DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

INFORMATION TECHNOLOGY SYSTEM CERTIFICATION AND ACCREDITATION INVENTORY GUIDE

Version 1.0

Document Configuration Control

Version	Release Date	Summary of Changes

TABLE OF CONTENTS

1.0 Overview 1

1.1 PURPOSE 1

1.2 OBJECTIVES & GOALS 1

1.3 AUDIENCE 2

1.4 DOCUMENT STRUCTURE 2

2.0 Methodology for Determination of GSS and MA Inventory 3

2.1 STEP 1: IDENTIFY GENERAL SUPPORT SYSTEMS AND APPLICATIONS 5
2.1.1 Step 1A: Identify Business Functions 5
2.1.2 Step 1B: Identify Automated Information Resources 5
2.1.3 Step 1C: Categorize Automated Information Resources as GSS or Application 8

2.2 STEP 2: CLASSIFY GSS AND APPLICATIONS 9
2.2.1 Information Sensitivity 10
2.2.2 Determining Information Sensitivity 10
2.2.3 Mission Criticality 15

2.3 STEP 3: IDENTIFY MAJOR APPLICATIONS 16
2.3.1 Major Application-General Support System Linkages 16

2.4 STEP 4: SUBMIT TO CIO 16
2.4.1 Deputy Assistant Secretary Office Review 17
2.4.2 CIO Inventory Publication 18

3.0 Changes to the Inventory Between Cycles 19

4.0 Relevant definitions 20

5.0 References 22

Appendix A - GSS and MA Inventory Submission Form A-1

Appendix B - Sample Inventory Submission Form B-1

1.0 OVERVIEW

1.1 PURPOSE

The purpose of this guide is twofold. First, the document describes the process that will be used by the Department of Housing and Urban Development (HUD) to establish and maintain an inventory of general support systems (GSSs) and major applications (MAs) for the purpose of certification and accreditation. Second, the document provides guidance to system owners (SOs) regarding the standards to be employed throughout this process. The concepts of GSSs and MAs are defined in 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 share 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 IT systems certification and accreditation inventory to formally identify and document the security classifications of GSSs and MAs in use by the Department in compliance with Federal requirements. This GSS and MA inventory is intended to complement existing Departmental security initiatives, such as those under the Federal Information Security Management Act (FISMA) and Critical Infrastructure Protection mandates.

1.2 OBJECTIVES & GOALS

The primary objective in developing a systematic approach for the inventory and classification of the GSSs 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 GSSs 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 GSSs 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 (i.e., applications that do not require additional security controls) rely on the GSSs in which they operate for the provision of adequate security. 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 GSSs

[1] *OMB Circular A-130.*

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

and MAs included in the inventory can be found in the Department's Certification and Accreditation related guidance.

1.3 AUDIENCE

This document is intended for the following Department personnel:

- System Owners – In their capacity to provide security controls appropriate for the protection of Department information.
- Information Systems Security Officers (ISSOs) – In their capacity for maintaining the information security program within the respective organizations.
- Designated Approving Authority (DAA) – In his/her capacity as the official who grants formal approval to operate an IT system.
- The Chief Information Officer (CIO) – In his/her capacity as the official responsible for providing guidance on information security throughout the Department.

1.4 DOCUMENT STRUCTURE

This document is organized into five sections, each discussing an aspect of the GSS and MA inventory process. The first section provides an overview of the guide. The second section details the steps to be taken to complete the process along with standardized definitions and criteria to be employed throughout the process. The third section includes guidance for ongoing maintenance of the GSS and MA inventory. The fourth section provides a listing of all applicable definitions. The fifth section is a list of references relevant to the creation and maintenance of the Department's GSS and MA inventory.

Appendix A provides the GSS and MA Inventory Submission Form that should be used to document and submit the results of the inventory process.

2.0 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 GSSs and Applications* – Determine 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

Step 2: *Classify GSSs and Applications* – Ascertain the security needs of each based upon additional considerations

Step 3: *Identify Major Applications (MAs)* – Use security classifications to determine if an application qualifies as an MA – those applications that require special security considerations due to the nature of the information in the application. (Only those applications determined to be MAs will be included in the GSS and MA inventory; see Section 2.3)

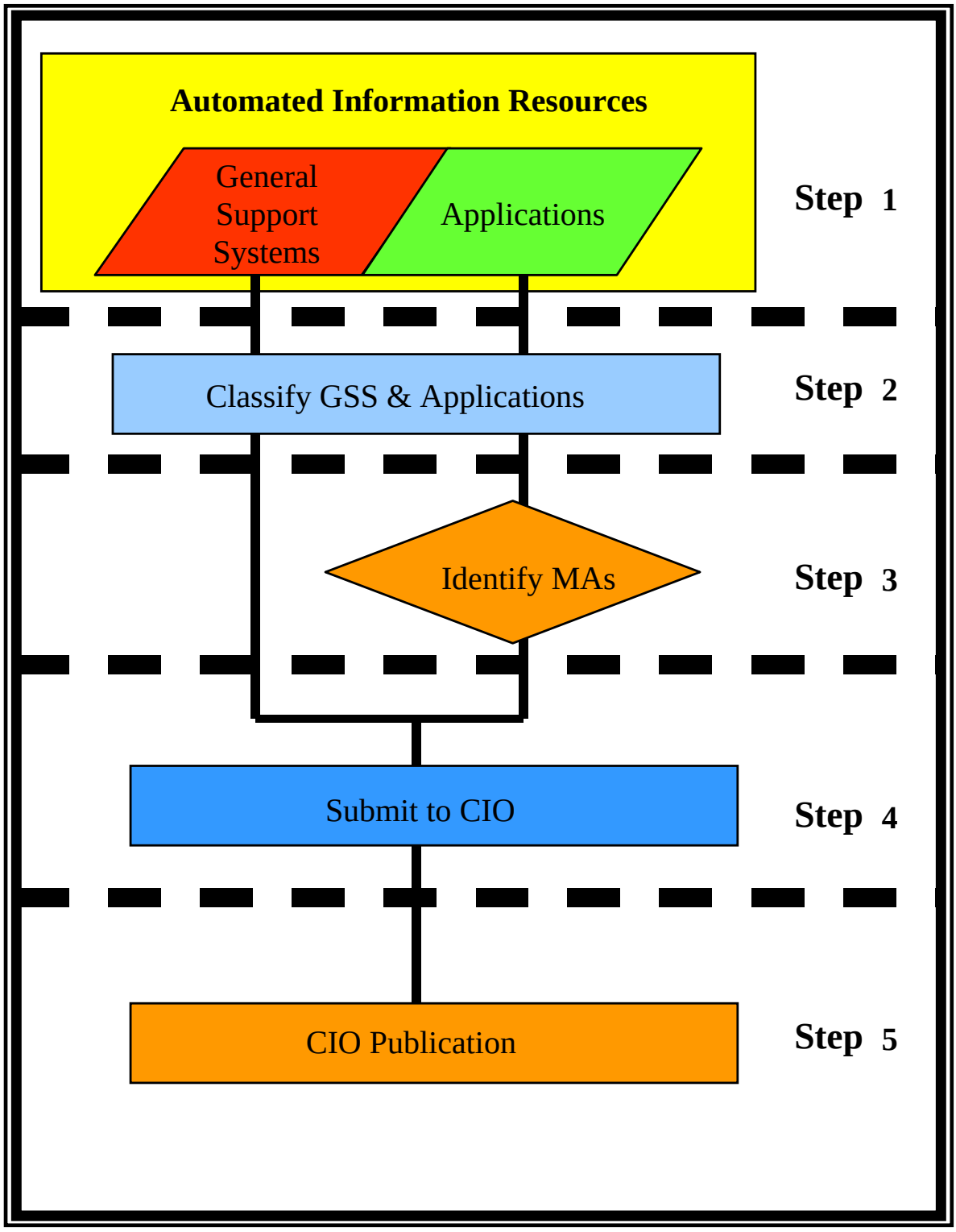
Step 4: *Submit to CIO* – System owners validate and acknowledge the GSS and MA inventory as accurate

Step 5: *CIO Publishes the Inventory* – Generate the official GSS and MA Inventory for the Department.

Once steps 1-3 are completed for a particular GSS or MA their results should be documented in the attached form in Appendix A and endorsed, with the entirety of the system owner's GSSs and MAs.

To retain a current and comprehensive list of the GSSs 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, system owners will need to validate the inventory on record or update information on the GSSs and MAs. CIO receipt of system owner validation of the GSS and MA inventory will be required no less than 2 weeks prior to the final validation date. If, at any point during the GSS and MA inventory process, there is need for clarification, system owners should consult with the CIO to ensure compliance with the applicable requirements.

Figure 2-1: GSS and MA Inventory Process



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 GSSs and MAs is to identify all automated information resources used by the OA to perform its business functions. All automated information resources used are either a GSS or an application. (See Section 2.1.3) Existing enterprise architecture documentation, etc. should be used to simplify this process.

To begin, identify the business functions that occur within the Department – the work the Department performs in support of the mission, vision, and goals. 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. Those automated information resources are included as candidates for the GSS and MA inventory.

For each business function, identify and describe any automated process that supports it. Identify the automated information resources employed by the automated process including databases, stand-alone systems, communications systems, networks, and any other type of information technology-related support. Automated information resources that utilize general-purpose software such as spreadsheets and word processing software are not included as candidates as their security is provided by the GSS on which they reside.[3]

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.

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

Shared Resources & System Interconnectivity

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.

Is any business function supported by automated information resources not owned by the Department?

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 system owner or 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.

If another agency runs a system that processes Department information, an interagency agreement should be put in place to officially verify terms of agreement for the protection of information between the agencies as well as to ensure adequate security measures are instituted to protect the information.[4] This same guideline will apply to interconnectivity of systems within HUD (intra-agency).

Any automated information resource that receives federal funding must be considered as a candidate general support system or application.

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."

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:

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

- 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.[5]

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.

- *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 records archives, should be excluded.

- *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." FISMA, along with the Clinger-Cohen Act and the Computer Security Act of 1987 direct the heads of agencies to "ensure that information security is addressed throughout the life cycle of each agency information system." 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 should be considered as they are planned to operate when fully functional, not necessarily how they currently operate. Security should be planned for the data that will be processed, whether or not that data is yet processed by the automated information

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

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

resource. It is understood that these classifications may change throughout the life of the automated information resource, but it is important to have accurate 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 should be updated to accurately reflect the current state of the data sensitivity or mission criticality. (See Section 2.4)

Similarly, an automated information resource may not be excluded from the list of candidates if it is only scheduled for retirement. The automated information resource may not be removed from consideration unless it has been completely disconnected or shut down, information requiring protection is properly removed from the automated information resource, and official confirmation of such action has been received by the CIO.

- *Information Technology Capital Planning*

  Consistent with the Lifecycle Considerations Subsection immediately above, 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

Per the guidance of OMB Circular A-130, Appendix III, Federal agencies are directed to provide adequate security for all automated information resources, which includes both government information and information technology.

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

Government information is information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

General Support Systems

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)."[6]

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

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

Is the automated information resource used by other automated information resources to transmit or store data?

Applications

An application is "the use of information resources to satisfy a specific set of user requirements."[7]

Identification as an MA is based upon the classifications in Section 2.2 and is fully explained in Section 2.3. **Note: Only applications identified as MAs will be included as separate systems in the final GSS and MA inventory. All other applications will be identified as part of the GSS.**

2.2 STEP 2: CLASSIFY GSS AND APPLICATIONS

To support the development and maintenance of appropriate security controls for GSSs and MAs on the inventory, it is necessary to identify security classifications for each, and for the information it handles. This section will describe and define several sets of security classifications to be applied to the GSSs and applications identified in Section 2.1 to appropriately evaluate the level of security required for each.

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

6 *OMB Circular A-130, Appendix III*

7 *OMB Circular A-130, Appendix III*

inventory. All other applications will be identified as part of the GSS.

2.2.1 INFORMATION SENSITIVITY

One of the considerations system owners must make in all phases of the system life cycle is that of privacy, i.e., how HUD collects and handles personal information. Two main privacy laws apply to federal government systems: Privacy Act of 1974 and E-Government Act of 2002.

To comply with these laws, HUD must first understand the nature of applicable data elements, determining whether the system in question contains personally identifiable information (PII). Personally Identifiable Information, or PII, is data that links back to an individual. For example, a name, phone number, address, email address, social security number, vehicle identification number, and driver's license number are all examples of PII. Aggregate statistical data are NOT PII.

If the system in question contains PII, contact your OA's Privacy Officer for assistance in complying with the Privacy Act of 1974 and E-Government Act of 2002.

Public Web sites must follow additional privacy guidance, as provided by the E-Government Act of 2002 and OMB M-03-22. If the system in question is a Web-enabled system and accessed by individuals other than federal government employees/contractors, or if the system is tied to a public Web site, contact your organization's Privacy Officer for assistance in complying with these privacy regulations.

2.2.2 DETERMINING INFORMATION SENSITIVITY

To appropriately protect information, its relationship to and impact on the mission of the Department or an OA 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.

The *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199), uses three basic protection requirements in order to determine information sensitivity - confidentiality, integrity (which, for the purposes of the Guide, includes non-repudiation and authenticity), and availability.

- Confidentiality – Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity – Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.
- Non-repudiation – Verification of the origin or receipt of a message.
- Authenticity – Verification that the content of a message has not changed in transit.
- Availability – Ensuring timely and reliable access to and use of information.

Each area must be rated on the scale of High, Moderate, or Low, using the following guidance from NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, and FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, for making the sensitivity determination.

Confidentiality

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.

How severe a loss would occur as a result of disclosure of data?

Note: If an application or GSS has information covered under the Privacy Act, the system owner should contact the HUD Privacy Officer to ensure compliance.

The following descriptions from FIPS 199 will be used as guidance in making this determination.

Confidentiality Considerations

High

A **severe or catastrophic** adverse effect means that the loss of confidentiality 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*;
- result in *major financial loss*; or
- result in *severe or catastrophic harm to individuals* involving loss of life or serious life threatening injuries.

Moderate

A **serious** adverse effect means that the loss of confidentiality 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*;
- result in *significant financial loss*; or
- result in *significant harm to individuals* that does not involve loss of life or serious life threatening injuries.

Low

A **limited** adverse effect means that the loss of confidentiality 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*;
- result in *minor financial loss*; or
- result in *minor harm to individuals*.

Integrity

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

How severe a loss would occur if the data were incorrect?

Included in this decision should be how the GSS or application is employed in the business process. 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 be generally 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 part of the business process.

The following descriptions from FIPS 199 will be used as guidance in making this determination.

Integrity Considerations

High

A **severe or catastrophic** adverse effect means that the loss of integrity 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*;
- result in *major financial loss*; or
- result in *severe or catastrophic harm to individuals* involving loss of life or serious life threatening injuries.

Moderate

A **serious** adverse effect means that the loss of integrity 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*;
- result in *significant financial loss*; or
- result in *significant harm to individuals* that does not involve loss of life or serious life threatening injuries.

Low

A **limited** adverse effect means that the loss of integrity 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*;

- result in *minor financial loss*; or
- result in *minor harm to individuals*.

Availability

How severe a loss would occur if the information were not available as needed?

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. Availability includes both the disruption of access to or use of information and an information system.

The availability requirement should 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.

The following descriptions from FIPS 199 will be used as guidance in making this determination.

Availability Considerations

High

A **severe or catastrophic** adverse effect means that the loss of 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*;
- result in *major financial loss*; or
- result in *severe or catastrophic harm to individuals* involving loss of life or serious life threatening injuries.

Moderate

A **serious** adverse effect means that the loss of 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*;
- result in *significant financial loss*; or
- result in *significant harm to individuals* that does not involve loss of life or serious life threatening injuries.

Low

A **limited** adverse effect means that the loss of 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*;
- result in *minor financial loss*; or
- result in *minor harm to individuals*.

2.2.3 MISSION CRITICALITY

Both Mission Critical and Non-Mission Critical systems must be included in the GSS and MA inventory. Mission criticality is an assessment of how integral the GSS or application is to the performance of the HUD mission, and must also be considered in the inventory process. Using the current Department definitions below, each must be evaluated to be Mission Critical or Non-Mission Critical.

Note: the criticality of some GSSs 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.

Mission Critical Systems

The term mission critical system means any telecommunications or information system (GSS and/or MA) used or operated by HUD or by a contractor of HUD, or other organization on behalf of HUD, that:

- is defined as a *national security system* under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452); or

- is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be *classified in the interest of national defense or foreign policy*; or

- processes any information, the loss, misuse, disclosure or unauthorized access to or modification of would have a *debilitating impact* on the HUD mission.

Non-Mission Critical Systems

Non - Mission critical GSSs and major applications are those automated information resources that do not fit under the mission critical definition and whose failure would not preclude the Department or one of its subordinate organizations from accomplishing core business operations in the short to long term, but would have an impact on the effectiveness or efficiency of day-to-day operations. Examples of non-mission critical GSSs or major applications are a system that:

- tracks or calculates data for organizational convenience, or
- would only cause loss of business efficiency and effectiveness for the owner.

Can the core business operations be accomplished through manual means, even if less efficient, if the GSS or application is unavailable for more than 1 month?

2.3 STEP 3: IDENTIFY MAJOR APPLICATIONS

Per OMB Circular A-130, an application should be considered a Major Application (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." According to OMB A-130 all Federal applications require some level of protection. However, certain applications, because of the information in them, require special management oversight and should be treated as major. Adequate security for other applications should be provided by the security of the GSS in which they operate."[8]

2.3.1 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 linkages will assist with the application of more appropriate security controls to both the MAs and the GSSs.

NOTE: If an MA is identified as mission critical, then the GSS upon which the MA resides must be considered mission critical also.

2.4 STEP 4: SUBMIT TO CIO

All GSSs and MAs included in the GSS and MA inventory must include justification for their respective information sensitivity classifications. The documentation should be submitted to the CIO via the GSS and MA Inventory Submission Form (Appendix A) accompanying an official, signed memorandum by the system owner acknowledging ownership of and responsibility for the security of those GSSs and MAs. Appendix A includes a worksheet that can be used to help identify the required information. A sample submission form and worksheet are also provided.

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

Once this documentation is provided for every GSS and MA, future cycles[9] of the GSS and MA inventory process will require all system owners to validate the inventory by reviewing those GSSs 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 the inventory is accurate.

Once the process is completed, an official, signed memorandum must be submitted to the CIO to verify that the GSS and MA inventory is accurate. This memorandum will also acknowledge responsibility for the security of those GSSs 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:

- Owning organization
- Information System Name and Acronym
- Status of System (i.e., operational)
- Accreditation Status (Yes/No, Date, If No – when accreditation is planned)
- Points of Contact to include: system owner, information systems security officer, primary and secondary system administrator, and Designated Approving Authority.
- Type of automated information resource – GSS or MA
- Associated URLs, IP addresses, and technologies
- Interconnectivity/information sharing/interfaces
- Description of data and business function supported by GSS or MA
- Mission Criticality (including justification)
- Information Sensitivity (including justification) in the areas of
  - Confidentiality
  - Integrity
  - Availability
- Comments

2.4.1 DEPUTY ASSISTANT SECRETARY OFFICE REVIEW

Following receipt of the system owners' submission, the offices of Deputy Assistant Secretaries will review the lists and the supporting classifications using the criteria outlined previously in this document to ensure the validity and completeness of the lists. If any issue is uncovered, the offices of Deputy Assistant Secretaries will work with the appropriate system owner to resolve any and all outstanding questions. Once it has completed the review process, and approved the

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

system owner's submission, the offices of Deputy Assistant Secretaries will forward it to the CIO.

2.4.2 CIO INVENTORY PUBLICATION

Following receipt of the offices of Deputy Assistant Secretaries' submission and the completion of the review process, the CIO will officially publish the comprehensive GSS and MA inventory on the Department's automated inventory management system to ensure it is accessible for reference. The CIO will notify the responsible office of the Deputy Assistant Secretary acknowledging approval of its GSS and MA inventory.

3.0 CHANGES TO THE INVENTORY BETWEEN CYCLES

The information included in the GSS and MA inventory, and even those GSSs and MAs included, may change between inventory cycles. Notification of these changes must be made to the CIO to maintain the appropriate level of security controls for respective GSSs and MAs. Edits 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 deployment and retirement or changes to the mission criticality or information sensitivity levels. For guidance on automated information resource birth and death, see Section 2.1 and subsections above; for guidance on changes to mission criticality or information sensitivity levels, see Section 2.2 and its subsections.

4.0 RELEVANT DEFINITIONS

Application	The use of information resources (information and information technology) to satisfy a specific set of user requirements.
Automated Information Resource	Both government information and information technology.
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 mode 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, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology 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 harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

5.0 REFERENCES

This is a listing of legislation, OMB guidance, and NIST documents relevant to the maintenance of an inventory of HUD General Support Systems and Major Applications.

LAWS

- Privacy Act of 1974, Public Law 93-579
- Computer Security Act of 1987, Public Law 100-235
- Paperwork Reduction Act, Public Law 104-13
- Clinger-Cohen Act, Public Law 104-106
- Freedom of Information Act, Public Law 104-231
- Government Information Security Reform Act, Public Law 106-398
- Federal Information Security Management 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*

NIST PUBLICATIONS

- Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*
- Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
- Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*
- Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*

DEPARTMENT GUIDANCE

- Handbook 2400.25, *HUD ADP Security Program*
- *HUD Certification and Accreditation Process Guide*

Appendix A - GSS and MA Inventory Submission Form

GENERAL SUPPORT SYSTEM (GSS) & MAJOR APPLICATION (MA) INVENTORY SUBMISSION FORM [10]

Owning Organization:_____

Date: _____

Information System Name and Acronym: _____

System Status: ☐ Operational ☐ Under Development

Accreditation Status: ☐ Yes/Date: _____ ☐ No/Scheduled Completion Date: _____

Points of Contact:

Position	Name	Telephone
Information System Owner		
Information Owner		
Information Systems Security Officer		
Primary System Administrator		
Secondary System Administrator		
Designated Approving Authority		

Type of Automated Information Resource ☐ GSS (General Support System) ☐ MA (Major Application)

[10] This form should be completed for every GSS and MA. In addition, completion of this form is highly recommended for each application (non-MA) in order for each system owner to document that all automated information resources are properly evaluated.

Associated URLs:	

Associated IP Addresses:	

Technologies (i.e., Windows, Oracle, etc.):	

Name(s) of System(s) the Information System is Interfaced, Interconnected, or Shares Data With:	

Description of Data and Business Function:	

Mission Criticality: ☐ Critical ☐ Non-Critical

Criticality Justification:	

Information Sensitivity:

Protection Requirements	High	Medium	Low	Justification
Confidentiality				
Integrity				
Availability				

Comments:

_____ _____

Operating Administration Chief Information Officer Date

Appendix B - Sample Inventory Submission Form

SAMPLE INVENTORY SUBMISSION FORM

Owning Organization: Deputy Assistant Secretary for

Date: April 1, 2005

Information System Name and Acronym: General Disbursement System (GDS)

System Status: ☒ Operational ☐ Under Development

Accreditation Status: ☒ Yes/Date: 11/13/2003 ☐ No/Scheduled Completion Date: _____

Points of Contact:

Position	Name	Telephone
Information System Owner	John Brown	202-123-4567
Information Owner	John Brown	202-123-4567
Information Systems Security Officer	Tom Green	202-123-5678
Primary System Administrator	Jane Black	202-123-6789
Secondary System Administrator	Bill White	202-123-7890
Designated Approving Authority	Mary Blue	202-123-8901

Type of Automated Information Resource ☐ GSS (General Support System) ☒ MA (Major Application)

Associated URLs:	http://www.gds.hud.gov

Associated IP Addresses:	123.45.678.90

Technologies (i.e., Windows, Oracle, etc.):	Microsoft Windows 2003; Microsoft SQL Server; Microsoft IIS 6.0

Name(s) of System(s) the Information System is Interfaced, Interconnected, or Shares Data With:	Resides on HUD Intranet General Support System; Interconnected to HUD Financial Management System

Description of Data and Business Function:	GBS data consists of financial information related to distribution of government funds. GBS is used to process disbursements of appropriated funds to state-level agencies

Mission Criticality: ☒ Critical ☐ Non-Critical

Criticality Justification:	GDS is essential to the performance of HUD's funds disbursement operations, which directly support one of the Department's major missions.

Information Sensitivity:

Protection Requirements	High	Medium	Low	Justification
Confidentiality		X		The application is used to process Department financial information that must be safeguarded from public access.
Integrity	X			System information is used in the disbursement of government funds and must be accurate.
Availability			X	Users access the system during normal hours only, and manual processes are available for use when required. The system can be down for 7 days without significant disruption.

Comments:

The General Billing System is currently scheduled for replacement by Universal Disbursement System within the next 12 months, at which time GBS will be retired.

_____ _____

Signature of Approving Official Date