ADMINISTRATIVE COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL DIRECTIVE

Handbook OCIO-09 **Cover Page for 49 Pages (03/16/2005)**

Distribution:
All Department of Education Employees

Approved by: for Michell Clark
William J. Leidinger
Assistant Secretary for Management

Handbook for General Support Systems And Major Applications Inventory Procedures

---

For technical questions concerning information found in this ACS document, please contact Jennifer Beale on (202) 245-6415 or via e-mail.

Supersedes OCIO-09, Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures dated 05/21/2003.

Office of the Chief Information Officer

Handbook for General Support Systems and Major Applications Inventory Procedures

Version 2.0
March 2005

Document Configuration Control

Version	Release Date	Summary of Changes
Version 1.0	September 1, 2004	Initial Release
Version 2.0	January, 2005	Changes made to ensure compliance with changes in Federal laws and Standards.

Table of Contents

1. Overview

1.1. Purpose

The purpose of this document is twofold. First, the document describes the process that will be used by the Department of Education (Department) to establish and maintain an inventory of general support systems (GSS's) and major applications (MAs). Second, the document provides guidance to the Principal Offices (POs) regarding the standards to be employed throughout this process.

GSS's and MAs are defined in Office of Management and Budget (OMB) Circular A-130 *Management of Federal Information Resources* as follows:

- GSS is "an interconnected set of information resources under the same direct management control which shares common (functionality),"
- MA is "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."

This process enables the Department's GSS and MA inventory to officially identify and document the security classifications of GSS's and MAs in use by the Department, in compliance with Federal requirements and guidance including FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Volumes I and II. This document establishes guidelines for the classification of data and information types with respect to its confidentiality, integrity and availability. By determining the sensitivities of the information, the Department will be able to apply those classifications to the overall categorization of the information systems that process or store the information.

This GSS and MA inventory is intended to complement existing Departmental security initiatives, such as those under the Federal Information Security Management Act (FISMA) Public Law 107-296 and Critical Infrastructure Protection (CIP) Presidential Decision Directive (PDD) 63 mandates.

1.1.1. Objectives & Goals

The primary objective in developing a systematic approach for the inventory and classification of the GSS's and MAs in the Department is to ensure that automated information resources, which "include both government information and information technology,"[1] have adequate security to protect "information collected, processed, transmitted, stored, or disseminated by the Department."[2] Without an accurate assessment of what constitutes the Department's GSS's and MAs, it is impossible to ensure that all automated information resources implement the appropriate level of protection.

While all automated information resources require a level of security, some require additional security controls due to the sensitivity of the information processed or criticality to the Department's missions. Successful completion of this GSS and MA inventory process will identify the GSS's and MAs that require additional security controls. This follows the tenet that applications that do not qualify for inclusion in this GSS and MA inventory rely on the GSS's in which they operate for the provision of adequate security. Thus, the applications are not required to undergo the certification and accreditation (C&A) process. It is therefore incumbent to accurately complete this GSS and MA inventory process to ensure that adequate security is applied to the entirety of the Department's automated information resources. The specific security requirements for the GSS's and MAs included in the inventory can be found in the Department's C&A related guidance.

[1] *OMB Circular A-130.*

[2] *OMB CircularA-130, Appendix III.*

1.1.2. Audience

This document is intended for the following Department of Education personnel:

- **Principal Officers** – In their capacity as the senior officials responsible for providing security for the information collected, processed, transmitted, stored, or disseminated by GSS's and MAs under their control[3]
- **Computer Security Officers (CSOs)** – In their capacity for maintaining the information security program within their respective POs
- **System Owners** – In their capacity to provide security controls appropriate for the protection of Department information
- **The Chief Information Officer (CIO)** – In his/her capacity as the official responsible for providing guidance on information security throughout the Department.

1.1.3. Assumptions

The Department made the following assumptions when creating this guidance:

- Data sensitivity levels are determined using Government-wide recommendations from FIPS 199 and NIST SP 800-60
- High availability is based on the assumption that the two Mission Essential functions for the Continuity of Operations Plan (COOP) (Title IV of the Higher Education Act (HEA) and Project SERV - School Emergency Response to Violence) are important at the U.S. Government level as well
- Information that is not covered by the Privacy Act and not considered sensitive is still labeled low.

1.1.4. Document Structure

This document is organized into five sections and five appendices, as shown below:

Section 1 – Overview

Section 2 – Methodology

Section 3 – Changes to the Inventory Between Cycles

Section 4 – Acronyms

Section 5 – Definitions

Section 6 – References

Appendix A – The GSS and MA Inventory Submission Form

Appendix B – A sample completed GSS and MA Inventory Submission Form.

Appendix C – Sample memoranda for PO and CIO validation of the GSS and MA inventory.

Appendix D – Additional guidance related to the classification of information.

Appendix E – Department of Education lines of business and information types

[3] *Federal Information Security Management Act, Public Law 107-347*

2. Methodology for Determination of GSS and MA Inventory

The following subsections provide detailed information on the five steps necessary for the Department to create and maintain its GSS and MA inventory:

Step 1: Identify GSS's and Applications

The Principal Office staff determines the business functions that are automated and identify the automated information resources that support them

a) Identify Business Functions
b) Identify Automated Information Resources
c) Categorize Automated Information Resources as GSS or Applications

Use the automated information resource definition (Section 2.1.2.2) and existing GSS and MA inventory to determine if it qualifies as a single automated information resource, can be integrated into an existing GSS or application, or qualifies as a similar system to another GSS or application.

Step 2: Classify GSS's and Applications

Principal Office staff ascertain the security needs of each based upon additional considerations

Step 3: Identify MAs

Principal Office staff use security classifications to determine if an application qualifies as an MA. MAs are applications that require special security considerations due to the nature of the information stored, processed or transmitted. (Only applications determined to be MAs will be included in the GSS and MA inventory; see Section 2.3)

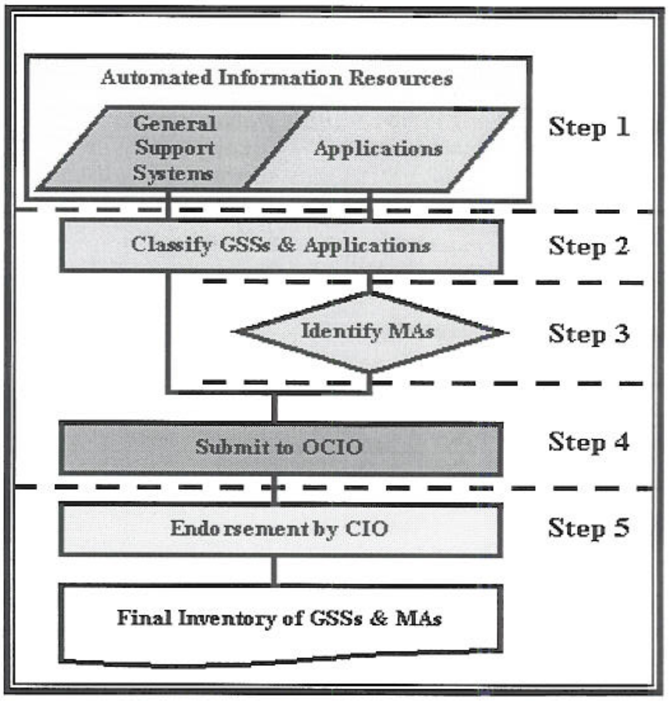

Figure 2-1: GSS and MA Inventory Process

Step 4: Submit to CIO

Principal Officers validate and acknowledge the GSS and MA inventory as accurate

Step 5: Endorsement by CIO

Generate the official GSS and MA Inventory for the Department.

Upon completion of steps 1, 2, and 3 for a particular GSS or MA, the results of their inventory categorization assessment must be documented in the Department's formal inventory (provided in Appendix A). All GSS's and MAs from a PO must be included under one memorandum that is validated by the Principal Officer and sent to the CIO. The CIO upon approval will provide a memorandum endorsing (and finalizing) the inventory submission. (Sample memoranda are provided in Appendix C.) If there is a need for clarification at any point during the GSS and MA inventory process, CSO's should consult with the Office of the Chief Information Officer (OCIO) to ensure compliance with the applicable requirements. This process is illustrated in Figure 2-1.

To retain a current and comprehensive list of the GSS's and MAs, the inventory process will be undertaken semi-annually, with final validation of the GSS and MA inventory to occur on January 31 and July 31. During each cycle, POs will need to validate the inventory on record or update information on the GSS's and MAs in their PO. CIO receipt of PO validation of the GSS and MA inventory will be required no less than 2 weeks prior to the final validation date.

2.1 Step 1: Identify General Support Systems and Applications

2.1.1 Step 1A: Identify Business Functions

The first step in creating and maintaining an inventory of GSS's and MAs is to identify all automated information resources used by the PO to perform its business functions. All automated information resources in the PO are either a GSS or an application. (See Section 2.1.3)

To begin, identify the business functions (the work the PO performs in support of the Department's mission, vision, and goals) that occur within the PO. This may include such functions as grants management, provision of public information, or human resources management. These functions should then be divided into the specific activities that support the overall business function.

2.1.2 Step 1B: Identify Automated Information Resources

Each business function identified may have certain associated automated processes. Once these automated processes have been identified, the automated information resources that support these processes must be identified. For each automated information resource identified, including databases, stand-alone systems, communications systems, networks, and any other type of information technology-related support, a description should be created. Automated information resources that utilize general-purpose software such as spreadsheets and word processing software are not included as candidates because their security is provided by the GSS on which they reside.[4] All other automated information resources are included as candidates for the GSS and MA inventory.

Note: It is possible to have several automated information resources to support a single business function. It is also possible to have a single automated information resource support several business functions.

2.1.2.1 Shared Resources & System Interconnectivity

Do automated information resources not owned by the Department support any business function?

OMB Circular A-130 delineates the need for agencies to ensure "information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information," regardless of its location or the owner of the automated information resource.

Therefore, all automated information resources that support automated processes must be identified, including those that are owned, in whole or in part, by a party other than the Department. All automated information resources that collect, process, transmit, store, or disseminate Department information must be identified, regardless of ownership. For example, if a payroll system is operated by another Federal agency but part of the system is loaded on the Department's computers to perform a business function, the Department is responsible for ensuring appropriate security controls are in place for that automated information resource.

Consideration must also be given to all automated information resources operated by contractors in support of Department work. OMB Circular A-130 states that information technology (and, thereby, automated information resources) includes those resources "used by a contractor under a contract with the executive agency which (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product."

[4] *NIST SP 800-18, Procedures for Developing Security Plans for Information Technology Systems*

Note: If another agency runs a system that processes Department information, an interagency agreement must be put in place to officially verify terms of agreement for the protection of information between the agencies as well as to ensure that adequate security measures are instituted to protect the information.[5]

2.1.2.2 Automated Information Resource Boundaries

An automated information resource is defined by constructing a logical boundary around a set of processes, communications, storage, and related resources. The elements within this boundary constitute a single automated information resource and must:

- Be under the same direct management control
- Have the same function or mission objective
- Have essentially the same operating characteristics and security needs, and
- Reside in the same general operating environment.[6]

Note: In some instances, the automated information resource identified is similar to another automated information resource except for the responsible organization or the physical environment in which they are located. In this case, it is appropriate and recommended to develop similar documentation except for those areas of difference. This approach provides consistent levels of protection for similar systems.

2.1.2.3 Additional Considerations in Identifying Automated Information Resources

The following additional items are guidance to be considered during the process of defining the automated information resources.

2.1.2.3.1 Manual Processes

The process described in this document is designed to identify and inventory the automated information resources that support automated processes. As such, manual processes or locations that support specific business functions, such as libraries and record archives, should be excluded.

2.1.2.3.2 Lifecycle Considerations

Providing security is an ongoing process, conducted throughout the lifecycle. Ideally security is incorporated into the development of an automated information resource. As noted in OMB Circular A-130, Appendix III, "for security to be most effective, the controls must be part of day-to-day operations. This is best accomplished by planning for security not as a separate activity, but as an integral part of overall planning."

Are there any automated information resources under development to support business functions?

Additionally FISMA, citing the Clinger-Cohen Act and the Computer Security Act of 1987, directs the heads of agencies to "incorporate information security principles and practices throughout the lifecycles of the agency's information systems." Therefore, any automated information resource under development, at any stage, must be included in the list of candidates identified in this step. Automated information resources must be considered as they are planned to operate when fully functional, not necessarily how they currently operate. Security must be planned for the data that will be processed, whether or not that data is yet processed by the automated information resource. It is understood that these classifications may change throughout the life of the automated information resource, but it is important to have accurate

[5] *NIST SP 800-18, Procedures for Developing Security Plans for Information Technology Systems*

[6] *NIST SP 800-18, Procedures for Developing Security Plans for Information Technology Systems*

classifications at each stage of the life cycle, so that appropriate security controls will applied. As the need for changes to the data classifications arise, the inventory must be updated to accurately reflect the current state of the data sensitivity or mission criticality. (See Section 3.0)

Similarly, an automated information resource may not be excluded from the list of candidates if it is only scheduled for retirement. Only when the automated information resource has been completely disconnected or shut down, information requiring protection is properly removed from the automated information resource, and the CIO has received official confirmation of such action, may the automated information resource be removed from the inventory. This must include completion of the System Disposal Checklist, which is included as an appendix of the *IT Security Risk Assessment Procedures*.

The consideration of automated information resources in all stages of the system development life cycle (SDLC) is in direct correlation with the Department's *IT Security Risk Assessment Procedures*, which provides specific guidelines for ensuring appropriate security for systems in all phases of the SDLC.

2.1.2.3.3 Information Technology Capital Planning

Consistent with Section 2.1.2.3.2, Lifecycle Considerations, all automated information resources that receive consideration during the information technology capital planning process must also be included among the list of candidates for the GSS and MA inventory, even if they are only in a developmental state.

If the automated information resource does not receive funding during the process, the inventory may be updated to reflect this decision. (See Section 3.0)

2.1.3 Step 1C: Categorize Automated Information Resources as GSS or Application

Each automated information resource identified in Section 2.1.2 must be reviewed to determine its status as a GSS or application. **Each automated information resource will be either a GSS or an application.** This status will be determined by applying the following definitions.

Is the automated information resource a local or wide-area network?

Does the automated information resource support multiple other automated information resources?

2.1.3.1 General Support System

A GSS is "an interconnected set of information resources under the same direct management control which 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 support a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO)."[7]

2.1.3.2 Application

An application is "the use of information resources to satisfy a specific set of user requirements."[8]

Some automated information resources may be identified as both a General Support System and an application, as in the case where a database is run from a stand-alone computer.

Automated information resources determined not to be GSS's are applications. Identification of an application as an MA is based upon the classifications in Section

[7] *OMB Circular A-130, Appendix III*

[8] *OMB Circular A-130, Appendix III*

2.2 and is fully explained in Section 2.3. **Only applications identified as MAs will be included in the final GSS and MA inventory.** Those determined not to be MAs are not required to undergo C&A as they rely on the GSS they reside on to provide adequate security.

2.2 Step 2: Classify GSS and Applications

To support the development and maintenance of appropriate security controls for GSS's and MAs on the inventory, it is necessary to identify security classifications for each and the information it handles. This section will describe and define several sets of security classifications to be applied to the identified GSS's and applications to appropriately evaluate the level of security required for each.

All automated information resources identified in Section 2.1.3 must be evaluated using the criteria contained in this section. If, in Section 2.1.3, the automated information resource is determined to be a **GSS**, it will be included in the GSS and MA inventory and requires the classifications outlined in the following sections.

If, in Section 2.1.3, the automated information resource is determined to be an application, the classifications outlined in the following sections must be used to determine if it qualifies as an MA (see Section 2.3). **Only applications determined to be MAs will be included in the final GSS and MA inventory.**

2.2.1 Methodology for Determining Impact Levels

The owner of each GSS or application, or an individual designated by the owner, should use the following methodology to categorize each GSS or application. The following steps provide guidance to determine the impact levels recommended for the confidentiality, integrity and availability of the data stored, processed or transmitted by each GSS or application. When determining impact, the evaluator should remember that FIPS 199 applies the level definitions of ***potential impact*** on organizations or individuals ***should there be a breach of security*** within the context of each organization and the overall national interest.

The following steps should be followed to appropriately determine the system categorization of the application or GSS:

1. Identify information types
2. Select provisional impact levels
3. Review provisional impact levels
4. Adjust/finalize information impact levels
5. Assign system security category

2.2.1.1 Identify Information Types

The following methodology must be used to identify the information types processed, stored, etc. by each automated information resource. To appropriately categorize the impact levels of the GSS or application, NIST SP 800-60 describe a process, including mapping the GSS or application to the information type in the Department's enterprise architecture that it supports, processes, or generates.

To complete this process, the system owner or designee must reference the Department's enterprise architecture, which includes 7 lines of business that are supported by 16 information types, to determine which line of business and information type are supported by the GSS or application that are being evaluated. The Department's Enterprise Architecture Line of Business Glossary provides a high-level description of the activities under each line of business and is available on the Enterprise Architecture website at http://connected1.ed.gov/po/ea/currarch.html#brm.

For each automated business function, identify the single line of business that best describes the purpose of the system in functional terms. The Department has identified the following 7 lines of business in its enterprise architecture:

- Grants
- Evaluation
- Research and Statistics
- Information Dissemination
- Compliance
- Administration
- Loans

Once the automated information resource has been aligned with a single Department line of business, next identify the associated business function from the Department's enterprise architecture. Following the process outlined in NIST SP 800-60, the Department is equating these business functions as the Department's basic information types. There are currently 16 business functions (information types) associated with the 7 lines of business:

- Grants
  - Discretionary Grants
  - Formula Grants
- Evaluation
  - Evaluation
- Research and Statistics
  - Education Research
  - Program Research
  - Collect and Analyze Statistics
- Information Dissemination
  - Information Dissemination
- Compliance
  - Compliance
- Administration
  - Acquire Goods and Services
  - Provide Legal Services
  - Manage Facilities and Travel
  - Manage Human Resources
  - Manage Financial Resources
  - Manage Information Resources
  - Develop Strategic Plan
- Loans
  - Federal Student Aid

2.2.1.2 Select Preliminary Impact Levels

Assign preliminary impact levels for confidentiality, integrity and availability to each identified information type. The Department's guidance based on FIPS 199 and NIST SP 800-60 criteria should be employed to determine provisional impact levels for confidentiality, integrity and availability of the information processed, stored, etc. by the automated information resource. Specific guidance for determining preliminary and final security impact levels may be found in Section 2.2.2.

Note: When determining the impact level, if confidentiality, integrity or availability is compromised, do not minimize the impact based on mechanisms that have been put in place to protect the system, such as backups. In general, the impact assessment is independent of mechanisms employed to mitigate the consequences of a compromise.[9]

2.2.1.3 Review Preliminary Impact Levels

Review the appropriateness of the preliminary impact levels recommended for the information types in the context of the whole organization environment, mission, use, and connectivity associated with the automated information resource under review.

2.2.1.4 Adjust/ Finalize Information Impact Levels

Based on the results of the review, adjustments should be made to the preliminary impact levels, as appropriate.

2.2.1.5 Assign System Security Category

Establish the level of confidentiality impact, integrity impact, and availability impact associated with the GSS or application under review. The adjusted impact levels for information types are reviewed with respect to the aggregate of all information processed in or by each system. In some cases, the consequences of loss of confidentiality, integrity, or availability of the aggregated information can be more serious than that for any single information type. In addition, a system's access control information and the system software that protects and invokes it can both affect the integrity and availability attributes of a system and even access to other systems to which the system under review is connected.

2.2.2 Information Sensitivity

To appropriately protect information, its relationship to, and impact on, the mission of the Department must be understood. Therefore, it is necessary to know the requirements of the data to be protected from specific risks to apply appropriate security controls.

2.2.2.1 Information Sensitivity Overview

FISMA and FIPS 199 use three security objectives to determine the information sensitivity - confidentiality, integrity (which, for the purposes of this guide, includes non-repudiation and authenticity), and availability.

- Confidentiality – Protection from unauthorized disclosure
- Integrity – Protection from unauthorized, unanticipated, or unintentional modification
    - Non-repudiation – Verification of the origin or receipt of a message

[9] *NIST 800-60 Volume I, Pg. 11*

  - Authenticity – Verification that the content of a message has not changed in transit
- Availability – Protection from the disruption of access to or use of information or an information system.

2.2.2.2 System Impact Overview

FIPS 199 categorizes impact into low, moderate or high levels. The Department evaluated the requirements in FIPS 199 and, as recommended by NIST, customized the requirements to the Department's environment. This section describes how the categorizations FIPS 199 are defined and how the Department is applying those definitions to adapt to its environment at a high level. The sections that follow explain special considerations that should be applied for each unique type of information sensitivity status - confidentiality, integrity and availability.

2.2.2.3 Low Impact

The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

FIPS 199 Definition
A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- Result in minor damage to organizational assets; or
- Result in minor financial loss.

Department of Education Application of FIPS 199
A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability would:

- Not affect essential functions required for Principal Office business continuity plans (BCP's) or the Department's COOP to a point that they could not be completed. The two essential COOP functions are the SERV program and Title IV;
- Not damage public confidence to such a severe degree that the Department would not be trusted to complete these functions; or
- Not cause a financial impact of more than $3 million over 3 years

2.2.2.4 Moderate Impact

The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

FIPS 199 Definition
A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- Result in significant damage to organizational assets; or

- Result in significant financial loss.

> ***Department of Education Application of FIPS 199***
> A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Affect essential functions required for Principal Office BCP's to a point that they could not be completed but would not affect the Department's COOP;
- Damage public confidence to such a severe degree that the Department would not be trusted to completed these functions; or
- Result in a financial impact between $3 million over 3 years and a total impact of $1 billion

2.2.2.5 High Impact

The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

> ***FIPS 199 Definition***
> A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
- Result in major damage to organizational assets; or
- Result in major financial loss

> ***Department of Education Application of FIPS 199***
> A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Result in death;
- Affect essential functions required for the Department's COOP to a point that they could not be completed;
- Damage public confidence to such a severe degree that the Department would not be trusted to complete these functions; or
- Result in a financial impact over $1 billion dollars

The following sections provide more specific detail to determine the overall impact relative to each type of information sensitivity status - confidentiality, integrity and availability.

2.2.2.6 Confidentiality Special Considerations

To determine the appropriate level of confidentiality, an application or GSS must take into consideration the need for its information to be protected from unauthorized disclosure. The level of confidentiality depends on the nature of the information. For example, information that is widely available to the public has a low level of confidentiality because it requires only minimal, or perhaps no, protection from disclosure. However, there are certain types of information that must be protected from disclosure due to the expectation or assurance of privacy, or because unauthorized disclosure could result in a loss to the Department.

Table 2-1. Confidentiality Special Considerations

Level	Description
Low	The system contains data that has no expectation of privacy or Privacy Act data that is not likely to cause identify theft, for instance, only an individual's name and home address. Refer to Appendix D.[10]
Moderate	The system contains Privacy Act information that could be used for identity theft such as social security numbers, PIN numbers, and Tax ID numbers. In addition, information types labeled moderate in NIST SP 800-60 Volume 2 including income information (other than government employee income information), personal identity and authentication, entitlement event information, and representative payee information).[11]
High	Any information that could result in death or major financial loss (over $1 billion).

Common Confidentiality Factors:

Using the FIPS 199 impact criteria, each information type should be evaluated with respect to the low/ moderate/ high impact associated with the answers to the following questions:

- How can a malicious adversary use the information to do limited/ serious/ severe harm to agency operations, agency assets, or individuals?
- How can a malicious adversary use the information to gain control of agency assets that might result in unauthorized modification of information, destruction of information, or denial of system services that would result in limited/ serious/ severe harm to agency operations, agency assets, or individuals?
- Would unauthorized disclosure/ dissemination of elements of the information type violate laws, executive orders, or agency regulations?
- Each use of the information type and each known variant of the information belonging to the type should be considered in determining the confidentiality impact level.

If an application or GSS has information covered under the Privacy Act, the System Owner, or designee, must contact the Department's Privacy Officer to ensure compliance through the completion of a Privacy Impact Assessment.

See Appendix D for more information on confidentiality special considerations.

Example Confidentiality Considerations:

High: The application or GSS contains information, which, if disclosed to unauthorized sources, could result in death or a financial impact over $1 billion. This level indicates that security requirements for assuring confidentiality are of high importance.

Moderate: The application or GSS contains information that could moderately impact the Department if disclosed. The GSS or application contains Privacy Act information that could be used for identity theft such as social security numbers, PIN numbers, and Tax ID numbers.

The application is used for large acquisitions in a contracting organization and contains both sensitive, pre-solicitation phase contract information and routine administration information. The unauthorized disclosure of information could result in a financial impact between $3 million over 3 years or a total impact of $1 billion. This level indicates that security requirements for assuring confidentiality are of moderate importance.

[10] *The unauthorized disclosure of information could be expected to have a* ***limited*** *adverse effect on organizational operations, organizational assets, or individuals (FIPS199, Table 1, pg 6)*

[11] *The unauthorized disclosure of information could be expected to have a* ***serious*** *adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)*

Low: The GSS or application contains general information that is widely available to the public and, if disclosed, would not have an impact on the Department. None of the information on the application or GSS requires protection against disclosure. The impact on the Department's assets and resources could be minor, resulting in less than $3 million over 3 years in damages and would not affect the public confidence of the Department to complete this business function. This level indicates that security requirements for assuring confidentiality are of low importance.

2.2.2.7 Integrity Special Considerations

To determine the appropriate level for integrity, consider the needs of the information to be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to, consideration of authenticity, non-repudiation, and accountability (requirements can be traced to the originating entity). For example, the nature of the loan information processed by the Department may cause it to be targeted for unauthorized modification. Records retention requirements should also be considered, when applicable.

The use of the GSS or application is employed in the business process must be included in this decision. For example, if the data in the GSS or application is not the sole source of input into the business process and the normal course of business is to check data provided electronically against the original source, the need for data integrity would generally be lower than if the data is fully relied upon to complete the business function. However, merely having a backup source of data does not fit this criteria; the data check must exist as a regular step of the business process.

Table 2-2. Integrity Special Considerations

Level	Description
Low	Information processed by the system is part of an overall project and is not the final version that is disseminated or processed. The issuance of improper information could be detected elsewhere and would not damage public confidence to such a severe degree that the Department would not be trusted to complete this business function or result in a financial impact over $3 million over 3 years.[12]
Moderate	Any information processed that a financial action is based on and disseminated to other organizations or to the public that will not be detected elsewhere in the business process, which could cause a financial impact over $3 million in 3 years but less than a total impact of $1 billion or cause Principal Office BCP essential functions to cease.[13]
High	Any information that could result in death or major financial loss (over $1 billion).

Common Integrity Factors:

Using the FIPS 199 impact criteria, each information type should be evaluated with respect to the low/ moderate/ high impact associated with unauthorized modification or destruction of 1) each known variant of the information belonging to the type and 2) each use of the information by the system under review. Unauthorized modification or destruction of information can take many forms. The changes can be subtle and hard to detect, or they can occur in a more obvious manner. One can construct an extraordinarily wide range of scenarios for modification of information and its likely consequences.

Each information type should be evaluated with respect to the low/ moderate/ high impact associated with the answers to the questions below.

[12] *The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)*

[13] *The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)*

How can unauthorized modification or destruction of information:

- Reduce public confidence in an agency,
- Fraudulently achieve financial gain,
- Influence personnel decisions,
- Interfere with or to manipulate law enforcement or legal processes,
- Influence legislation, and
- Achieve unauthorized access to government information or facilities.

In most cases, the most serious impacts of integrity compromise occur when some action is taken that is based on the modified information or the modified information is disseminated to other organizations or the public. Undetected loss of integrity can be catastrophic for many information types. The consequences of integrity compromise can be either direct (e.g., modification of a financial entry, medical alert, or criminal record) or indirect (e.g., facilitate unauthorized access to sensitive or private information or deny access to information or information system services). For example, unconstrained malicious write access to information and information systems can do enormous harm to an agency's missions and can be employed to use an agency system as a proxy for attacks on other systems. In many cases, the consequences of unauthorized modification or destruction of information to agency mission functions and public confidence in the agency can be expected to be limited. In other cases, integrity compromises can result in the endangerment of human life or other severe consequences. The impact can be particularly severe in the case of time-critical information.

Example Integrity Considerations

High: The application or GSS contains information, which, if modified by unauthorized sources, could result in death or a financial impact over $1 billion. This level indicates that security requirements for assuring confidentiality are of high importance.

Moderate: Information processed by the system is the final version that is disseminated or processed. The issuance of improper information may not be detected elsewhere and would damage public confidence to such a severe degree that the Department would not be trusted to complete this business function or result in a financial impact between $3 million over 3 years and a total impact of $1 billion.

Low: The GSS or application mainly contains messages and reports. If these messages and reports were modified by unauthorized, unanticipated, or unintentional means, employees would detect the modifications; however, these modifications would not be a major concern for the organization.

2.2.2.8 Availability Special Considerations

To determine the appropriate level for availability, consider the needs of the information to be available on a timely basis to meet mission requirements or to avoid substantial losses.

The availability requirement must be based on the period of operation during which the GSS or application is most critical to the business function it enables. For instance, if a GSS or application operates only one month a year, consider the availability requirement for that month.

Table 2-3. Availability Special Considerations

Level	Description
Low	Information that is considered Supportive to the operations of the Department and is not required to be operational to enable the Department to perform essential functions for a Principal Office Business Continuity Plan (BCP) or the Department's Continuity of Operations (COOP). This

Level	Description
	information is processed/ stored in Education assets that are determined to be Mission Supportive Education assets based on the Department's Critical Infrastructure Protection (CIP) survey.[14]
Moderate	Information that is considered Important to the operations of the Department and/ or is required to be operational to enable the Department to perform essential functions for a Principal Office Business Continuity Plan (BCP). This information is processed/ stored in Education assets that are determined to be Mission Important Education assets based on the Department's Critical Infrastructure Protection (CIP) survey.[15]
High	Information that is considered Critical to the operations of the Department and/ or is required to be operational to enable the Department to perform essential functions for the Department's Continuity of Operations (COOP). This information is processed/ stored in Education assets that are determined to be Mission Critical Education assets based on the Department's Critical Infrastructure Protection (CIP) survey.[16]

Common Availability Factors:

Using the FIPS 199 impact criteria, each information type should be evaluated with respect to the low/ moderate/ high impact associated with loss of availability of 1) each known variant of the information belonging to the type and 2) each use for the information by the system under review. For many information types and information systems, the availability impact level depends on how long the information or system remains unavailable. Undetected loss of availability can be catastrophic for many information types. For example, permanent loss of budget execution, contingency planning, continuity of operations, service recovery, debt collection, taxation management, personnel management, payroll management, security management, inventory control, logistics management, or accounting information data bases would be catastrophic for almost any agency. Complete reconstruction of such databases would be time-consuming and expensive. The disruption to agency operations would be serious to severe. In most cases, the adverse effects of limited-duration availability compromise agency mission functions and public confidence in the agency will be limited. In contrast, for time-critical information resources, there is a limited likelihood of successful restoration prior to serious harm to agency assets, operations or personnel.

Each information type should be evaluated with respect to the low/ moderate/ high impact associated with the answers to the questions below.

- Is the system considered a mission critical asset per the Critical Infrastructure Protection efforts?
- Is the system part of the organization's business continuity plan?

Example Availability Considerations

High: The application is required to provide emergency funding to school districts during a crisis. If unavailable, one of the Department's COOP functions, Project SERV, could not be completed.

Moderate: The application supports a business function required for a Principal Office BCP. If unavailable, the business function could not be completed.

Low: The GSS or application has a duplicate from which the information can be accessed and processed, causing no interruption in the continuity of business functions. The application is not required

[14] *The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)*

[15] *The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)*

[16] *The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)*

to complete a function for a Principal Office BCP or the Department's COOP and was determined to be Mission-Supportive via the Critical Infrastructure Protection (CIP) Survey.

2.2.3 Mission Criticality

Mission criticality, or how integral the GSS or application is to carrying out the mission of the agency,[17] must also be considered in this inventory process. The criticality of some GSS's and applications for performing a business function may be more critical during certain periods of operation. **Determine the mission-criticality based on the period of operation during which it is most essential for the business function to be conducted.** Each GSS and application must be evaluated to be mission critical, mission important, or mission supportive.

Employing the Department's CIP Survey will validate mission criticality. This evaluation will provide a more objective, repeatable means of determining mission criticality, based on answering a range of questions related to the business functions of the Department. All candidate GSS's and applications must complete the CIP Survey to determine mission criticality. The resultant data will be considered as the official Department list of mission critical, mission important, and mission supportive GSS's and applications.

2.3 Step 3: Identify Major Applications

Per OMB Circular A-130, an application must be considered an MA when it "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. Certain applications, because of the information in them, however, require special management oversight and must be treated as major. Adequate security for other applications must be provided by the security of the GSS in which they operate."[18]

Note: The term major application is not synonymous with the term "major information system," defined in OMB Circular A-130 as "an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources." The status of an application as a major information system also does not preclude it from being a major application.

2.3.1 Determination of Status as Major Application

An application will be considered an MA if it meets one of the following criteria:

- Determined to be Mission Critical or Mission Important
- Determined to be Mission Supportive, but for which at least one of the Information Sensitivity categories is rated as medium or high.

Only applications determined to be MAs are included in the GSS and MA inventory. **Those applications determined not to be MAs are not required to undergo C&A as they rely on the GSS they reside on to provide adequate security.**

[17] *See Critical Missions and Mission-Essential Infrastructure Assets, May 17, 2001*

[18] *OMB Circular A-130, Appendix III*

2.3.2 Major Application-General Support System Linkages

If the application meets the definition of an MA, it is necessary to identify the GSS upon which it resides. Identifying these links will assist with the application of more appropriate security controls to both the MAs and the GSS's.

Additionally, due to the existence of these links, a GSS must be rated, at a minimum, at the same levels as the highest-rated MA that resides on that GSS. Therefore, if the highest-rated MA receives a high for confidentiality, the GSS must also receive a high rating; if the highest-rated MA receives a medium for availability, the GSS must receive at least a medium rating.

2.4 Step 4: Submit to CIO

All GSS's and MAs included in the GSS and MA inventory must include justification for their respective information sensitivity classifications. The documentation must be submitted to the CIO via the GSS and MA Inventory Submission Form (Appendix A) accompanying an official, signed memorandum by the Principal Officer acknowledging ownership of, and responsibility for, the security of those GSS's and MAs (see Appendix C for sample memorandum).

The GSS and MA Inventory Submission Form and CIP Survey must be completed for all other applications as well, to document the reason for not considering them GSS's or MAs.

Once this documentation is provided for every GSS and MA, future cycles[19] of the GSS and MA inventory process will require all POs to validate the inventory by reviewing those GSS's and MAs under their responsibility as listed in the published GSS and MA inventory. This review will determine whether changes need to be made or that the inventory is accurate. In addition, any new automated information resources must be assessed.

Once the process is complete, an official, signed memorandum must be submitted to the CIO by the Principal Officer to verify that the GSS and MA inventory is accurate. This memorandum will also acknowledge responsibility for the security of those GSS's and MAs. If a change(s) must be made, a GSS and MA Inventory Submission Form, with the change(s) incorporated, including justification for the change(s), must accompany this memorandum.

The GSS and MA Inventory Submission Form will include the following information:

- Principal Office
- Automated information resource name
- Points of contact
- Type of automated information resource – GSS, MA or Application
- Description of data and business function supported by GSS, MA or Application and technical information
- Personally identifiable information responses
- E-authentication responses
- In development or operational
- Line of business and information type
- Information sensitivity (including justification) in the areas of

[19] *The GSS and MA inventory validation process will be completed semi-annually, on January 31 and July 31, with CIO receipt of PO validation of the GSS and MA inventory no less than 2 weeks prior to the final validation date.*

  - Confidentiality
  - Integrity
  - Availability
- Mission criticality (including justification)
- Interconnectivity
- Comments

2.5 Step 5: Endorsement by the CIO

2.5.1 OCIO Review of Inventory

Following receipt of the Principal Officers' submission and prior to finalizing the inventory, OCIO will review the lists and the supporting classifications using the criteria outlined above to ensure the validity and completeness of the lists. If any issue is uncovered, OCIO will work with the appropriate Principal Officer to resolve all outstanding questions.

Following receipt of the Principal Officers' submission and the completion of the review process, the CIO will send an endorsement memorandum to each Principal Officer, as highlighted in Figure 2-2.

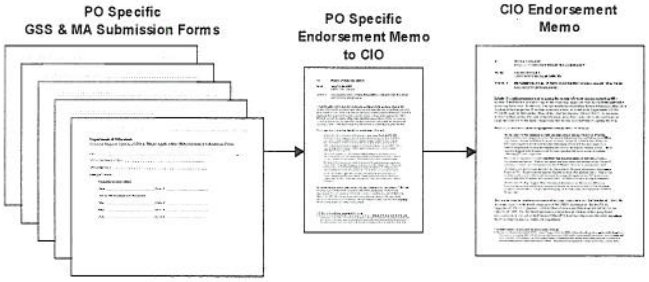

Figure 2-2: Review and Endorsement of GSS and MA Inventory

3. Changes to the Inventory Between Cycles

The information included in the GSS and MA inventory may change between inventory cycles. Notification of these changes must be made to OCIO to maintain the appropriate level of security controls for GSS's and MAs. Updates to the GSS and MA inventory may occur for any number of reasons including changes in the nature of the information processed or a change in dependence on a GSS or MA. These changes may also include system implementation or disposal or changes to the mission criticality or information sensitivity levels. For guidance on automated information resource implementation or disposal, see Section 2.1.2.3.2; for guidance on assessing changes to mission criticality or information sensitivity levels, see Section 2.2 and its subsections.

Appendix A. Acronyms

BCP	Business Continuity Plan
C&A	Certification and Accreditation
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
COOP	Continuity of Operations Plan
CSO	Computer Security Officer
ED	Department of Education
EDNet	Department of Education Network
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GSS	General Support System
IA	Information Assurance
IPSO	Information Processing Service Organization
IT	Information Technology
LAN	Local Area Network
MA	Major Application
MEI	Mission Essential Infrastructure
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCR	Office of Civil Rights
OEF	Office of Educational Furniture
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PO	Principal Office
RAS	Remote Access Service
SDLC	System Development Life Cycle
SP	Special Publication

Appendix B. Definitions

Application	The use of information resources (information and information technology) to satisfy a specific set of user requirements.
Automated information resource	Any (government) equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes, but is not limited too computers, ancillary equipment, applications, software, firmware, similar procedures, services, and related resources."
Capital planning and investment control process	A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.
General Support System (GSS)	An interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network (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).
Government information	Information created, collected, processed, disseminated, or disposed of by or for the Federal Government.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.
Information life cycle	The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.
Information resources	(Information and related resources, such as personnel, equipment, funds, and information technology.
Information technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulations, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. This includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Major Application (MA)	An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
Major Information System	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Appendix C. References

This is a listing of legislation, OMB guidance, and NIST documents relevant to the maintenance of an inventory of GSS's and MAs.

FIPS Guidance

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems

Laws

Clinger-Cohen Act, Public Law 104-106
Paperwork Reduction Act, Public Law 104-13
Freedom of Information Act, Public Law 104-231
Computer Security Act of 1987, Public Law 100-235
Privacy Act, Public Law 93-579
Federal Information Security Management Act, Title III of the E-Government Act of 2002, Public Law 107-347
Higher Education Act (HEA), Public Law 105-244
E-Government Act of 2002, Public Law 107-347

OMB Circulars

OMB Circular A-130, *Management of Federal Information Resources*
OMB Circular A-11, *Planning, Budgeting, Acquisition of Capital Assets, Strategic Plans, Performance Plans*
OMB Circular M04-04. *E-Authentication Guidance for Federal Agencies*

NIST Guidance

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*
NIST SP 800-18, *Procedures for Developing Security Plans for Information Technology Systems*
NIST SP 800-26, *Self-Assessment Procedures for Information Technology Systems*
NIST SP 800-60, Volumes I & II, *Guide for Mapping Types of Information and Information Systems to Security Categories*
NIST SP 800-63, *Electronic Authentication Guidelines*
NIST SP 500-167, *Information Management Directions: The Integration Challenge*

Department Guidance

Handbook OCIO-01 *Handbook for Information Technology Security Policy*
Handbook OCIO-05 *Handbook for Information Technology Security Certification and Accreditation Procedures*
Handbook OCIO-07 *Handbook for Information Technology Security Risk Assessment Procedures*
Project SERV (School Emergency Response to Violence)

Appendix D. GSS and MA Inventory Submission Form

Department of Education Data Sensitivity Worksheet

Date: [Enter Date]

Principal Office: [Enter Principal Office]

Automated Information Resource Name: [Enter Automated Information Resource Name]

Point(s) of Contact:

Computer Security Officer

Name: [Enter Name] Phone #: [Enter Phone Number]

Automated Information Resource Owner(s)

Name: [Enter Principal Officer Name] Phone #: [Enter Phone Number]

Automated Information Resource Owner Representative(s)

Name: [Enter Name] Phone #: [Enter Phone Number]

Automated Information Resource Manager(s)

Name: [Enter Name] Phone #: [Enter Phone Number]

Category (check one)	Explanation (Please respond to each section)	Example Response	
□ General Support System (GSS) □ Major Application (MA) Identified as: Mission-critical or important; or mission-supportive and an Information Sensitivity category rated as 'Moderate' or 'High' □ Application Identified as mission-supportive and all Information Sensitivity categories rated as 'Low'	Business Function: [Enter business function] Data: [Enter Data] Privacy Act Related Questions: Does the system contain personally identifiable information (PII) within any database(s), record(s), file(s), or document(s) such as name, address, social security number, etc.? Yes □ No □ If Yes, describe PII contained by system: Does the system collect any PII from individuals or other resources (i.e., databases, websites, use of cookies)? Yes □ No □ If Yes, describe if PII collected from individuals or other resources: Does the system process any PII with internal or external parties of ED? Yes □ No □ If Yes, describe what internal or external parties process PII contained by system: Hardware: [Enter Hardware] Hardware Location: [Enter Hardware Location] Software: [Enter Software] Software Location: [Enter Software Location] E-Authentication Questions: Does the system require or support authentication for at least a portion of its users? Note: It is assumed that most systems require authentication to perform administrative and maintenance tasks. If this is the only requirement for authentication, then the answer is "No" for whether authentication is required. Yes □ No □ Does the system support browser-based access? Yes □ No □	**Example Response:** □ General Support System (GSS) □ Major Application (MA) Identified as: Mission-critical or important; or Mission-supportive and an Information Sensitivity category rated as 'Moderate' or 'High' ☒ Application Identified as mission- Information Sensitivity categories rated as 'Low' supportive and all	**Example Response:** Business Function: Supports a PO-wide activity limited to just the Office of Educational Furniture. The database helps produce an annual report on the chairs in the POC. It is used to assist in the assignment of new chairs. OEF tests all kinds of Educational Furniture. There are more chairs to be tested than any other type of furniture. OEF assigns a particular chair to one staff member for one month and then the chair is rotated to another staff person for another month. The database tracks the initial delivery of the chair and its pertinent information, and then follows the chair through five staff assignments. Only Executive Office staff can assign chairs, but everyone must complete their chair evaluations in the database. A weekly chair status report is prepared for the Executive Officer. A monthly report and briefing is prepared for the Assistant Secretary. Data: Specific details about the chairs such as, color, brand, model number, category (arm, side, table), or fabric. Details about where the chair is currently assigned such as staff name, room number, and date assigned. The last four digits of the SSN are used in conjunction with the staff name as a staff ID number. Does the system contain personally identifiable information (PII) within any database(s), record(s), file(s), or document(s) such as name, address, social security number, etc.? Yes - it contains staff name. Does the system collect any PII from individuals or other resources (i.e., databases,

		In development or operational: [Enter 'in development' or 'operational']		websites, use of cookies)? Yes - it collects PII from individuals. Does the system process any PII with internal or external parties of ED? No Hardware: EDNET Application Server – Compaq 3000 and EDNET DELL workstations used by OEF staff. Hardware Location: EDNET server room in ROB3, the RAS server in ROB3 (for those dialing into EDNET) and OEF offices in FB6. Software: Access 97 Software Location: Two Access 97 database files (forms and tables) reside on EDNET server (\\ROB3FPR02\Groups\OEP); access 97 is launched off of local EDNET workstations and connects to the forms database that accesses linked tables from the table's database. E-Authentication Questions: Does the system require or support authentication for at least a portion of its users? Note: It is assumed that most systems require authentication to perform administrative and maintenance tasks. If this is the only requirement for authentication, then the answer is "No" for whether authentication is required. Yes ☐ No ☒ Does the system support browser-based access? Yes ☐ No ☒ In development or operational: Operational

	Category (check one)	Explanation (Please respond to each section)	Example Response	
Line of Business	Check the line of business that maps to the main purpose of the automated information resource: Check only 1 of the following: □ Grants □ Loans □ Evaluation □ Research and Statistics □ Information Dissemination □ Compliance □ Administration	Check the business function associated with the line of business chosen. These business functions equate to the Department's basic information types. Check only 1 of the following: **Grants** □ Discretionary Grants □ Formula Grants **Loans** □ Federal Student Aid **Evaluation** □ Evaluation **Research and Statistics** □ Education Research □ Program Research □ Collect and analyze statistics **Information Dissemination** □ Information Dissemination **Compliance** □ Compliance **Administration** □ Acquire Goods and Services □ Provide Legal Services □ Manage Facilities and Travel □ Manage Human Resources □ Manage Financial Resources □ Manage Information Resources □ Develop Strategic Plans	**Example Response:** Check the line of business that maps to the main purpose of the automated information resource: Check only 1 of the following: □ Grants □ Loans □ Evaluation □ Research and Statistics □ Information Dissemination □ Compliance ☒ Administration	**Example Response:** Check the business function associated with the line of business chosen. These business functions equate to the Department's basic information types. Check only 1 of the following: **Grants** □ Discretionary Grants □ Formula Grants **Loans** □ Federal Student Aid **Evaluation** □ Evaluation **Research and Statistics** □ Education Research □ Program Research □ Collect and analyze statistics **Information Dissemination** □ Information Dissemination **Compliance** □ Compliance **Administration** □ Acquire Goods and Services □ Provide Legal Services ☒ Manage Facilities and Travel □ Manage Human Resources □ Manage Financial Resources □ Manage Information Resources □ Develop Strategic Plans

	Category (check one)	Explanation	Example Response	
Information Sensitivity	Confidentiality[20] □ High □ Moderate □ Low	[Enter Explanation - see example responses on the right]	**Example Response:** Confidentiality ☒ High □ Moderate □ Low Confidentiality □ High ☒ Moderate □ Low Confidentiality □ High □ Moderate ☒ Low	**Example Response:** The system includes information that if viewed by an unauthorized individual could result in death The system includes Privacy Act information that could be used for identify theft such as social security numbers, PIN numbers, Tax ID numbers, income information, etc. The system only contains data that has no expectation of privacy or Privacy Act data that is not likely to cause identify theft, for instance, only an individual's name and home address.

[20] *Systems that may contain personally identifiable information are required to conduct a Privacy Impact Assessment (PIA) per OMB Circular A-11, sections 31.8, 53.1 and 300.9 In addition, The E-Government Act of 2002 requires: the completion of a PIA; review of the PIA by the CIO; publication of the PIA in the Federal Register; and submission to OMB of the PIA with all funding requests (i.e., Exhibit 300s). The scope of the PIA should be commensurate with the size of the system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information. At a minimum, a PIA should address: 1) what information is to be collected; 2) why the information is being collected; 3) the intended use of the agency of the information; 4) with whom the information will be shared; 5) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; 6) how the information will be secured; and 7) whether a system of records is being created under the ''Privacy Act''. In the event that the system does not collect, use, or store privacy information the resulting scope of the PIA will be limited to a one-page summary of findings. Please see the Department's Privacy Officer for complete guidance on conducting a full PIA.*

Category (check one)	Explanation	Example Response	
Integrity □ High □ Moderate □ Low	[Enter Explanation - see example responses on the right]	**Example Response:**	**Example Response:**
		Integrity ☒ High □ Moderate □ Low	The system includes information that if modified by an unauthorized individual could result in death
		Integrity □ High ☒ Moderate □ Low	The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Payments activities are not generally time-critical. In most cases, the adverse effects of consequent negative publicity and institution of corrective action programs on mission functions or public confidence in the agency can be serious.
		Integrity □ High □ Moderate ☒ Low	Information processed by the system is part of an overall project and is not the final version that is disseminated or processed. The issuance of improper information could be detected elsewhere and would not damage public confidence to such a severe degree that the Department would not be trusted to complete this business function or result in a financial impact over $3 million over 3 years.

Category (check one)	Explanation	Example Response	
Availability □ High = Mission-Critical/Department COOP Essential □ Moderate = Mission-Important or Principal Office BCP Essential □ Low = Mission-Supportive Per the results of the Critical Infrastructure Protection (CIP) Survey and the Principal Office Business Continuity Plan (BCP): Mission-Critical/ Department COOP Essential = High *Mission-Important or Principal Office BCP Essential = Moderate* Mission-Supportive = Low	[Enter Explanation - see example responses on the right]	**Example Response:**	**Example Response:**
		Availability ☒ High = Mission-Critical/Department COOP Essential □ Moderate = Mission-Important or Principal Office BCP Essential □ Low = Mission-Supportive	This system was determined to be Mission-Critical via the Critical Infrastructure Protection Survey. This system is required to be operational to enable the Department to perform [enter function], which is an essential function during the Department's Continuity of Operations (COOP).
		Availability □ High = Mission-Critical/Department COOP Essential ☒ Moderate = Mission-Important or Principal Office BCP Essential □ Low = Mission-Supportive	This system was determined to be Mission-Important via the Critical Infrastructure Protection Survey And/or is required to be operational to enable the Department to perform [enter function name], an essential function for the [enter Principal Office name] Business Continuity Plan (BCP).
		Availability □ High = Mission-Critical/Department COOP Essential □ Moderate = Mission-Important or Principal Office BCP Essential ☒ Low = Mission-Supportive	This system was determined to be Mission-Supportive via the Critical Infrastructure Protection Survey And is not required to be operational to enable the Department to perform essential functions for a Principal Office Business Continuity Plan (BCP) or the Department's Continuity of Operations (COOP).

Category (check one)		Explanation	Example Response	
Mission Criticality	Mission-Criticality □ Critical □ Important □ Supportive	[Enter Explanation - see example responses on the right]	**Example Response:**	**Example Response:**
			Mission-Criticality ☒ Critical □ Important □ Supportive	The overall mission-criticality was determined per the results of the Critical Infrastructure Protection survey.
			Mission-Criticality □ Critical ☒ Important □ Supportive	The overall mission-criticality was determined per the results of the Critical Infrastructure Protection survey.
			Mission-Criticality □ Critical □ Important ☒ Supportive	The overall mission-criticality was determined per the results of the Critical Infrastructure Protection survey.

Interconnectivity	If an application or major application, list the GSS on which it resides. Does the automated information resource have interconnectivity with other GSS's or applications? □ Yes □ No	[Enter Explanation - see example responses on the right]	**Example Response:** If an application or major application, list the GSS on which it resides. Does the automated information resource have interconnectivity with other GSS's or applications? □ Yes ☒ No Does the automated information resource have interconnectivity with other GSS's or applications? ☒ Yes □ No	**Example Response:** The GSS is EDNet. The system does not interconnect with other GSS's or applications. The GSS is EDNet. The system also interconnects with the Human Resources System.

Appendix E. Sample GSS and MA Inventory Submission Form

Department of Education Data Sensitivity Worksheet

Date: July 30, 2004

Principal Office: Office of Educational Furniture

Automated Information Resource Name: Imaginary Chair Tracking System (ChTS)

Point(s) of Contact:

Computer Security Officer

Name: I.B. Security Phone #: 202-111-2222

Automated Information Resource Owner(s)

Name: Jane Smith Phone #: 202-111-9999

Automated Information Resource Owner Representative(s)

Name: Ethan Allen Phone #: 202-111-5684

Automated Information Resource Manager(s)

Name: Bob Jones Phone #: 202-111-8453

Category (check one)	Explanation (Please respond to each section)
□ General Support System (GSS) □ Major Application (MA) Identified as: Mission-critical or important; or mission-supportive and an Information Sensitivity category rated as 'Moderate' or 'High' ☒ Application Identified as mission-supportive and all Information Sensitivity categories rated as 'Low'	Business Function: Supports a PO-wide activity limited to just the Office of Educational Furniture. The database helps produce an annual report on the chairs in the POC. It is used to assist in the assignment of new chairs. OEF tests all kinds of Educational Furniture. There are more chairs to be tested than any other type of furniture. OEF assigns a particular chair to one staff member for one month and then the chair is rotated to another staff person for another month. The database tracks the initial delivery of the chair and its pertinent information, and then follows the chair through five staff assignments. Only Executive Office staff can assign chairs, but everyone must complete their chair evaluations in the database. A weekly chair status report is prepared for the Executive Officer. A monthly report and briefing is prepared for the Assistant Secretary. Data: Specific details about the chairs such as, color, brand, model number, category (arm, side, table), or fabric. Details about where the chair is currently assigned such as staff name, room number, and date assigned. The last four digits of the SSN are used in conjunction with the staff name as a staff ID number. Does the system contain personally identifiable information (PII) within any database(s), record(s), file(s), or document(s) such as name, address, social security number, etc.? Yes - it contains staff name. Does the system collect any PII from individuals or other resources (i.e., databases, websites, use of cookies)? Yes - it collects PII from individuals. Does the system process any PII with internal or external parties of ED? No Hardware: EDNET Application Server – Compaq 3000 and EDNET DELL workstations used by OEF staff. Hardware Location: EDNET server room in ROB3, the RAS server in ROB3 (for those dialing into EDNET) and OEF offices in FB6. Software: Access 97 Software Location: Two Access 97 database files (forms and tables) reside on EDNET server (\\ROB3FPR02\Groups\OEP); access 97 is launched off of local EDNET workstations and connects to the forms database that accesses linked tables from the table's database. E-Authentication Questions: Does the system require or support authentication for at least a portion of its users? Note: It is assumed that most systems require authentication to perform administrative and maintenance tasks. If this is the only requirement for authentication, then the answer is "No" for whether authentication is required. Yes □ No ☒ Does the system support browser-based access? Yes □ No ☒ In development or operational: Operational

	Category (check one)	Explanation (Please respond to each section)
Line of Business	Check the line of business that maps to the main purpose of the automated information resource: Check only 1 of the following: □ Grants □ Loans □ Evaluation □ Research and Statistics □ Information Dissemination □ Compliance ☒ Administration	Check the business function associated with the line of business chosen. These business functions equate to the Department's basic information types. Check only 1 of the following: **Grants** □ Discretionary Grants □ Formula Grants **Loans** □ Federal Student Aid **Evaluation** □ Evaluation **Research and Statistics** □ Education Research □ Program Research □ Collect and analyze statistics **Information Dissemination** □ Information Dissemination **Compliance** □ Compliance **Administration** □ Acquire Goods and Services □ Provide Legal Services ☒ Manage Facilities and Travel □ Manage Human Resources □ Manage Financial Resources □ Manage Information Resources □ Develop Strategic Plans

	Category (check one)	Explanation
Information Sensitivity	Confidentiality[21] ☐ High ☐ Moderate ☒ Low	The system only contains data that has no expectation of privacy or Privacy Act data that is not likely to cause identify theft, for instance, only a staff member's name.
	Integrity ☐ High ☐ Moderate ☒ Low	Information processed by the system is part of an overall project and is not the final version that is disseminated or processed. The issuance of improper information could be detected elsewhere and would not damage public confidence to such a severe degree that the Department would not be trusted to complete this business function or result in a financial impact over $3 million over 3 years.

[21] *Systems that may contain personally identifiable information are required to conduct a Privacy Impact Assessment (PIA) per OMB Circular A-11, sections 31.8, 53.1 and 300.9 In addition, The E-Government Act of 2002 requires: the completion of a PIA; review of the PIA by the CIO; publication of the PIA in the Federal Register; and submission to OMB of the PIA with all funding requests (i.e., Exhibit 300s). The scope of the PIA should be commensurate with the size of the system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information. At a minimum, a PIA should address: 1) what information is to be collected; 2) why the information is being collected; 3) the intended use of the agency of the information; 4) with whom the information will be shared; 5) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; 6) how the information will be secured; and 7) whether a system of records is being created under the "Privacy Act". In the event that the system does not collect, use, or store privacy information the resulting scope of the PIA will be limited to a one-page summary of findings. Please see the Department's Privacy Officer for complete guidance on conducting a full PIA.*

	Category (check one)	Explanation
	Availability ☐ High = Mission-Critical/Department COOP Essential ☐ Moderate = Mission-Important or Principal Office BCP Essential ☒ Low = Mission-Supportive **Per the results of the Critical Infrastructure Protection (CIP) Survey and the Principal Office Business Continuity Plan (BCP):** Mission-Critical/ Department COOP Essential = High *Mission-Important or Principal Office BCP Essential = Moderate* Mission-Supportive = Low	This system was determined to be Mission-Supportive via the Critical Infrastructure Protection Survey **And** is not required to be operational to enable the Department to perform essential functions for a Principal Office Business Continuity Plan (BCP) or the Department's Continuity of Operations (COOP).
Mission Criticality	Mission-Criticality ☐ Critical ☐ Important ☒ Supportive	The overall mission-criticality was determined per the results of the Critical Infrastructure Protection survey.

	Category (check one)	Explanation
Interconnectivity	If an application or major application, list the GSS on which it resides. Does the automated information resource have interconnectivity with other GSS's or applications? □ Yes ☒ No	The GSS is EDNet. The system does not interconnect with other GSS's or applications.

Appendix F. Sample Memoranda

SAMPLE MEMORANDUM FROM THE CHIEF INFORMATION OFFICER

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

From: [CHIEF INFORMATION OFFICER NAME]
Chief Information Officer

Subject: Endorsement of [PO NAME]'s General Support System and Major Application Inventory.

As the Chief Information Officer for the Department of Education, I hereby acknowledge that the following General Support System (GSS) and Major Application (MA) inventory is accurate and comprehensive – consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, the Clinger-Cohen Act[22], the Federal Information Security Management Act (FISMA), and the Computer Security Act of 1987[23] – as of [DATE OF SUBMISSON] for the [PO NAME].

GSS/MA Name	Type (GSS or MA)	Mission Criticality	Information Sensitivity			Last Inventory Update
			Confidentiality	Integrity	Availability	

My point of contact for the maintenance of this GSS and MA inventory is Jenny Beale at 202-245-6415.

[22] *Public Law 104-106*

[23] *Public Law 100-235*

SAMPLE MEMORANDUM FROM PRINCIPAL OFFICERS TO THE CHIEF INFORMATION OFFICER VALIDATING THE GSS AND MA INVENTORY

To: [CHIEF INFORMATION OFFICER NAME]
Chief Information Officer

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

Subject: Endorsement of [PO NAME]'s General Support System and Major Application Inventory.

As the Principal Officer for the [PO NAME], I hereby acknowledge that the following General Support System (GSS) and Major Application (MA) inventory and the attached inventory submission forms for each GSS and MA is accurate and comprehensive – consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, the Clinger-Cohen Act,[24] the Federal Information Security Management Act (FISMA), and the Computer Security Act of 1987,[25] as of [DATE OF SUBMISSON] for the [PO NAME].

GSS/MA Name	Type (GSS or MA)	Mission Criticality	Information Sensitivity			Last Inventory Update
			Confidentiality	Integrity	Availability	

My point of contact for the maintenance of this GSS and MA inventory is [POC NAME & NUMBER].

Attachments [N] inventory submission forms

[24] *Public Law 104-106*

[25] *Public Law 100-235*

Appendix G. Confidentiality Special Considerations

NIST SP 800-60 provides baseline information sensitivity ratings for information types transmitted, stored, or processed on GSS's or MAs based on definitions provided in FIPS 199. Per this guidance, recommended information sensitivity ratings for confidentiality are provided below.

<table>
<tr><th colspan="2">INFORMATION RATED AS MODERATE FOR CONFIDENTIALITY</th></tr>
<tr><td>• Social Security Numbers
• Credit History
• Personal Financial Information
• Financial Account Information and/or Numbers (e.g., checking account numbers and PIN's)
• Driver's License
• Mother's Maiden Name
• Medical Records Numbers
• Medical Notes
• Income Information
• Personal Identity and Authentication Information (that could cause identity theft or fraud)
• Entitlement Event Information
• Representative Payee Information
• ED Law Enforcement Investigations
• Confidential Sources
• Law Enforcement Techniques
• Student Records</td><td>Exemption (b)(6) of the FOIA protects from disclosure information about individuals contained in "personnel, medical or similar files" when release of the information "would constitute a clearly unwarranted invasion of personal privacy." An individual's name and address may not be sold or rented by an agency unless specifically authorized by law. Any contractor or employee of a contractor is considered to be an employee of the agency.

Exemption (b)(7) of the FOIA protects from disclosure records or information compiled for law enforcement purposes to the extent such records could reasonably be expected to interfere with enforcement proceedings, constitute an unwarranted invasion of personal privacy, disclose the identity of a confidential source, endanger the life or safety of any individual, or risk circumvention of the law by disclosing law enforcement techniques. Law enforcement refers to both civil and criminal laws. As such, it includes OIG, OCR, and similar investigations.</td></tr>
<tr><th colspan="2">INFORMATION RATED AS LOW FOR CONFIDENTIALITY</th></tr>
<tr><td>• Grantee name (business contact information)
• Employee names, titles, grades, salaries, position descriptions, duty stations, office phone numbers or e-mail addresses
• Contractor names, e-mail addresses or business contact information</td><td>Exemption (b)(6) of the FOIA states that information submitted with no expectation of privacy should be considered non-confidential information.</td></tr>
</table>