Security Domain	Security Criteria
Management Controls **Procedures and management controls established for use of and access to the GSS or MA and its resources*	▪ Assignment of responsibilities ▪ Risk Management ▪ Authorize Processing ▪ Security Controls Review ▪ Privacy Act ▪ Rules of Behavior ▪ System Security Plan
Operational Controls **Procedures and operational controls established that focus on mechanisms implemented and that are executed by people*	▪ Configuration Management ▪ Contingency Planning ▪ Personnel Security ▪ Security Awareness and Training ▪ Physical Security ▪ Environmental Security ▪ Production Input/Output Controls ▪ Information Sharing ▪ Public Access Control ▪ Data integrity ▪ Incident Handling
Technical Controls **Procedures and technical controls established for securing processing, storage, and transmission of information*	▪ Identification and Authentication ▪ Logical Access Controls ▪ Auditing

2.9 What Information Gathering Techniques Should be Used When Conducting a Risk Assessment?

2.9.1 Questionnaire

To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management, operational, and technical controls planned or used for the GSS or MA. This questionnaire must be distributed to the appropriate technical and nontechnical management personnel who are designing or supporting the GSS or MA. The questionnaire must be used during site visits and interviews.

2.9.2 Interviews

Interviews with the Department's IT security professionals (e.g., CSO, NSO, SSO) and management personnel enable the risk assessment team to collect pertinent information about the system. Site visits enable the risk assessment team to observe and gather information about the physical, environmental, operational, and technical security of the GSS or MA.

2.9.3 Documentation Review

Risk assessments vary in scope and level of effort. Therefore, documentation used during the risk assessment may vary as well. The following documents must be used to assist in the preparation of the risk assessment—

- Mission statements
- GSS and MA Inventory Submission Form
- NIST SP 800-26, Security Self-Assessment Procedures for Information Technology Systems
- Organization and site-specific security policies and procedures
- Organization charts
- System functional requirements
- System and architecture design, including—
  - Lists of system components and applications
  - Diagrams and descriptions of the system architecture
  - Printouts of system component configurations (e.g., firewall and router policies, server and workstation configuration files)
  - System security controls documentation.
- Site operations manuals (facility specific)
- Standard operating procedures (SOP)
- Reports from prior risk analyses
- Physical security plans
- Configuration management plans and procedures
- Disaster recovery plans
- Site floor maps
- User manuals for specific systems under assessment.

2.9.4 Scanning Tools

Proactive technical methods can be used to collect system information efficiently. An example of this is the use of network mapping tools. These tools can provide a rapid profile of the GSS or MA being assessed.

While the Department does not advocate a particular scanning tool, the following tools are examples of products that have been used across the industry—

- **Network Mapper** (nmap) is a utility for scanning large networks using a variety of techniques to increase speed and minimize detection. It does not build a network topology, but identifies the services that are running on a large group of hosts by scanning networks for the open transport control protocol (TCP) and user datagram protocol (UDP) ports on each host. Usually, nmap is used for initial scans because it provides a quick way to build individual profiles of the target systems.

- **CyberCop Scanner** is a commercial network security vulnerability detection product that scans an entire network or individual hosts to verify and report network and system security issues. It tests for a comprehensive set of known security

vulnerabilities, but does not provide details on how to exploit them. Since CyberCop takes some time to complete a scan, this tool is normally applied after narrowing the targets down to a focus group.

- **Nessus** is a free, powerful, and easy-to-use security scanner that remotely audits a given network in order to determine whether crackers may break into it, or misuse it in some way. Taking nothing for granted, Nessus does not consider that a given service is running on a fixed port.

- **Security Auditor's Research Assistant (SARA)** is a third-generation, Unix-based security analysis tool that is based on the SATAN (Security Administrator Tool for Analyzing Networks) model. SARA is adapted to interface with other community products. For example, SARA interfaces with the nmap package for superior "operating system fingerprinting." Additionally, SARA provides a transparent interface to Samba (an open source suite that provides seamless file and print services to SMB[10]/CIFS[11]) for security analysis.

- **Internet Security Systems (ISS) Database Scanner** is a commercial tool that automatically scans databases for vulnerabilities from a single-user interface and displays scan results and fixes information in clear reports that allow users to respond quickly to critical vulnerabilities. Specifically, the Database Scanner penetration testing feature automatically probes a database through default accounts and password cracking, finding vulnerabilities that a knowledgeable attacker would exploit to gain access to database servers and an organization's critical data or network.

- **Security Administrator's Integrated Network Tool (SAINT)** is a tool that gathers information about remote hosts and networks by examining services such as finger, network file system (NFS), Network Information System (NIS), file transfer protocol (ftp), trivial file transfer protocol (tftp), and Remote Execution Daemon (rexd). Based on initial data collection and a user-configurable rule set, SAINT examines the avenues of trust and dependency and iterates further data collection runs over secondary hosts. This allows the user to analyze the network or hosts, as well as examine the real implications inherent in network trust and services.

10 Small Message Block that is utilized for Windows NT packets.
11 Common Internet File System.

3. CONDUCTING A RISK ASSESSMENT

Figure 4 illustrates the multi step methodology that must be used when conducting a risk assessment. Inputs, major activities, and outputs for each step are represented. Inputs are identified by an 'I', and outputs are identified by an 'O'.

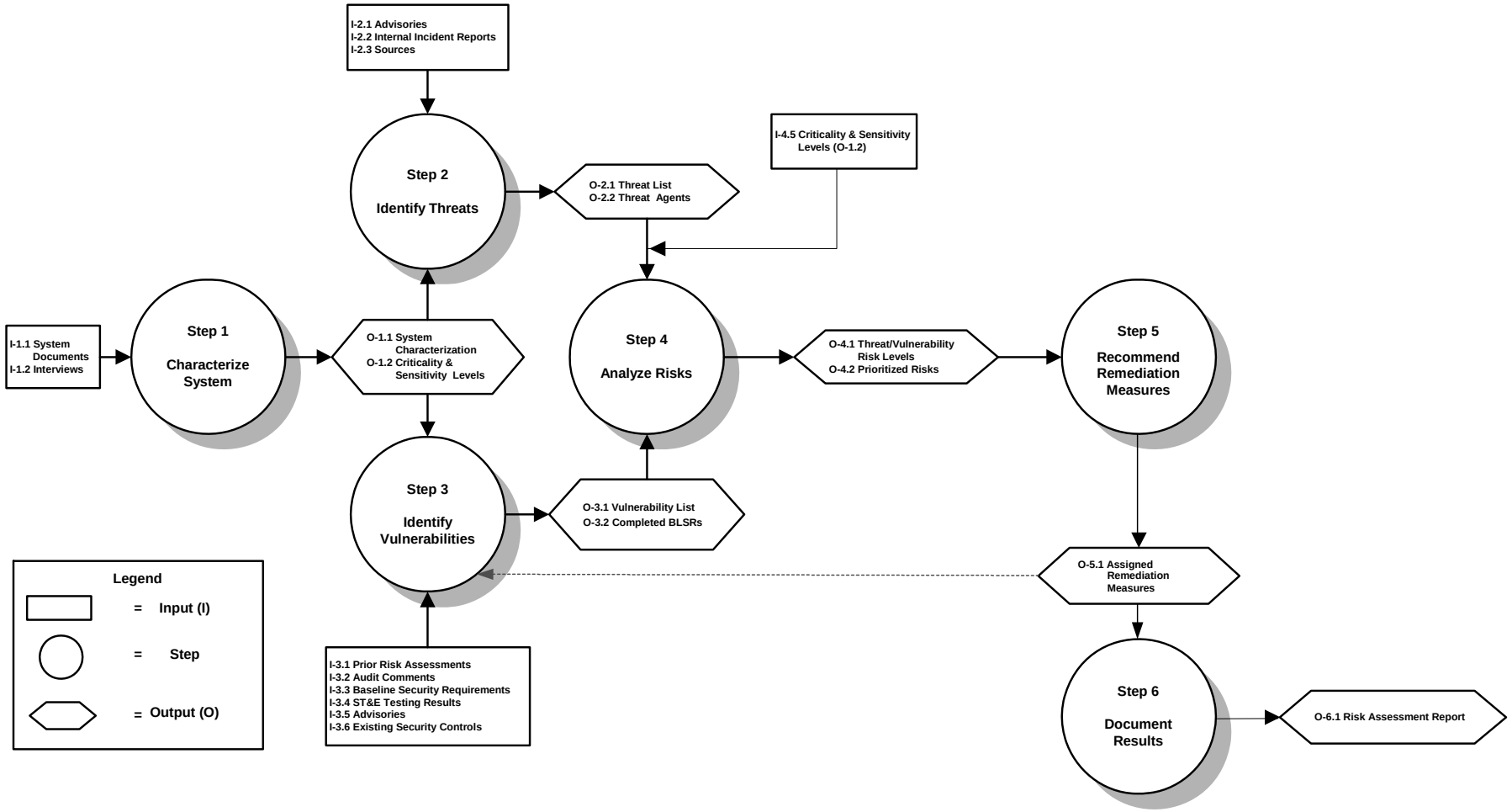

Figure 4: Risk Assessment Process Details

The following sections provide detailed step-by-step actions that must be taken when performing a risk assessment. The methodology described below is based on a qualitative approach to assessing risk. This means that there are no numerical values calculated, rather a rating of *high*, *medium*, or *low* is assigned. The methodology is based on NIST SP 800-30 (Risk Management Procedures for IT Systems)[12].

3.1 Step 1: Characterize the System

The first step to be performed as part of the risk assessment is to *characterize* the system. Figure 5 illustrates inputs and outputs to consider in this initial step. Step 1 requires gathering inputs such as system documents (I-1.1)[13] and conducting interviews (I-1.2) to obtain important information such as—

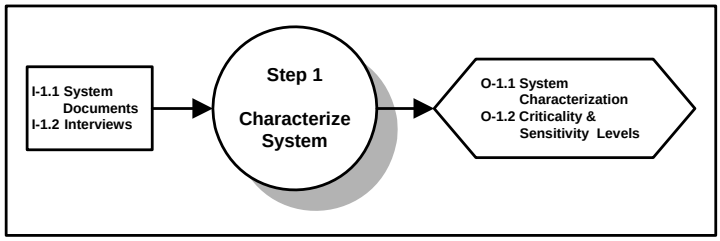

Figure 5. Characterize System

- Organization's mission
- Operations of the organization
- Policies of the organization or system
- Processes of the organization
- Operating environment of the organization or system
- Information storage and flows
- System security requirements
- System security architecture
- System and network security controls
- Physical and procedural security controls
- Functional requirements
- Organization's security posture

Data collected from existing documentation including the GSS and MA inventory submission form for the system and personnel interviews must be reviewed and analyzed to determine the system boundaries, functionality, and security requirements. These data points are essential elements of the risk assessment. A proper risk assessment cannot be performed until the system boundaries are identified and the security requirements are established. These requirements, along with other system-unique security requirements, will form the BLSRs. The characterized system provides the foundation for the remaining steps of the risk assessment process.

Mission criticality and information sensitivity levels must be determined as part of Step 1 activities[14]. The mission criticality and information sensitivity of systems and data are instrumental in determining threats (Step 2) to and vulnerabilities (Step 3) of the GSS or MA.

---

12 NIST SP 800-30 identifies nine steps while this methodology streamlines the process into six steps. Step 4 consolidates four of the nine NIST risk assessment steps (i.e., Step 4: Control Analysis, Step 5: Likelihood Determination, Step 6: Impact Analysis, Step 7: Risk Determination) into one and is entitled "Risk Analysis".

13 Section 2.9.3 contains a list of documents that may be used as part of the risk assessment.

14 Refer to the Section 2.6 for further information on how criticality and sensitivity levels are determined.

3.2 Step 2: Identify Threats

The outputs from Step 1, system characterization (O-1.1) and the mission criticality and information sensitivity levels (O-1.2) are used in identifying and developing a realistic list of *potential* natural and man-made *threats and threat agents*. Advisories, interviews, incident reports, and other sources must be used as resources to determine potential threats. Figure 6 illustrates the data flow for Step 2.

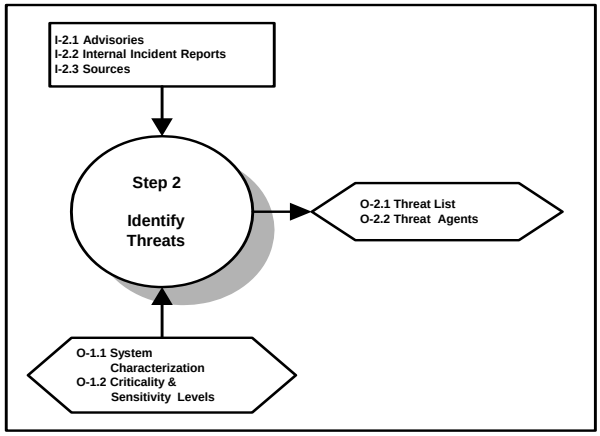

Figure 6. Identify Threats

3.3 Step 3: Identify Vulnerabilities

Step 3, depicted in Figure 7, systematically evaluates the weaknesses associated with the system resources and information, thus resulting in a list of potential *vulnerabilities*. Several inputs are used to identify the system's vulnerabilities: prior risk assessments, audit comments, ST&E results, advisories, interviews with key personnel,[15] and existing security controls. System characterization and mission criticality and information sensitivity levels must also be considered when identifying vulnerabilities.

The most challenging part of this step is to thoroughly assess the GSS or MA in accordance with the BLSRs[16]. Upon completing the BLSRs, any requirement not met must be deemed a vulnerability. In addition to using the BLSRs, refer to other valid vulnerability sources (e.g., testing results, security advisories) to ensure that all resources are exhausted and a thorough list of vulnerabilities is compiled.

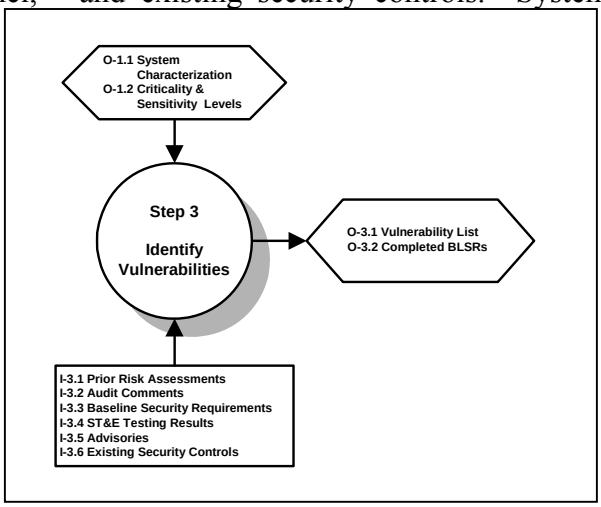

Figure 7. Identify Vulnerabilities

At the end of Step 3, a list of system vulnerabilities must be created. This list must be mapped to the threats identified in Step 2. To help track the findings, it is recommended that a Risk Assessment Matrix, be used to record the BLSRs, threats, and vulnerabilities. Note that there might be several threat/vulnerability pairs mapped to a single BLSR.

15 See Appendix E, Vulnerability Questionnaire for a list of suggested questions.

16 See Appendix D, Baseline Security Requirements.

3.4 Step 4: Analyze Risk

Analyzing risk to the system requires assessing threats, vulnerabilities, mission criticality, and information sensitivity levels (see Figure 8). These components were determined in the prior steps of the risk assessment. Therefore, the objective of Step 4 is to compose a *risk statement* and assign *risk levels* to each of the threat/vulnerability pairs documented on the Risk Assessment Matrix. To determine risk, use the following equation:

Risk = Impact x Likelihood

The following steps provide specific instructions for analyzing risk.

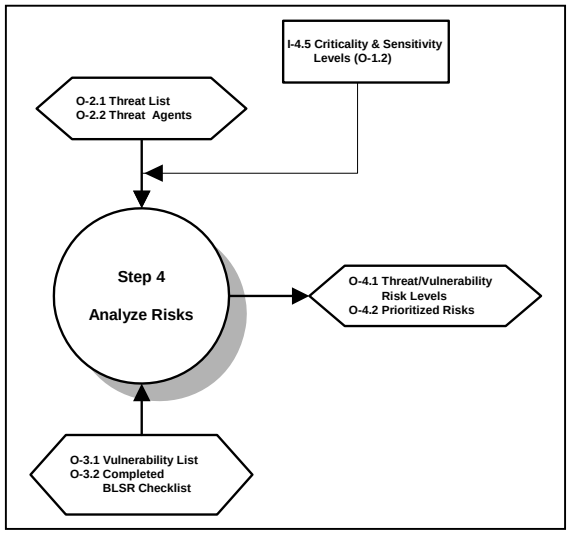

Figure 8. Analyze Risk

Step 4.1: Determine Impact. Impact refers to the magnitude of potential harm that may be caused by exploitation of a vulnerability. The mission criticality and information sensitivity of both the system and data are useful procedures for assessing the potential impact of an exploited vulnerability. However, other attributes must be taken into consideration when determining impact. For example, the value of the resource at risk, both in terms of its inherent value and its importance to the Department's mission as well as the negative effects (i.e., lost revenue or public embarrassment) that the Department may experience must be considered. The level of impact will be rated as high, medium, or low. Table 6 provides a description for each level of impact. These are standard definitions to be used for all Department risk assessments.

Table 6. Impact Descriptions

Impact	Description
High	May result in the *loss of significant* or major tangible assets, information, or information resources. May significantly disrupt or impede the organization's mission or seriously harm its reputation or interest (e.g., loss of mission-critical system data by unauthorized users gaining access to the Department's intranet).
Medium	May result in the *loss of some* tangible assets, information, or information resources. May disrupt or harm the organization's mission or harm its reputation or interest. For example, authorized users are not able to access mission-supportive data for several days.
Low	May result in the *loss of minimal* tangible assets, information, or information resources. May adversely affect the organization's mission, reputation, or interest. For example, authorized users are not granted access to mission-supportive data for an hour.

Step 4.2: Determine Likelihood. Likelihood is determined by considering threats and vulnerabilities. The likelihood that a vulnerability will be exploited by a threat can be assessed and described as *high, medium*, or *low*. Factors that govern the likelihood of vulnerability exploitation include threat capability, frequency of threat occurrence, and effectiveness of current remediation measures. Refer to Table 7 to determine the likelihood level for the threat/vulnerability pair for Department risk assessments.

Table 7. Likelihood Descriptions

Likelihood	Description
High	The capability of the threat is significant, and/or remediation measures to reduce the probability of vulnerability exploitation are insufficient.
Medium	The capability of the threat is medium, and implemented remediation measures lessen the probability of vulnerability exploitation.
Low	The capability of the threat is limited, and remediation measures are in place that effectively reduces the probability of vulnerability exploitation.

Once the threat capability and remediation measure effectiveness have been assessed for each threat/vulnerability pair, use Table 8 below, for Department risk assessments, to determine the overall likelihood of the threat exploiting the vulnerability. For example, suppose the capability level of having your computer hacked is *high,* but due to the installation of various system scanning tools your remediation measure is also *high*. Based on the likelihood matrix found in Table 8, the likelihood of your computer actually getting hacked is *medium*.

Table 8. Likelihood Matrix

	Remediation Measure Effectiveness		
Threat Capability	***High***	***Medium***	***Low***
High	Medium	High	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

Step 4.3: Assign Risk Level. Now that values have been assigned to impact and likelihood, use the matrix below, for Department risk assessments, to determine the risk level for the threat/vulnerability pair. The level of risk equals the intersection of the likelihood and impact values. For example, suppose the likelihood level is *high* and the impact level is *low* for the threat/vulnerability pair. Based on the risk level matrix found in Table 9, the risk level would be *medium*[17].

[17] In reference to Table 9 Risk Level Matrix, impact carries greater weight than likelihood.

Table 9. Risk Level Matrix

	Likelihood		
Impact	***High***	***Medium***	***Low***
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Step 4.4: Prioritize Risks. After a system owner receives the independent risk assessment report, the system owner will need to prioritize each risk in the process of developing a remediation plan to address the identified risks. This process must be performed based on the mission and objectives of the GSS or MA. Mission criticality and business functions included in the GSS or MA inventory submission form for the system must be considered in this process. In addition, the cost analysis and benefits of mitigating the risks must be assessed. While some offices may choose to rank their risk levels based on time constraints (long term vs. short term) others may choose to prioritize risk level based on cost and level of effort. The process of prioritizing risk mitigation is something that must be tailored based on system-specific needs.

3.5 Step 5: Identify Recommendations

Step 4 yielded a risk statement with an associated risk level. This input is used to determine *remediation measures* that must be applied as a means to mitigate risks. Figure 9 provides a visual procedures of how outputs from Step 4 are used as inputs for Step 5.

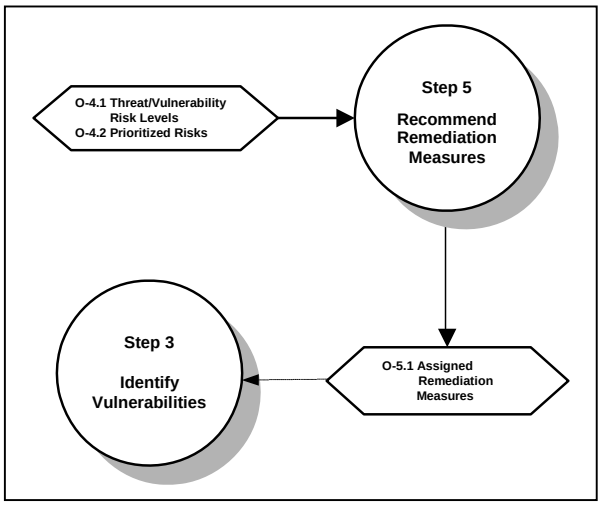

Figure 9. Recommend Remediation Measures

A remediation measure is any device, procedure, safeguard, technique, or other measure that reduces a risk or a vulnerability. When identifying recommended remediation measures be sure to consider level of effort, costs, emerging technologies, time constraints, and feasibility. There are three types of controls that must be implemented: management, operational, and technical[18]. After remediation measures are identified, they must be re-evaluated to ensure that new vulnerabilities are not introduced.

By completing Step 5, the risk assessment is complete. Step 6 explains how the risk assessment must be documented in a final report.

[18] See Section 2.8 for a definition of each security control category.

3.6 Step 6: Document Results

Appendix G provides the format to be used when documenting the risk assessment approach, documentation used, personnel interviewed, and the completed Risk Assessment Findings. Inputs and outputs of this step are illustrated in Figure 10.

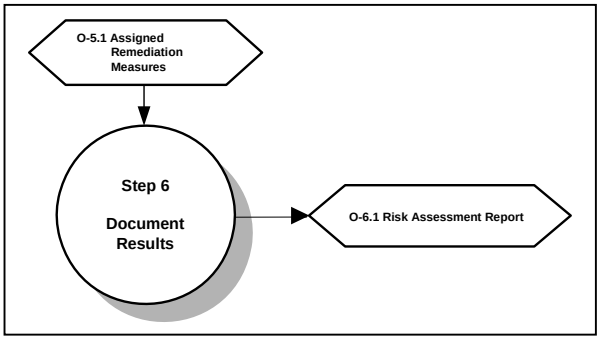

Figure 10. Document Results

POs are responsible for taking necessary action steps to fulfill the Department's IT security requirements for each risk assessment. As documented below, cover memos, which outline agreements between established parties, must be submitted with each risk assessment report. Following receipt of the risk assessment report the Senior Officer will analyze the results, identify risk mediation measures and costs, and develop a security action plan.

Each Senior Officer must submit their PO security action plan to the CIO. The CIO will review the PO security action plan and contact the Senior Officer if there are any questions or concerns. The security action plan includes the following:

- **Memorandum from the Principal Officer**—This cover memo is submitted to the CIO from the Principal Officer. This letter acknowledges that a comprehensive risk assessment was performed for a specific GSS or MA as in accordance with Federal requirements. The letter further establishes concurrence or non-concurrence with the risk assessment findings.

- **Remediation Measure Chart**—This form is submitted to the CIO from the Principal Officer and documents the risk assessment findings and their corresponding remediation measures. Remediation measures must be acknowledged for each risk assessment finding that the PO concurs with.

- **Non-Concurrence Chart**—This form is submitted to the CIO from the Principal Officer and documents the risk assessment findings that the PO did not concur with. The rationale must be documented for each non-concurrent finding. This form is only submitted when non-concurrence exists for a risk assessment finding.

- **Memorandum from the CIO**—This cover memo is submitted to the Principal Officer from the CIO. This letter acknowledges that appropriate remediation measures have been proposed which adequately address all of the risk identified in the risk assessment report.

Templates of these documents are located in Appendix H. Remediation measures must be provided for all High and Medium risks as identified in the report. For all risks identified as Low, the submission will include either proposed remediation measures or explanations of a risk-based decision not to apply a remediation measure.

4. SUMMARY

Risk assessments are an integral part of securing IT assets and are required for all GSSs and MAs under OMB Circular A-130. These procedures provide the parameters and minimum security requirements for Department risk assessments. The process documented in these procedures must be used consistently throughout the Department, resulting in a standardized approach to performing risk assessments. These procedures were prepared to assist those IT security professionals who are responsible for conducting risk assessments on various GSSs or MAs. The procedures address key risk assessment concepts and terms and provides a step-by-step methodology that can be used as a roadmap when measuring risks to the GSSs or MAs. It is not, however, a textbook on how to execute a risk assessment or a comprehensive examination of the skills needed, or factors to consider, when performing a risk assessment.

For specific questions or comments regarding the content of these procedures, please contact the Information Assurance staff within the OCIO.

APPENDIX A. GLOSSARY OF TERMS

Baseline Security Requirements
A set of obligatory standards, which serves as the basis for Management, Operational and Technical system security configuration, and by which system security controls are measured. Baseline Security Requirements can only be modified through a formal process of change control.

General Support System
An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports 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 (IPSO). Reference the *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures* for more details.

Major Application
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 protection. 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 systems in which they operate. See the *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures* for more details.

Remediation Measures
Any action, device, procedure, technique, or other measure that reduces a risk or a vulnerability.

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

Risk
A measure of the degree to which information resources are exposed based on the exploitation of a vulnerability by a threat.

Risk Assessment
The process of analyzing threats to and vulnerabilities of an information system to determine the risks (potential for losses), and using an analysis as a basis for identifying appropriate and cost-effective measures.

Risk Management
The process concerned with identification, measurement, control, and minimization of security risk in information systems.

Safeguards
Protective measures and controls that are prescribed to meet the security requirements specified for the system to include security features as well as management constraints; personnel security; and security of physical structures, areas and devices.

System
A collection of components organized to accomplish a specific function or set of functions.

System Development Life Cycle
A structured approach for systems development from planning and support to disposal of the system. A proven series of steps and tasks utilized to build and maintain quality systems faster, at lower costs, and with less risk.

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

Vulnerability
A condition that has the potential to be exploited by a threat. A weakness in an information system or component that could be exploited by a threat.

APPENDIX B. ACRONYMS

AIS	Automated Information System
BLSR	Baseline Security Requirements
C&A	Certification and Accreditation
CERT	Computer Emergency Response Team
CIAC	Computer Incident Advisory Board
CIFS	Common Internet File System
CMP	Configuration Management Plan
CP	Contingency Plan
CSO	Computer Security Officer
FedCIRC	Federal Computer Incident Response Capability
FTP	File Transfer Protocol
GSS	General Support System
IPSO	Information Processing Service Organization
ISS	Internet Security Systems
IT	Information Technology
LAN	Local Area Network
MA	Major Application
NFS	Network File System
NIS	Network Information System
NIST	National Institute of Standards and Technology
NMAP	Network Mapper
NSO	Network Security Officer
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PO	Principal Office
REXD	Remote Execution Daemon
SAINT	Security Administrator's Integrated Network Tool
SARA	Security Auditor's Research Assistant
SATAN	Security Administrator Tool for Analyzing Networks
SDLC	System Development Life Cycle
SMB	Small Message Block

SOP	Standard Operating Procedures
SP	Special Publication
SSO	System Security Officer
SSP	System Security Plan
ST&E	Security Test and Evaluation
TFTP	Trivial File Transfer Protocol
TCP	Transport Control Protocol
UDP	User Datagram Protocol

APPENDIX C. REFERENCES

CSA of 1987 Computer Security Act of 1987

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

ED C&A Procedures Department of Education Information Technology Security Certification and Accreditation Procedures, current version on connectED

ED CIPP Department of Education Critical Infrastructure Protection Plan

ED CMPG Department of Education Configuration Management Program Procedures

ED COOP Department of Education Continuity of Operations Planning Program Guidance, current version on connectED

ED IT Security Awareness and Training Program Procedures

Department of Education Information Technology Security Awareness and Training Program Procedures, current version located on connectED

ED ITSP Department of Education Information Technology Security Policy, current version located on connectED

ED ITGSS & MA Inventory Procedures

Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures, current version located on connectED

ED ITSPMP Department of Education Information Technology Security Program Management Plan, current version located on connectED

ED Incident Handling Program Procedures

Department of Education Incident Handling Program Procedures, current version located on connectED

ED Personal Use of Department Equipment

Department of Education Personal Use of Department Equipment Policies and Procedures, current version located on connectED

ED Portable AIS Security Guidance

	Department of Education Portable Automated Information System Security Guidance
ED SDLC	Department of Education ED/System Development Life-Cycle Methodology *Handbook* Release 1.0 March 1999, current version located on connectED
FIPS 31	National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), Procedureslines for Automatic Data Processing Physical Security and Risk Management, June 1974 (http://csrc.nist.gov/publications/fips/)
FIPS 87	National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), Procedureslines for ADP Contingency Planning, March, 1987 (http://csrc.nist.gov/publications/fips/)
FIPS 102	National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), Procedureslines for Computer Security Certification and Accreditation, September 1983 (http://csrc.nist.gov/publications/fips/)
FIPS 112	National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), Password Usage, May 1985 (http://csrc.nist.gov/publications/fips/)
FIPS 191	National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), Procedureslines for The Analysis of Local Area Network Security November 1994 (http://csrc.nist.gov/publications/fips/)
NIST SP 800-12	National Institute of Standards and Technology (NIST), An Introduction to Computer Security: The NIST Handbook, October 1995 (http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf)
NIST SP 800-18	National Institute of Standards and Technology (NIST), Procedures for Developing Security Plans for Information Technology Systems, December 1998 (http://csrc.nist.gov/publications/nistpubs/800-18/Planprocedures.pdf)
NIST SP 800-26	National Institute of Standards and Technology (NIST), Security Self-Assessment Procedures for Information Technology Systems, November 2001 (http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf)
NIST SP 800-30	National Institute of Standards and Technology (NIST), Risk Management Procedures for Information Technology Systems, October 2001

(http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

NIST SP 500-169 National Institute of Standards and Technology (NIST), Executive Procedures to the Protection of Information Resources, 1989 (http://csrc.nist.gov/publications/nistpubs/500-169/sp500-169.txt)

OMB Circular A-130

Office of Management and Budget (OMB), Management of Federal Information Resources, Circular A-130, 28 November 2000 (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)

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

APPENDIX D. BASELINE SECURITY REQUIREMENTS (BLSRS)

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
5. MANAGEMENT CONTROLS							
5.1.1 Authorize Processing							
1.	The system is certified and accredited at least every three years, or when a significant change occurs to the system.	▪ ED Handbook for IT Security Policy ▪ FIPS 102 ▪ ED Handbook for IT Security C&A Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
5.1.2 Life Cycle							
2.	Security requirements are identified during the system design.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26					
3.	An initial risk assessment is performed to determine system security requirements.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26 ▪ NIST SP 800-30					
4.	Appropriate security controls with associated evaluation and test procedures are developed before the procurement action.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
5.	System documentation is modified to reflect the current system environment	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
6.	Design reviews and system tests are performed prior to placing the system into production and the results are documented and maintained.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
7.	A system development life cycle methodology is documented and implemented.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26					
8.	Solicitation documents (e.g., Request for Proposal) include security requirements and evaluation/ test procedures	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					
9.	The requirements in the solicitation documents permit updating security controls as new threats/ vulnerabilities are identified and as new technologies are implemented.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					
10.	The budget request includes the security resources required for the system.	▪ ED Handbook for IT Security Policy ▪ FISMA ▪ Clinger-Cohen ▪ NIST SP 800-26					
11.	The business case documents the resources required for adequately securing the system.	▪ ED Handbook for IT Security Policy ▪ Clinger-Cohen ▪ NIST SP 800-26					
	Privacy Act						
12.	Appropriate administrative, technical, and physical security controls are documented and implemented to ensure the security and confidentiality of Privacy Act information.	▪ ED Handbook for IT Security Policy ▪ Privacy Act ▪ ED IT Security Controls Reference Guide					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
13.	Policies and procedures for disclosing Privacy Act information upon the request by an individual are documented and implemented.	▪ ED Handbook for IT Security Policy ▪ Privacy Act					
14.	Policies and procedures regarding the storage, retrieval, access, retention, and disposal of Privacy Act information are documented and implemented.	▪ ED Handbook for IT Security Policy ▪ Privacy Act ▪ ED IT Security Controls Reference Guide					
5.1.3 Risk Management							
15.	An independent risk assessment is conducted on the system at least every three years or when a significant change occurs to the system to identify risks based on the adequacy of the security controls in place.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Risk Assessment Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
16.	All security controls, currently implemented and planned, are consistent with the system criticality and data sensitivity levels.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
17.	Threat sources, both natural and manmade, are identified and a list of known system vulnerabilities that could be exploited by a threat source is developed and updated.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Risk Assessment Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
18.	A mission/ business impact analysis is conducted	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Contingency Planning Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
19.	The system criticality and data sensitivity levels of the system are determined and documented.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security C&A Procedures ▪ NIST SP 800-12 ▪ NIST SP 800-18 ▪ NIST SP 800-26					
20.	Corrective Actions are developed and implemented by management to address system risks identified during independent risk assessments and security reviews.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Risk Assessment Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
5.1.4 Rules of Behavior							
21.	Rules of behavior are established in writing to clearly delineate respons-bilities, document expected behavior of all users, and consequences of inconsistent behavior or noncompliance.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
22.	Rules of behavior are available to every user prior to receiving authorization for access to the system. The rules of behavior contain a signature page for each user to sign acknowledge receipt of, understanding of, and compliance with the rules.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
Security Controls Review							
23.	A NIST Self-Assessment is conducted on a regular basis.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
24.	Security controls are reviewed on a periodic basis (a minimum of once every three years or whenever the system facilities, or other conditions change).	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide					
5.1.5 System Security Plan							
25.	The system security plan is periodically reviewed and adjusted to reflect current conditions and risks.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
26.	The system security plan is documented in accordance with OMB Circular A-130, Appendix III and NIST Special Publication 800-18 and approved by management.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26					
27.	A summary of the system security plan is incorporated into the strategic IRM plan.	▪ NIST SP 800-18 ▪ NIST SP 800-26					
28.	The system security plan clearly identifies the system owner and who is responsible for managing access to the system.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18					
29.	The individual responsible for security of the system is assigned, in writing, in the system security plan.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ OIG Logical Access Controls Checklist					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
6. OPERATIONAL CONTROLS							
6.1.1 Configuration Management							
30.	The system configuration baseline is documented and is updated to reflect the current system environment. All hardware and software supporting the system is identified and documented in detail (i.e., manufacturer/ vendor name, model number/ version, serial number, etc.) as part of the baseline.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security CM Planning Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
31.	Change control procedures are documented and followed to ensure that changes are controlled as a system progresses from testing to final approval.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ ED Handbook for IT Security CM Planning Procedures ▪ NIST SP 800-26					
32.	All hardware and software change requests are documented, approved, and maintained.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ ED Handbook for IT Security CM Planning Procedures ▪ NIST SP 800-26					
33.	An impact analysis is conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security CM Planning Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
34.	Emergency change requests are documented, either prior to or after the changes are implemented, approved by management and are maintained.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security CM Planning Procedures ▪ NIST SP 800-26 ▪ FISCAM					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
35.	All hardware and software maintenance and repair activities are approved and documented.	▪ ED Handbook for IT Security Policy ▪ ED Information Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
36.	New or revised software distribution implementation orders, including effective dates, are documented, reviewed, and provided to all locations.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
37.	System components (operating system, utility, applications) are tested using test data and results that are documented and approved prior to production.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM					
6.1.2 Contingency Planning							
38.	An inventory is documented for all system software, applications, and computer and telecommunications hardware, including the name and brief description of sensitive applications and facilities.	▪ ED Handbook for IT Security Policy ▪ FISMA ▪ FIPS 31 ▪ FIPS 87 ▪ NIST SP 500-169					
39.	Emergency response procedures are documented, distributed to all personnel, and periodically tested and updated.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					
40.	Backup procedures are documented and implemented.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Contingency Planning Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
41.	A contingency plan is documented, periodically tested (at least once a year) under conditions that simulate disasters, and readjusted as appropriate, including all associated documentation.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Contingency Planning Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
42.	The contingency plan is distributed to all appropriate personnel.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Contingency Planning Procedures ▪ NIST SP 800-26 ▪ FISCAM					
43.	The contingency plan is approved by key affected parties.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26					
44.	Processing priorities are established, documented, and approved by management.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
45.	Copies of system and application documentation are maintained at the off-site location.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Contingency Planning Procedures ▪ NIST SP 800-26 ▪ FISCAM					
46.	An up-to-date copy of the contingency plan is securely stored off-site.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Contingency Planning Procedures ▪ NIST SP 800-26 ▪ FISCAM					
47.	Detailed instructions for restoring operations are documented.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Contingency Planning Procedures ▪ NIST SP 800-26 ▪ FISCAM					
48.	An alternate processing site with a contract or interagency agreement exists.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Contingency Planning Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
49.	The off-site storage facility and alternate processing site are geographically removed from the primary site and provide proper physical and environmental security controls.	▪ ED Handbook for IT Security Policy ▪ FIPS 31 ▪ ED Handbook for IT Security Contingency Planning Procedures					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
50.	Specific responsibilities are documented and assigned in the contingency plan and affected employees have been trained and are aware of their roles and responsibilities contained in the contingency plan.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Contingency Planning Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
51.	The most critical data files and sensitive operations and their supporting computer resources are identified and documented.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
52.	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	▪ ED Handbook for IT Security Policy ▪ ED Handbook for IT Security Contingency Planning Procedures ▪ NIST SP 800-26 ▪ FISCAM					
53.	All system defaults are reset after being restored from a backup.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
	Data Integrity						
54.	Integrity verification programs are used by applications to look for evidence of data tampering, errors, and omissions.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					
55.	Reconciliation routines are used by applications (i.e., checksums, hash totals, and record counts).	▪ NIST SP 800-18 ▪ NIST SP 800-26					
56.	Trust relationships among hosts and external entities are appropriately restricted.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26					
57.	Sensitive data transmissions are encrypted.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
58.	If encryption is used, it meets federal standards and includes procedures for key generation, distribution, storage, use, destruction, and archiving.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
59.	All workstations and Department-owned portable computing devices have Department approved virus detection software installed. Updates to the virus definition tables are automatically "pushed" to each machine.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
60.	Virus scans are automatic and virus signature files are routinely updated.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
61.	Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended.	▪ NIST SP 800-26					
62.	Message authentication is used.	▪ NIST SP 800-18 ▪ NIST SP 800-26					
63.	Cryptographic tools are implemented to protect the integrity and confidentiality of sensitive and critical data and software programs.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-12					
64.	Sensitive data files are encrypted on all portable systems.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-14 ▪ NIST SP 800-26					
6.1.3 Documentation							
65.	Software and hardware testing procedures and results are documented and maintained.	▪ NIST SP 800-18 ▪ NIST SP 800-26					
66.	Network diagrams and setups of routers and switches are documented and maintained.	▪ NIST SP 800-18 ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
67.	Standard operating procedures are documented and are available.	▪ ED IT Physical Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
68.	Vendor-supplied documentation of hardware, software, and application documentation (i.e., in-house or COTS), including user manuals, is available.	▪ ED IT Physical Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
6.1.4 Environmental Security							
69.	Controls are implemented, regularly tested, and properly maintained to mitigate environmental threats (e.g., long-term power failure, liquid leakage, and pollution).	▪ ED IT Physical Security Policy ▪ FIPS 31 ▪ ED IT Security Controls Reference Guide					
70.	Fire suppression and prevention devices are installed, working, and are tested (e.g., smoke detectors, fire extinguishers, and sprinkler systems).	▪ ED IT Physical Security Policy ▪ FIPS 31 ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
71.	Building plumbing lines do not endanger the computer room, or, at a minimum, shut-off valves and procedures exist and are known.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18					
72.	The computer room has an uninterruptible power supply (UPS) and/or back up generator(s) in case of power outage.	▪ ED IT Physical Security Policy ▪ FIPS 31 ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
73.	Heating systems are regularly maintained.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
74.	The computer room has a redundant air-cooling system.	▪ ED IT Physical Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26 ▪ FISCAM					
75.	Electric power distribution, heating plants, water, sewage, and other utilities are periodically reviewed for risk of failure.	▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM					
6.1.5 Incident Handling							
76.	System performance monitoring is used to analyze system performance logs in real time to look for availability problems, including active attacks.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
77.	Inappropriate, unusual, and suspicious access activity is reported, investigated, and appropriate actions are taken.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26 ▪ FISCAM					
78.	Up-to-date procedures are in place for using and monitoring use of system utilities.	▪ NIST SP 800-26 ▪ FISCAM					
79.	A formal incident response capability, including a process for reporting, monitoring, tracking incidents until resolved, and maintaining the reports for a specified period of time, is documented and available.	▪ ED IT Security Controls Reference Guide ▪ ED Information Security Incident Handling Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
80.	Incident information and common vulnerabilities or threats are shared with owners of interconnected systems and are reported to FedCIRC, NIPC, and local law enforcement when necessary.	▪ ED Information Security Incident Handling Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
81.	Intrusion detection reports are routinely reviewed and suspected incidents are handled accordingly.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
82.	Personnel have been trained to recognize and handle incidents. All users are instructed to report security problems or incidents to their respective SSOs or other appropriate security official.	▪ ED IT Security Controls Reference Guide ▪ ED IT Security Incident Handling Procedures ▪ NIST SP 800-18 ▪ NIST SP 800-26					
83.	Incident handling procedures and control techniques are modified as appropriate after an incident occurs.	▪ NIST SP 800-18 ▪ NIST SP 800-26					
84.	A help desk or group that offers advice is available to provide help to users when a security incident occurs in the system.	▪ ED IT Security Controls Reference Guide ▪ ED Information Security Incident Handling Procedures ▪ NIST SP 800-26					
6.1.6 Information Sharing							
85.	Limit the sharing of information to that which is legally authorized and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information.	▪ ED Handbook for IT Security Policy ▪ ED Information Security Incident Handling Procedures					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
86.	Assure that information, which is shared with federal organizations, state and local governments, and the private sector, is appropriately protected comparable to the protection provided when the information is within the system.	▪ ED Handbook for IT Security Policy ▪ ED Information Security Incident Handling Procedures					
87.	Use of commercial Internet services (e.g., AOL) and online file sharing programs (e.g., Napster) from government-owned networks is in accordance with the Department's policy.	▪ ED Personal Use of Department Equipment Policy					
6.1.7 Personnel Security							
88.	All positions are reviewed for sensitivity level.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
89.	Conditions are established and documented for allowing system access prior to completion of background screening.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM					
90.	Background checks are performed prior to being authorized access to the GSS or MA and periodic reinvestigations are performed at least once every five years, consistent with the sensitivity of the position per criteria from the Office of Personnel Management.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
91.	Personnel, including contractors, who operate SBU information system equipment, are instructed on appropriate security procedures before being granted system access.	▪ ED Handbook for IT Security Policy ▪ FIPS 31					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
92.	System specific user termination and transfer procedures are established and documented, including prompt revocation of user Ids, and return of property keys, ID cards, access badges, etc.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
93.	Employees/contractors are required to take regularly scheduled vacations and have their responsibilities temporary reassigned.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM ▪ OIG Security Program Checklist					
94.	Confidentiality or security agreements are required for employees assigned to work with sensitive information.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
95.	Policies are developed and implemented for hiring, transfer, termination and performance of employees/contractors.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM					
96.	Position descriptions, including system specific position descriptions, are documented and are up-to-date, accurately reflecting assigned duties and responsibilities and segregating duties.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
97.	Segregation of duties exists within the IT function. (Security personnel who administer the access control function do not administer the audit trails and distinct systems support functions are performed by different individuals).	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide					
98.	Individual accountability, least privilege, and separation of duties are enforced by access controls.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ FISCAM					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
6.1.8 Physical Security							
99.	Emergency shutoff controls protect the system against smoke or high temperature air and are easily accessible at points of exit.	▪ ED Handbook for IT Security Policy ▪ FIPS 31 ▪ ED IT Security Controls Reference Guide					
100.	Access to telecommunications hardware or facilities is restricted and monitored.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26 ▪ FISCAM					
101.	The computer room has raised floors.	▪ ED Handbook for IT Security Policy ▪ ED IT Physical Security Policy ▪ FIPS 31 ▪ ED IT Security Controls Reference Guide					
102.	Physical access to data transmission lines are controlled.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
103.	Computer monitors are located to eliminate viewing by unauthorized persons.	▪ ED Handbook for IT Security Policy ▪ ED IT Physical Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					
104.	Emergency exit and re-entry procedures are documented and implemented to ensure that only authorized personnel are allowed to re-enter after fire drills, etc.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
105.	Entry codes to computer rooms and other sensitive areas are changed periodically.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26 ▪ FISCAM					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
106.	Management regularly reviews the documented list of persons with physical access to sensitive areas/facilities.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
107.	Unused keys or other entry devices are secured.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
108.	Key locks or other access devices are implemented to restrict access to the computer room, tape/media library, and other sensitive areas.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM ▪ ED IT Physical Security Policy					
109.	Deposits and withdrawals of tapes and other storage media from the library are authorized and logged.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26 ▪ FISCAM					
110.	Access to facilities is controlled through the use of guards, ID badges, or entry devices such as key cards or biometrics.	▪ ED Handbook for IT Security Policy ▪ FIPS 31 ▪ NIST SP 800-18 ▪ ED IT Physical Security Policy ▪ NIST SP 800-26					
111.	Adequate physical security controls have been implanted that are commensurate with the risks of physical damage or access.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ ED IT Security Controls Reference Guide					
112.	Visitors, contractors and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ ED IT Physical Security Policy ▪ NIST SP 800-26					
113.	Mobile and portable systems are protected and stored securely.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26					
114.	Individuals requiring temporary access to a sensitive area are required to obtain temporary access (e.g., sign-in, visitor badge) and must be escorted by an authorized individual.	▪ ED IT Security Controls Reference Guide					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
115.	The operational areas of computer facilities have been designated, as controlled areas (e.g., computer rooms, communications equipment areas, telephone closets) and access to these areas is permitted only if specifically authorized or required for job performance.	▪ ED Handbook for IT Security Policy ▪ ED IT Physical Security Policy ▪ ED IT Security Controls Reference Guide ▪ OIG Network Media Checklist					
6.1.9 Production Input/Output Controls							
116.	Official electronic records are properly disposed/archived.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
117.	Information or media is purged, overwritten, degaussed, sanitized, or destroyed when disposed or reused.	▪ ED Handbook for IT Security Policy ▪ ED IT Physical Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					
118.	A record is maintained of individuals who implement disposal actions and the sanitization of the information or media is verified.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					
119.	Procedures are documented and implemented to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information and media.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					
120.	Procedures are documented and implemented to ensure that only authorized users can pick up, receive, or deliver input and output information and media.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					
121.	Damaged media is stored and/or destroyed.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
122.	Procedures are documented and implemented for shredding or other destructive measures for hardcopy media when no longer required.	▪ ED Handbook for IT Security Policy ▪ ED IT Physical Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					
123.	Internal/external labeling procedures for appropriate sensitivity (e.g., Privacy Act, Department Sensitive) are established, including special handling instructions.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
124.	Procedures and controls used for transporting or mailing media or printed output are documented and implemented.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
125.	Audit trails are used for receipt of sensitive inputs/outputs and are maintained for inventory management.	▪ NIST SP 800-18 ▪ NIST SP 800-26					
126.	Media used to record and store sensitive software or information is protected, controlled, and secured when not in actual use.	▪ ED IT Security Controls Reference Guide					
6.1.10 Public Access Controls							
127.	If the public accesses the system, appropriate pubic access controls are implemented to promote or permit public access and additional security controls are added to protect the integrity of the application and the confidence of the public.	▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
6.1.11 Security Awareness and Training							
128.	Mandatory annual security awareness refresher training is provided.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26					
129.	Methods are employed to increase employee awareness of security (i.e., posters, booklets).	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
130.	An employee training and development program is established and implemented to ensure employees/contractors obtain necessary skills to perform required job functions.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26 ▪ OIG Security Program Checklist					
131.	Employees/contractors receive a copy of or is provided access to the Department's security policies and procedures.	▪ NIST SP 800-18 ▪ NIST SP 800-26					
132.	Specialized training is provided for all individuals given access to the system.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
7. TECHNICAL CONTROLS							
7.1.1 Auditing							
133.	System auditing is enabled and the logs are consistently reviewed by authorized personnel, at least once a week.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-12 ▪ NIST SP 800-14 ▪ NIST SP 800-18 ▪ NIST SP 800-26					
134.	The system generates audit logs that are stored and are accessible for a specified period of time.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-12					
135.	Access to online audit logs is strictly controlled and restricted to authorized personnel.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-12 ▪ NIST SP 800-18 ▪ NIST SP 800-26					
136.	Audit logs are retained in off-line storage for a period of time. And access to the audit logs is strictly controlled.	▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ OIG Application Control Checklist					
137.	The audit trail can support after-the-fact investigations of how, when, and why normal operations ceased.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
138.	Automated tools are used to review audit records in real time or near real time.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ OIG Application Control Checklist					
139.	Activity involving access to and modification of sensitive or critical files is logged and monitored; possible security violations are investigated.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
140.	Keystroke monitoring is used, and users are notified that it is taking place.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
141.	Audit logs are configured to capture security relevant events.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide					
7.1.2 Identification and Authentication							
142.	An approved list of authorized users and their access is updated and maintained.	▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM ▪ OIG Application Control Checklist					
143.	Procedures for removing expired user accounts are documented and implemented.	▪ NIST SP 800-26 ▪ OIG Application Control Checklist					
144.	Personnel files are matched with user accounts to ensure that terminated or transferred individuals do not retain system access.	▪ NIST SP 800-26 ▪ FISCAM					
145.	Procedures for monitoring and disabling inactive user accounts after a specified period of time (no more than 90 days) are documented and implemented.	▪ FIPS 191 ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM					
146.	Data owners periodically review access authorizations to determine whether they remain appropriate and periodically re-certify users, including for single sign-on computers.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM					
147.	A limit to the numbers of invalid access attempts that may occur for a given user is established.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
148.	Users log out when they leave terminals, workstations, and networked personal computers unattended.	▪ NIST SP 800-18					
149.	A process for requesting, authorizing, establishing, issuing, and closing user accounts is documented and implemented.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM					
150.	If digital signatures are used, they conform to FIPS 186-1.	▪ FIPS 186-1 ▪ NIST SP 800-18 ▪ NIST SP 800-26					
151.	Procedures for determining compliance with password policies are documented and implemented.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ OIG Application Control Checklist					
152.	Users are individually authenticated via passwords, tokens, or other devices.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26 ▪ OIG Logical Access Control Checklist					
153.	Passwords are unique and require alpha numeric, upper/lower case, special characters, and must be a minimum length of 6 characters long.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
154.	Initial passwords, assigned by system administrators, are securely distributed and are required to be changed immediately upon receipt by the user.	▪ FIPS 112 ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18					
155.	All vendor-supplied passwords, including those for software packages, maintenance accounts, and network devices, are changed upon installation.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ OIG Checklist for Network Equipment					
156.	Procedures for handling lost and compromised passwords are documented and implemented.	▪ FIPS 112 ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
157.	Passwords are not displayed when entered.	▪ NIST SP 800-18 ▪ FISCAM ▪ NIST SP 800-26					
158.	Passwords are transmitted and stored using secure protocols/ algorithms.	▪ NIST SP 800-18 ▪ FISCAM ▪ NIST SP 800-26					
159.	Access scripts with embedded passwords are prohibited.	▪ NIST SP 800-18 ▪ NIST SP 800-26					
160.	All vendor-supplied default security parameters are reinitialized to secure settings that meet the Department's standards.						
161.	Access to all accounts issued to the subject employee are revoked or removed within 24 hours of notification (e.g., transfer, termination, retirement, resignation, or reassignment), or immediately, if requested by the PO senior official or CSO.	▪ ED Handbook for IT Security Policy					
162.	Passwords used to authenticate identity are owned only be the individual having that identity.	▪ ED Handbook for IT Security Policy					
	Logical Access Controls						
163.	Management reviews access controls to operating system software and system utilities to determine if controls are operating as intended.	▪ NIST SP 800-18 ▪ OIG System ▪ NIST SP 800-26 Software Controls Checklist					
164.	Management authorizes interconnections to all systems (including systems owned and operated by another program, agency, organization, or contractor) and documents this authorization in an MOU/A. The MOU/A describes how data is shared between interconnected systems.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
165.	A process for requesting, authorizing, establishing, issuing, and closing emergency and temporary access is documented and implemented.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-26 ▪ FISCAM ▪ OIG Logical Access Control Checklists					
166.	Inactive user sessions are terminated after a period of inactivity (30-90 minutes) and password-protected screensavers are activated.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ OIG Application Control Checklist					
167.	Access to security software is restricted to security administrators.	▪ NIST SP 800-26 ▪ FISCAM ▪ OIG Application Control Checklist ▪ OIG Logical Access Control Checklist					
168.	Internal security labels (naming conventions) are used to control access to specific information types or files.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM					
169.	Access is restricted to files at the logical view or field.	▪ NIST SP 800-26 ▪ FISCAM					
170.	Logical access controls restrict users to authorized transactions and functions.	▪ NIST SP 800-26					
171.	Access to tables defining network options, resources, and operator profiles are restricted.	▪ NIST SP 800-26 ▪ FISCAM					
172.	Network connections automatically disconnect at the end of a session.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM					
173.	Firewalls, proxy devices, or security gateways are installed to control access to the internal network.	▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ OIG Checklist for Wireless					
174.	Insecure protocols (e.g., UDP, ftp) are disabled.	▪ NIST SP 800-26					
175.	Logical controls are implemented over network access.	▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
176.	Remote access to the system is restricted.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
177.	Communication software is implemented to restrict access through specific terminals.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-26 ▪ FISCAM ▪ OIG Checklist for Dial Up Lines					
178.	Dial-in access authorizations are documented on standard forms and are maintained on file.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18					
179.	Access control software is used to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-18 ▪ NIST SP 800-26 ▪ FISCAM					
180.	All dial-up access to the system is protected with approved devices or techniques that provide explicit identification and authentication and audit trails; only allowed through the OCIO-operated (or approved) access servers; never through direct modem access.	▪ ED Handbook for IT Security Policy ▪ NIST SP 800-12 ▪ NIST SP 800-18 ▪ NIST SP 800-26					
181.	Penetration testing has been performed on the system.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
182.	Access to all program libraries is restricted and controlled.	▪ NIST SP 800-26 ▪ FISCAM					
183.	The operating system is configured to prevent circumvention of the security software and application controls.	▪ NIST SP 800-26 ▪ FISCAM					
184.	Access is limited to system software and hardware.	▪ NIST SP 800-26					

	Security Requirement	Source	System Compliance			Provided by GSS	Comments
			Yes	No	NA	Yes	
185.	Intrusion detection tools are installed on the system and the intrusion detection reports are generated.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
186.	An approved standardized warning banner is displayed on the system before user login, warning unauthorized users that they have accessed a U.S. Government system and prosecution may arise from unauthorized use.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide ▪ NIST SP 800-18 ▪ NIST SP 800-26					
187.	Firewall policies and procedures, in compliance with the Department's firewall policies, are documented, implemented, reviewed periodically, and updated as necessary.	▪ NIST SP 800-26 ▪ FISCAM					
188.	Vulnerability scanners are used to identify weaknesses, which could lead to security violations and could uncover possible breaches.	▪ ED Handbook for IT Security Policy ▪ ED IT Security Controls Reference Guide					
189.	Telephone numbers for dial-up communications are controlled, only provided to authorized users and not publicly listed, and are accounted for by the OCIO.	▪ ED Handbook for IT Security Policy					

APPENDIX E. VULNERABILITY QUESTIONNAIRE

Security Management			
No.	Question	Answer	Comments
	Who is the head of IT security?		
	Who is the head of physical security?		
	Is management aware of or informed about vital security issues?		
	Has a cost-benefit analysis been performed on the facility?		
	Is there a security policy & plan in place?		
	Are there proactive measures for security updates in place?		
	What type of security training is being administered?		
	Are security incidents properly reported and analyzed?		
	What would be the consequences of system compromise?		
	Are security measures in place to detect misuse of connectivity privileges and/or devices?		
	Are procedures subject to periodic review?		
	Is there a system in place for monitoring use of the facility?		
	Are inventories taken of connectivity components and applications?		
	How is critical data flow regulated (including dissemination, transmission, and receipt)?		
	How are non-regular staff regulated (contractors, visitors, etc.)?		
Policies and Procedures			
No.	Question	Answer	Comments
	Is there an overriding security policy that has been distributed to all personnel covering important vital aspects of operations in place?		
	Are personnel required to acknowledge acceptance of this policy (and its terms) in writing?		
	Do the terms include consequences for possible violations?		
	Are various forms of media covered and protected under existing policies and procedures?		
	Are work areas monitored? If so, how?		
	Does the disaster recovery plan cover the protection of critical system components?		
Risk Assessments			
No.	Question	Answer	Comments
	When was the last risk assessment performed?		
	How often are the assessments performed?		
	Who administers them?		
	What vulnerabilities were assessed?		
	How is the copying of files controlled?		
	Are audit traits recorded?		

Personnel Security			
No.	Question	Answer	Comments
	Are employees asked to sign a confidentiality agreement that stipulates what types of data require extra vigilance, and the consequences of not following policies?		
	Are personnel background checks routinely performed?		
	Are role-based authorization and separation of duties enforced?		
	Are violations dealt with quickly?		
	Is electronic access properly regulated?		
Computer Security			
No.	Question	Answer	Comments
	Is there a formal computer security training program in place for security personnel? If so, is management involved?		
	Are users educated in proper methods for the disposal of external storage media?		
	Is system use a subject of the training program?		
Disaster Recovery			
No.	Question	Answer	Comments
	Who is the Disaster Recovery Manager (DRM)?		
	Has there been an unscheduled shutdown of the facility? How long?		
	Are severe weather or other environmental conditions a factor in the area?		
	Is there an existing disaster recovery plan?		
	What was the date of the last disaster recovery (DR) test?		
Physical Security			
No.	Question	Answer	Comments
	What is the layout of the building?		
	What are the construction materials used?		
	Are emergency exits alarmed?		
	Are emergency drills practiced? If so, how often?		
	Are emergency contact numbers on file?		
	Is entry to the area controlled?		
	Are visitors escorted while in the building?		

APPENDIX F. SYSTEM DISPOSAL CHECKLIST

Name of System

System Disposal Checklist					
No.	**Requirement**	**Compliance**			**Comments**
		Yes	**No**	**N/A**	
1.	All information has been moved to another system, archived, discarded, or destroyed.				
2.	Legal requirements for records retention were considered before disposing of the system.				
3.	All information is cleared and purged from the system.				
4.	All information has been removed from storage medium (e.g., hard disk or tape).				
5.	Appropriate steps have been taken to ensure the level of sanitization is appropriate for the type of storage medium (e.g., overwriting, degaussing (for magnetic media only), and destruction).				
6.	All hardcopy media has been destroyed (e.g., shredded, burned, etc.).				
7.	Appropriate steps have been taken to ensure that all contractors implement sanitization policies and procedures for removing information processed or residing on a contractor's site.				
8.	Leased equipment for processing information has been sanitized before returned to the vendor.				
9.	When data has been removed from storage media, every precaution has been taken to remove duplicate versions that may exist on the same or other storage media, back-up files, temporary files, hidden files, or extended memory.				

_____

System Owner Printed Name

_____ _____

System Owner Signature Date

APPENDIX G. RISK ASSESSMENT REPORT FORMAT

EXECUTIVE SUMMARY

Provide a high level summary of the risk assessment methodology and findings, suitable for a senior executive audience. Briefly describe the system characterization, data gathering techniques and ratings definitions. List the total number of high, medium, and low risks that were discovered.

INTRODUCTION

Include the following sections: purpose, background, scope, and structure.

Purpose

Explain the purpose of conducting a risk assessment for the GSS or MA (e.g., to comply with OMB Circular A-130 requirements). Include the date of the most recent risk assessment. Reserve detail for scope statement below.

Background

Provide an overview of the system's characterization and current SDLC phase. Include a brief description of the risk assessment team and the analysis process.

Scope

Describe the elements of the network, architecture, system components, field site locations (if any), and any other details about the system considered in the analysis. References to appropriate diagrams included in the appendices must be inserted here, as they will assist others in understanding the scope of the project.

Structure

Describe the organization structure of the document.

RISK ASSESSMENT APPROACH

Define system boundaries, describe information gathering techniques, and outline steps taken to complete the risk assessment. Include ratings, definitions, and the risk-rating matrix used.

SYSTEM CHARACTERIZATION

Provide the fullest description of the System Characterization, identifying system resources and information that constitute the system and its boundaries. The characterization must provide a system overview and describe its interfaces, users, and data content, mission criticality and information sensitivity. This will provide the foundation for the remaining steps in the risk analysis process. Use the system characterization statement to give readers a detailed view of the hardware, software, and setup examined.

THREAT STATEMENT

Identify and explain the existing threats to the GSS or MA, both sources and agents, that are later considered when developing the threat and vulnerability pairs in the Findings section.

FINDINGS

Include a separate discussion for each threat and vulnerability pair resulting from an analysis of the Threat Statement and Vulnerability List. A threat and vulnerability pair discussion must include the identification of existing mitigating security controls, impact analysis discussion, risk rating, and recommended remediation measures

APPENDICES

Include a few descriptive sections such as: system diagram, anticipated major changes/upgrades, glossary of terms, list of references, and a list of acronyms and abbreviations. The diagram is particularly important, as it will provide staff and administration with an overall view of the architecture employed by the system, as well as the individual components mentioned in the report. Additionally, a list of key staff members with individual contact information, including phone, fax, and e-mail is helpful. Also include the BLSRs that were used for the assessment.

APPENDIX H. RISK ASSESSMENT SECURITY ACTION PLAN LETTER TEMPLATES

SAMPLE MEMORANDUM FROM THE PRINCIPAL OFFICER

Date:

To: William J. Leidinger
Chief Information Officer

From: [PRINCIPAL OFFICER NAME]
Principal Officer for [PO NAME]

Subject: Submission of [PO NAME]'s Risk Assessment for [Name of General Support System or Major Application]

As the Principal Officer for [PO NAME], I hereby acknowledge that (Name of GSS or MA) has undergone a comprehensive Risk Assessment– consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, the Clinger-Cohen Act[19], the Federal Information Security Management Act (FISMA), the Computer Security Act of 1987[20], the procedures guidelines provided by the National Institute of Standards and Technology (NIST), the Department of Education Information Technology Risk Assessment Procedures, and all other applicable Federal and Departmental guidance. This risk assessment is attached.

INCLUDE ONLY THE APPROPRIATE PORTIONS OF THE PARAGRAPHS BELOW
Whatever one matches your response

I concur with the findings of the attached assessment, both in the listing of risks and their respective ratings of high, medium or low. I have attached a remediation measure chart that includes assigned due dates and estimated costs for a remediation measure for each identified risk.

OR

I do not concur with all of the findings of the attached assessment. I have specified which findings and/or risk ratings with which I disagree in a separate attachment. I have attached a remediation measure chart that includes assigned due dates and estimated costs for a remediation measure for each identified risk.

ALL MEMOS MUST INCLUDE THE FOLLOWING CONTACT INFORMATION

19 *Public Law 104-106*
20 *Public Law 100-235*

My point of contact for this Risk Assessment is [PO Computer Security Officer] at 202-[XXX-XXXX].

Attachments:

Risk Assessment
Remediation Measure Chart
Non-Concurrence Chart (if applicable)

Remediation Measure Chart for the [Name of General Support System or Major Application] Risk Assessment for **[PO NAME]**

Identified Risk (include Observation # from assessment report)	Rating	Remediation Measure	Due Date	Estimated Cost
EXAMPLE M1: A comprehensive contingency plan has not been developed.	Medium	A disaster recovery plan will be developed for the system.	07/31/2002	$4,000
EXAMPLE O1: There are no sign-in logs for visitors accessing the computer room.	Low	None – we are mitigating this risk with audit logs on the servers and the use of access cards for entry. We do not believe that sign-in logs will be maintained		
EXAMPLE T1: Remote registry access is not restricted to administrators	High	Adjust registry setting to restrict remote access to administrators	06/15/2002	$0 – existing staff will make the correction

Non-Concurrence Chart for the [Name of General Support System or Major Application] Risk Assessment for **[PO NAME]**

Identified Risk (include observation # from assessment report)	Rating	Non-Concurrence	Rationale
EXAMPLE T1: The accounts of users who no longer require access may not be deleted immediately from the system.	Medium	This is not accurate.	The system administrators are responsible for deleting accounts within 24 hours. A weekly status report is prepared on these accounts
EXAMPLE T2: Passwords on the server are not required to be changed every 90 days.	Medium	The risk level is Low, not medium, for this risk.	Passwords are changed every 120 days which is adequate when combined with the Audit Logs and additional passwords required for the system itself.

SAMPLE MEMORANDUM FROM THE CHIEF INFORMATION OFFICER

Date:

To: [PRINCIPAL OFFICER NAME]
Principal Officer for [PO NAME]

From: William J. Leidinger
Chief Information Officer

Subject: Endorsement of [PO NAME]'s Risk Assessment for [Name of General Support System or Major Application]

As the Chief Information Officer for the Department of Education, I hereby acknowledge that (Name of GSS or MA) has undergone a comprehensive risk assessment– consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, the Clinger-Cohen Act[21], the Federal Information Security Management Act (FISMA), the Computer Security Act of 1987[22], the procedures guidelines provided by the National Institute of Standards and Technology (NIST), the Department of Education Information Technology Risk Assessment Procedures, and all other applicable Federal and Departmental guidance. This risk assessment was completed [date of submission] for the [PO Name].

I also acknowledge that appropriate remediation measures have been proposed which adequately address all of the risks identified in this risk assessment.

If you have any questions regarding these matters, my point of contact for this task is Jennifer Beale on 202-401-2195 or via e-mail.

21 *Public Law 104-106*
22 *Public Law 100-235*