Standard ID.GV: Required Authorization Documentation

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	08/22/2019	Initial draft
1.1	2/7/2020	Reviewed for accuracy and timeliness
1.2	2/12/2020	Updated to include SSP Checklist and IRP Test
1.3	2/5/2021	Reviewed for accuracy and timeliness. Updated Risk Acceptance and Policy Exception section and NIST SP 800-53 in Appendix A. New CSAM fields were referenced with and clarifications on CSPs and Shared Services.

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.11 12:40:24 -05'00'

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

Table of Contents

1. INTRODUCTION

1.1 Purpose

This document establishes the U.S. Department of Education (ED) standards for developing, managing, and maintaining system security plans (SSP) and establishes requirements for narratives, appendices, and artifacts which support the SSP. In doing so, it supersedes any prior documentation establishing such standards.

1.2 Scope

This standard applies 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. Information systems not in full compliance with the requirements of this standard may have their Authorization to Operate (ATO) denied or revoked.

All employees, contract personnel, third party service providers, 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 Cyber Security Assessment and Management (CSAM)

The CSAM tool is the authoritative source for developing, managing and maintaining the Department's information technology (IT) systems; the system of record for FISMA reporting; and the enterprise tool used to support Cybersecurity Risk Management Framework (CRMF) processes. All Information System Owners (ISO) and Information System Security Officers (ISSOs) must use CSAM to:

- Document, track, and report security Information System FIPS 199 categorization;
- Review, assess, maintain, and report on the status of their system security controls.
- Create, monitor, manage, track and report Plans of Actions & Milestones (POA&Ms) across enterprise-level and at the system level;
- Document and report system life cycle management status from initiation through retirement; and
- Document and report the status of the Authority to Operate (ATO) or Ongoing Authorization.

2.2 System Security Plans

a) All system security plans (SSP) must be CSAM generated. In developing an SSP, system owners must ensure that all required artifacts include narratives, appendices, and all fields within CSAM as well as applicable security control implementation statements are fully and accurately completed and maintained throughout the system life cycle. The SSP Review Checklist must be completed (for all systems except for the Cloud Service Providers (CSPs) and Shared Services) to ensure a complete and thorough SSP in accordance with the *ID.GV SSP Review* Standard.

b) The CSAM-generated SSP, must be approved by the assigned Authorizing Official (AO) or AO delegate (only if it is the first time the SSP is generated (initiation) OR if there a major change), the Information System Owner (ISO) and Information System Security Officer (ISSO).

c) Annually thereafter as part of continuous monitoring and in support of ongoing authorization, the ISO, in coordination with the ISSO, must ensure that the SSP and all supporting narratives and appendices are reviewed and updated. These actions ensure accurate, up-to-date information with sufficient detail is available to enable the AO to identify potential risks to ED systems.

d) Initially and at a minimum annually thereafter, the SSP approval must be documented by digitally signing the CSAM generated SSP signature page. The signed SSP signature page along with the SSP Review Checklist must be uploaded into the CSAM Status and Archive screen as an artifact.

2.2 Required Narratives, Appendices, and Other Documentation

Principal Offices must use Department approved templates available on the IAS Document Library within ConnectED (https://connected.ed.gov/cybersecurity/Documents/Forms/AllItems.aspx) to develop, implement, and maintain the following artifacts which support the SSP and are required to obtain and maintain an ATO. These required documents must be uploaded into CSAM using the locations shown in Table 1.

Table 1. Other Required Documentation

CSAM Location	Document Type	Description	Review Frequency	Signature Requirement	Comments
Narratives	Technical Description	All ISOs must download and complete the current version of the Department approved Technical Description Narrative template from CSAM. This template describes technical characteristics of an information system including network architecture, data flow, and system ports, protocols and services.	Annual	Covered by initial and annual CSAM-generated SSP signature; no separate signature required	Not required from the CSPs nor the Shared services
Narratives	System	All ISOs must download and	Annual	Covered by initial and	Not required

CSAM Location	Document Type	Description	Review Frequency	Signature Requirement	Comments
	Description	complete the current version of the Department approved System Description Narrative template from CSAM. This template describes the functional and technical characteristics of an information system, including system function or purpose, system user types, system components and boundaries, and system environment description.		annual CSAM-generated SSP signature; no separate signature required	from the CSPs nor the shared services
Appendix Q2; Status & Archive	Configuration Management Plan (CMP)	To satisfy the most current revision of NIST SP 800-53, Control CM-9, all systems must use the current version of the Department approved template which is available on ConnectED to develop, document, and implement a Configuration Management Plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and	Annual	Covered by initial and annual CSAM-generated SSP signature; no separate signature required	Not required from the CSPs nor the shared services

CSAM Location	Document Type	Description	Review Frequency	Signature Requirement	Comments
		procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; and c. Defines the configuration items for the information system and places the configuration items under configuration management;			
Appendix L; Continuity & Incident Response	Information System Contingency Plan (ISCP)	To satisfy NIST SP 800-53, Rev 4 Control CP-2, all ISOs must use the current version of the Department approved template to develop, document, and implement an ISCP for the information system that: 1. Identifies essential missions, business functions, and associated contingency plan requirements; 2. Provides recovery objectives,	Annual	Information System Owner (ISO), and Information System Security Officer (ISSO)	Not required from the CSPs nor the shared services

CSAM Location	Document Type	Description	Review Frequency	Signature Requirement	Comments
		restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented;			
Continuity & Incident Response	Contingency Plan Test Results (CPT)	To satisfy NIST SP 800-53, Rev 4 Control CP-4, all ISOs must use the current version of the ISCP to document results of annual contingency plan testing (e.g., ISCP, Appendix K).	Annual	Covered by initial and annual ISCP signatures	Not required from the CSPs nor the shared services
Appendix O; Continuity & Incident	Incident Response Plan (IRP)	To satisfy NIST SP 800-53, Rev 4 Control IR-8, all	Annual	Covered by initial and annual CSAM-	Not required from the

CSAM Location	Document Type	Description	Review Frequency	Signature Requirement	Comments
Response		ISOs must use the current version of the Department approved template to develop, document, and implement an Incident Response Plan for the information system that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response		generated SSP signature; no separate signature required	CSPs nor the shared services

CSAM Location	Document Type	Description	Review Frequency	Signature Requirement	Comments
		capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;			
Appendix S	Hardware Listing	To satisfy NIST SP 800-53, Rev 4 Control CM-8, all systems must use the current version of the Department approved Hardware List template to document system hardware.	Quarterly	Covered by initial and annual SSP signature; no separate signature required	Not required from the CSPs nor the shared services
Appendix T	Software Listing	To satisfy NIST SP 800-53, Rev 4 Control CM-8, all systems must use the current version of the Department approved Software List template to document system software.	Quarterly	Covered by initial and annual SSP signature; no separate signature required	Not required from the CSPs nor the shared services
Appendix V2; Privacy	Privacy Threshold Analysis (PTA)	All systems must use the current version of the Department approved PTA.	Every two years	ISO, Privacy Safeguards Division, and Senior Agency Official for Privacy (SAOP)	
Appendix V3; Privacy; System Identification	Privacy Impact Assessment (PIA), if required	To comply with Department policy, OM 6-108, *Privacy: Section 208 of the E-*	Every two years	ISSO, ISO, Privacy Safeguards Division, and	Please consult the Department SAOP for

CSAM Location	Document Type	Description	Review Frequency	Signature Requirement	Comments
		Government Act of 2002 Policy and Compliance and NIST SP 800-53, Rev 4 Control PL-5*,* when the PTA shows that a PIA is necessary, systems must use the current version of the Department approved PIA.		Senior Agency Official for Privacy (SAOP)	CSPs and Shared Services
Relationships Section	Memoranda of Understanding (MOU), Interconnection Security Agreements (ISAs), Inter-Agency Agreements (IAA), and Service Level Agreements (SLAs) – if required	Systems which provide controls to other dependent systems or receive controls from other systems (GSS/ Parent system) must complete the current version of the Department's MOU template. To comply with NIST SP 800-53, Rev 4 Control AC-20, Use of External Information Systems and Department Directive OPEPD 1-101, *Interagency Agreements,* terms and conditions must be established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized	Annual	Based upon connection type and Department template	

CSAM Location	Document Type	Description	Review Frequency	Signature Requirement	Comments
		individuals to access an information system from external information systems; and process, store, or transmit organization-controlled information using external information systems. Principal Offices must complete the current version of the Department's approved template for Inter Agency Agreements (IAA) or Interconnection Security Agreements (ISA) to establish and approve these terms and conditions. Completed MOUs, IAAs , ISAs and SLAs must be uploaded into CSAM (if applicable).			
Appendix W; Continuity & Incident Response	Business Impact Analysis (BIA)	To satisfy NIST 800-34 Revision 1. The BIA is a key step in implementing the CP controls in NIST SP 800-53 and in the contingency planning process overall. All systems must use the current version of	Annual	Information System Owner (ISO), and Information System Security Officer (ISSO)	Not required from the CSPs nor the shared services

CSAM Location	Document Type	Description	Review Frequency	Signature Requirement	Comments
		the Department approved template which is available on ConnectED to develop and document a BIA which; 1. Determines mission/business processes and recovery criticality along with outage impacts, estimated downtime, and recovery time objectives; 2. Identify resource requirements including facilities, personnel, equipment, software, data files, system components, and vital records and; 3. Identify recovery priorities for system resources.			
Status & Archive and Appendix CL: SSP Review Checklist	SSP Checklist	To ensure system security information is accurate, thorough and timely in accordance with the *ID.GV SSP Review*	Annual	Information System Owner (ISO), and Information System Security	Not required from the CSPs nor the shared

CSAM Location	Document Type	Description	Review Frequency	Signature Requirement	Comments
		standard.		Officer (ISSO)	services
Continuity & Incident Response	Incident Response Plan Test Results (IRPT)	To satisfy NIST SP 800-53, Rev 4 Control IR-3, all ISOs must use the current version of the IRP to document results of annual incident response plan testing.	Annual	Covered by initial and annual IRP signatures	Not required from the CSPs nor the shared services
Appendix P; Status & Archive	Disaster Recovery Plan (DRP)	To establish comprehensive procedures to restore operability of the system quickly and effectively at an alternate site in the event of a major hardware or software failure or destruction of facilities.	Annual	Information System Owner (ISO), and Information System Security Officer (ISSO)	Not required from the following: CSPs, the shared services, the sub systems and the Low FIPS 199 categorized system

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).

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	SP 800-39, *Managing Information Security Risk* - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
4	SP 800-53 (as amended), *Security and Privacy Controls for Federal Information Systems and Organizations* - https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
5	Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 17, 2014 - https://www.federalregister.gov/d/2014-25439
6	OMB A-130, *Managing Information as a Strategic Resource,* July 27, 2016
7	OMB M-17-25: *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* May 19, 2017