Standard ID.AM: System Inventory

February 11, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	01/15/2019	Initial draft
1.1	02/25/2019	Incorporate comments received from the ED ISSM
1.2	03/5/2019	Incorporate comments received from Principal Offices
1.3	07/22/2019	Clarify that an Authorization to Operate (ATO) is only required for Federal Information Security Modernization Act (FISMA) reportable systems.
1.4	09/11/2019	Revised system types to correspond with best practices for system identification as depicted within the current version of NIST 800-37
1.5	02/12/2020	Reviewed for accuracy and timeliness, added authorization boundary requirements
1.6	2/5/2021	Reviewed for accuracy and timeliness and added Risk Acceptance/Policy Exceptions

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.11 12:39:34 -05'00'

Steven Hernandez **Date**
Director, IAS/Chief Information Security Officer (CISO)

Table of Contents

Table of Contents

1. INTRODUCTION

1.1 Purpose

The *Federal Information Security Modernization Act (FISMA) of 2014* requires federal agencies to maintain a complete inventory of all its major information systems. Office of Management and Budget (OMB) Circular No. A-130, *Managing Information as a Strategic Resource*, requires agencies to identify information technology (IT) assets and maintain an inventory of agency information resources, and it specifically directs each agency to maintain an inventory of its respective information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII). OMB A-130 also requires Departments and agencies to apply these inventory requirements to include information systems used or operated by contractors or other entities on behalf of the Federal government or that collect or maintain Federal information on behalf of the Federal government. The establishment and management of a single authoritative source for all the Department of Education (ED) IT systems within the Cyber Security Assessment and Management (CSAM) tool makes possible a data source that is accurate, reliable, and readily available to all functional components, such as, IT Security, IT Capital Planning and Investment Control, Records Management, Telecommunications, etc.

This document establishes the Department standards for developing, managing, and maintaining an inventory of information technology (IT) systems across ED, primarily for the purposes of satisfying the FISMA system reporting requirements. In doing so, it supersedes any prior documentation establishing such standards.

1.2 Scope

The inventory methodology and processes that support FISMA reporting within this standard pertains to all ED technology-based information systems operated by, funded by or on behalf of ED, including contractor owned, grantee owned, and ED-owned information systems regardless of current lifecycle phase or location. This comprehensive inventory is herein referred to as the ED System Inventory; the inventory is maintained with the Department's system of record for FISMA reporting, CSAM. Information systems that process information that are not in compliance with the requirements of this standard may have their Authorization to Operate (ATO) denied or revoked.

All employees, contract personnel (including grantees) consultants, licensees, and any person or entity providing, operating, maintaining, or supporting any information systems that process ED information are required to comply with this standard.

2. STANDARDS

2.1 System Registration

All Department technology-based information systems must be registered in CSAM. All requests by a Principal Office (PO) to add a new system to the inventory require Enterprise Architecture Technology Insertion (EATI) approval and the submission of a properly completed ED CSAM System Registration form.

2.2 System Authorization Boundaries

The authorization boundary establishes the scope of protection for an information system and includes the people, processes, and information technologies (i.e., system elements) required to support the Department or a PO's missions and business functions. Identifying system authorization boundaries in an accurate and consistent manner is critical to the integrity of ED's System Inventory. OMB A-130, defines an authorization boundary as "all components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected. Boundaries shall be determined in accordance with the current, finalized version of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* and the Department's *System Inventory Methodology and Guidance* and NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems.* The authorization boundary must:

- Describe the information system's internal components and connections to external services and systems and include all federal data collected, stored, processed, generated, transmitted, or disseminated [1]by the system.
- Account for the flow of all federal information, data, and metadata through the system. Metadata identified should be accounted for, adequately protected, and documented within the System Security Plan and applicable system appendices and artifacts.
- Illustrate the scope of control over the system as well as any system components or services that are leveraged from external systems or services.
- Describe interconnections, Application Programming Interfaces (APIs), and other synchronous/asynchronous connections that are used to share federal data, metadata, and other information resources.
- Development environments may be considered outside the authorization boundary if there is no federal information within this environment. If interconnections exist between the development environment and the system's authorization boundary, they must be transparent and provided to the AO for review and risk acceptance.
- Clearly delineate any external systems, components, and services used by the system which are not a part of the system and for which the system typically has no direct control over the application of required security and privacy controls or the assessment of security and privacy effectiveness. This shall be documented using ISA(s) or MOU(s) and interconnection fields within CSAM.
    - Use of MTIPS for internet connectivity must be documented in ISA/MOU and CSAM
- Identify any corporate services such as customer relationship, ticketing, billing systems, etc. which are a subset of external services used by the system or used to support the system. If data that is being transmitted to these corporate services does not affect the confidentiality, integrity and availability of federal information, these services may be excluded from the authorization boundary; and

[1] Federal Information Security Modernization Act (FISMA) of 2014: https://www.govtrack.us/congress/bills/113/s2521

- Provide a diagrammatic illustration of the system's internal services, components, and other devices along with connections to external services and systems.

2.3 System Types

System types determine whether a system is reportable in accordance with FISMA. A FISMA-reportable system is an information system that supports the operations and assets of the Department, and FISMA requires the Department to implement a Department-wide program for information security for those systems. Only one type may be assigned to a system. Only FISMA reportable systems are required to obtain and retain an ED Authorization to Operate (ATO). Table 1 (below) details the ED system types:

Table 1. ED System Types

System Type	Description	FISMA Reportable
System (SYS)	A System (SYS) is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A SYS requires special management oversight because of its importance to the mission of the Department or a PO; its high development, operating, or maintenance costs; or its significant role in the administration of Department or PO programs, finances, property, or other resources. A SYS may include many individual programs and hardware, software, and telecommunications components. These components can be a single software application, or a combination of hardware/software focused on supporting a specific, mission-related function. A SYS may also consist of multiple individual applications if all are related to a single mission function (e.g., payroll or personnel). SYS require a Department specific ATO. A SYS inherits controls from the ED Program and may inherit controls from other programs, systems and subsystems. A SYS may also serve as a Common Control Provider (CCP) and offer controls for inheritance to other systems and subsystems. A SYS may serve as a parent system to one or more subsystems (e.g., child systems) which are included in its authorization boundary, documented in its system security plan (SSP) and supporting appendices, and covered by its ATO memorandum. Previously SYS were identified as General Support Systems (GSS) and Major Applications (MAJ). Cloud Service Providers (CSP) providing Infrastructure as a Service (IaaS), Platform as a Service	Yes

System Type	Description	FISMA Reportable
	(PaaS) and Software as a Service (SaaS) are SYS. Cloud dependent systems are typically SYS as these systems are not included in the CSP's SSP and authorization boundary.	
Subsystem (SUB)	A Subsystem (SUB) is a major subdivision of an SYS consisting of information, information technology, personnel, etc. that perform one or more specific functions. A SUB must be designated as a child of a parent system and must be included in the parent system's authorization boundary, SSP and supporting appendices, and ATO memorandum. As SUBs are authorized through the parent system's ATO, no separate ATO for the SUB is required. A SUB must be assigned a security category in accordance with FIPS 199 which is equal to or less than that assigned to its parent system. SUBs must document system specific information and controls within CSAM. A SUB inherits controls from the ED Program, its parent system, and may inherit controls from other SUBs within its parent system's authorization boundary. In certain situations, a SUB may serve as a CCP and offer controls for inheritance to its parent system and other SUBs within its parent system's authorization boundary. Previously many SUBs may have been labeled as Minor (MIN) applications.	No
Federal Shared Service	A Federal shared service is a business or mission function that is provided for consumption by multiple organizations within or between Federal agencies. Shared services enable the Department of Education to efficiently aggregate resources and systems to improve the quality, timeliness, and cost effectiveness of service delivery. The external agency which owns the service is responsible for authorizing the information to operate and the Department is responsible for explicitly accepting the risk to use the service based on agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of controls in the system or service. All Federal shared services shall be registered in the Department's official FISMA system inventory within CSAM. Federal Shared Services are managed via an Inter-Agency Agreement (IAA) and no explicit ED ATO is required based on the information in an existing authorization package generated by the providing agency. However, information necessary to manage the ED use of the shared service must be documented within CSAM. This includes the shared service's: hosting location, FIPS categorization, information types,	No

System Type	Description	FISMA Reportable
	Information System Owner (ISO), Information System Security Officer (ISSO), Authorizing Official (AO), and Risk Executive. The SSP must also be signed by the designated ISO and ISSO.	
Program	Each PO is represented within CSAM using a program. Programs are used to document and track PO Business Continuity Plans (BCP), document PO specific controls and offer those controls for inheritance to SYS and SUBs within the PO, and document and track Plans of Action and Milestones (POA&Ms) assigned to the PO.	No

2.4 System Transfer or Merger

In the event that a SYS or SUB is transferred from one PO to another PO or merged with another existing SYS or SUB, a Memorandum for the Record (MFR) form must be completed to authorize the transfer and the completed form must submitted to the ED CSAM Support Team to update the system in ED's System Inventory within CSAM. The transfer or merger of a system will invalidate an existing ATO and require rescoping of the authorization boundary. The Information System Owner (ISO) and Information System Security Officer (ISSO) must notify the ED Information System Security Manager (ED ISSM) and request the system be added to the Assessment and Authorization (A&A) schedule.

2.5 System Disposition

To dispose an existing system(s) from ED's System Inventory within CSAM, a Disposal Plan and Disposal Checklist must be submitted to the EATI for review and approval. Requests to decommission a SYS or SUB must also address actions for the underlying systems and/or SUBs. Decommissioned systems are not removed from CSAM for tracking purposes; instead, the system status shall be updated to reflect retired status.

3. RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

4. APPENDIX A: Resources and References

#	Reference Description
1	SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* - https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
2	SP 800-18, *Guide for Developing Security Plans for Information Technology Systems.* - https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final
3	NIST SP 800-39, *Managing Information Security Risk* - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
4	Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 17, 2014 - https://www.federalregister.gov/d/2014-25439
5	OMB A-130, *Managing Information as a Strategic Resource,* July 27, 2016
6	OMB M-17-25: *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* May 19, 2017
7	A FedRAMP Authorization Boundary - https://www.fedramp.gov/assets/resources/documents/CSP_A_FedRAMP_Authorization_Boundary_Guidance.pdf