Standard ID.GV: System Security Plan (SSP) Review

February 11, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.11 12:38:00 -05'00'

Steven Hernandez **Date**

Director, IAS/Chief Information Security Officer (CISO)

Revision History

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

Version	Draft Date	Summary of Changes
0.1	09/04/2019	Initial draft
0.2	10/03/2019	ISSM revisions
0.3	10/09/2019	CISO Revisions
0.4	10/28/2019	ISSM Revisions
1.0	10/29/2019	CISO Revisions and Signature
1.1	01/22/2020	CISO Revisions and Signature
1.2	02/11/2020	CISO Revisions and Signature
1.3	1/22/2021	Underwent annual policy review for accuracy and timeliness. Updated SSP review checklist and added Risk Acceptance and exception section.

Table of Contents

1 INTRODUCTION

The completion of a System Security Plan (SSP) is required by the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources and Public Law 113-283, the Federal Information Security Modernization Act (FISMA). The Department of Education is required to identify each computer system containing sensitive information to prepare and implement a plan for the security and privacy of those system(s). In accordance with NIST SP 800-37 Rev. 2 and NIST SP 800-53 (as amended). The objective of system security planning is to improve protection of Information Technology (IT) resources. All federal system(s) have some level of assurance and require protection. The System Security Plan memorializes the due care and due diligence in protecting the Department's systems.

The security plan is viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It reflects input from management responsible for the system, including information system owners, the system operator, the information system security manager, information system security officer, and system administrators. The system security plan delineates responsibilities and expected behavior of all individuals who access the system.

1.1 Purpose

The purpose of the system security plan is to describe the controls and critical elements in place or planned for the system of interest, based on the latest versions of:

- NIST Special Publication (SP) 800-53 (as amended), Recommended Security Controls for Federal Information Systems,
- FIPS 200, Minimum Security Requirements for Federal information and Information System.
- NIST SP 800-30, Risk Management Guide for Information Technology Systems,
- NIST Special Publication (SP) 800-37, rev.2, Guide for Applying the Risk Management Framework to Federal Information Systems.
- NIST SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

The SSP identifies applicable security control as either in place (implemented) or planned. This SSP follows guidance contained in NIST Special Publication (SP) 800-18, Guide for Developing Security Plans for Federal Information Systems, and the Department of Education Cybersecurity Risk Assessment and Authorization Guide.

This document will assist reviewers in assessing if the SSP meets the minimum Department requirements for signature.

1.2 Scope

The standards established in this document apply to all appointed Information System Owners (ISO) and Information System Security Officers (ISSO) for all Department systems including High-Value Assets (HVAs), High and Moderate FIPS-199 categorized systems in addition to OCIO FIPS-199 Low categorized systems. This standard does not apply to the Office of Inspector General (OIG).

2 SSP Review Checklist

The SSP Review Checklist must be completed (for all systems as included in the scope section (except for the Cloud Service Providers (CSPs) and Shared Services) to ensure a complete and thorough SSP.

The following table identifies the SSP review checklist of the standards for the Authorizing Official acceptance:

Checklist Item	Satisfied?
1. Verify and validate all referenced policies, procedures, and standards and instructions represent the latest versions. E.g., no existence of OCIO-01 should be documented. It was superseded by OCIO- 3-112. Ensure referenced NIST documents and standards are current: o NIST Special Publication (SP) 800-18, rev.1, Guide for Developing Security Plans for Information Technology Systems o NIST Special Publication (SP) 800-53A (as amended)., Assessing Security and Privacy Controls in Federal Information Systems and Organizations o NIST FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems o Office of Management and Budget (OMB) Circular A-130 o NIST Special Publication (SP) 800-37, rev.2, Guide for Applying the Risk Management Framework to Federal Information Systems o NIST Special Publication (SP) 800-39, Managing Information Security Risk o NIST Special Publication (SP) 800-53(as amended), Security and Privacy Controls for Federal Information Systems and Organizations	☐
2. Verify and validate any reference to any GSS (internal or external) is accurate. This includes specifically validating a host GSS is presently authorized and fully documented in CSAM. The GSS must be appropriate FIPS categorization and have a current authorization. Additionally, verify and validate no existence of references to non-existent GSS, for example: EDUCATE Infra GSS (NTT Data, Dell, or Plano TX), the Department's former General Support System was replaced by ETS-Infra-GSS. Also, FSA VDC references must be replaced by NGDC, etc.	☐

3. Ensure no references to contract names exist *in the place of* system names in the SSP and associated documents such as the contingency plan, privacy impact assessment or incident response plan. (e.g. PIVOT, PIVOT-H, PIVOT-I, PIVOT-P, PIVOT-N, PIVOT-P, AT&T, GDIT, IBM, Perspecta, etc.)	☐
4. Verify and validate accurate organizational titles are consistent with current organizational charts. For example, for an OCIO system, verify no existence of Information Technology Services (ITS) within the document, also known as OCIO ITS. The correct name after the re-org is OCIO Enterprise Technology Services (ETS).	☐
5. Ensure no conflict of interest exist in assigned roles. E.g., Information System Owner (ISO) and Information System Security Officer (ISSO) are not identified as the same person.	☐
6. "Risk Executive" is identified by the role of the Department CISO (currently Mr. Steven Hernandez).	☐
7. Authorizing Official (AO) for all High-Value assets, all FIPS-199 High systems, and all FIPS-199 Moderate systems is the Department CIO (currently Mr. Jason Gray). Ensure that the AO for FIPS-199 Low Systems is reflected in the latest delegation **memo**.	☐
8. Confirm thorough, current and accurate system description and system diagram (which must be part of the System and Technical narratives) These descriptions and diagrams must explain the system boundary, interconnected systems, sub systems, and data flows.	☐
9. FIPS 199 Security categorization must be the highest water mark of the Confidentiality, Integrity and Availability (CIA) of the data processed, stored, or transmitted by the system.	☐
10. Information Types are selected and documented in accordance with NIST 800-60 as amended and any data type listed as "Other" must include a full analysis as to why it does not conform with 800-60. This new data type must be authorized by the Department CISO through the ISSM.	☐
11. Information system type for FISMA Reportable systems fall into the category of (System/subsystem) and are correctly entered in CSAM.	☐
12. System Locations are identified (Mgmt. Office and Primary location at a minimum.) Ensure data center location is accurately documented.	☐

13. Verify and validate that all referenced Interconnection Security Agreements (ISAs), Memorandum of Understanding (MOU), Inter Agency Agreements (IAAs) and Computer Matching Agreements (CMAs) are up to date and reference correct roles, systems and organizations.	☐
14. Verify and validate that the SSP is free from grammatical, spelling, and formatting errors. Confirm that SSP was generated from CSAM.	☐
15. Verify and validate that any applicable Privacy Threshold Analysis, (PTA) Privacy Impact Assessment (PIA) and System of Records Notice (SORN) is up to date.	☐
16. Ensure security control consistency, by validating and verifying controls are mapped to their corresponding mandatory documentation. For example, the Information System Contingency Plan (ISCP) must be consistent with the "CP" controls, the Configuration Management Plan (CMP) must be consistent with the "CM" controls, The Incident Response Plan (IRP) must be consistent with the "IR" controls and the Disaster Recovery Plan (DRP) and Business Impact Analysis (BIA) must be consistent with the "CP" and "CM" controls).	☐
17. All fields below have been reviewed and determined to reflect the accurate and current status of the system:	☐

Document/ Field/ Question	Section in CSAM
External URL (if applicable)	System Information/ System Identification/ Agency Defined Data Items
Internal URL	System Information/ System Identification/ Agency Defined Data Items
External IP address(es) (if applicable)	System Information/ System Identification/ Agency Defined Data Items
Internal IP address(es) (optional)	System Information/System Identification/ Agency Defined Data Items
System a Cloud Service Provider (CSP) (Q4)	System Information/System Identification/ Agency Defined Data Items
System a Cloud Dependent System (Q5)	System Information/System Identification/ Agency Defined Data Items
System an External Shared Service (Q6)	System Information/System Identification/ Agency Defined Data Items
Quantity of PII Records (Q11)	System Information/ System Identification/ Agency Defined Data Items
Is this an External or Internal Facing System (Q13)	System Information/ System Identification/ Agency Defined Data Items
System TIC compliant (Q15)	System Information/ System Identification/ Agency Defined Data Items
System an HVA (Q16)	System Information/ System Identification/ Agency Defined Data Items
UII Code	System Information/ System Identification/ Funding Information
Investment Name	System Information/ System Identification/ Funding Information
OMB Exhibit	System Information/ System Identification/ Funding Information
System Description	System Information/ Narratives
Technical Description	System Information/ Narratives

Business Impact Analysis	System Overview/ Continuity & Incident Response
Hardware Listing	System Information/ Appendices/ Appendix "S"
Software Listing	System Information/ Appendices/ Appendix "T"
ConMon Briefing Slide Deck (as applicable)	System Information/ Appendices/ Appendix "U"
ISSO Appointment Memo	System Information/ Appendices/ Appendix "X"
ISO Appointment Memo	System Information/ Appendices/ Appendix "Y"
ISO and ISSO Briefing Checklist	System Information/ Appendices/ Appendix "Z"
Information Types	System Information/ Information Types
Backup Location	System Information/ Locations

18. SSP is signed by both the ISO & ISSO	☐

ISO signature: _____ Date: _____

ISSO signature: _____ Date: _____

3. RISK ACCEPTANCE/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: ACRONYMS

AO	Authorizing Official
BIA	Business Impact Analysis
CISO	Chief Information Security Officer
CMA	Computer Matching Agreement
CMP	Configuration Management Plan
DRP	Disaster Recovery Plan
ETS	Enterprise Technology Services
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
HVA	High-Value Asset
IAA	Inter Agency Agreement
IAS	Information Assurance Services
IRP	Incident Response Plan
ISCP	Information System Contingency Plan
ISO	Information System Owner
ISSO	Information Systems Security Officer
NIST	National Institute of Standards and Technology
OCIO	OCIO Program
PIA	Privacy Impact Assessment
PIVOT	Portfolio of Integrated Value-Oriented Technologies
SORN	System of Records Notification
SSP	System Security Plan