Standard ID.RM: Cybersecurity Risk Management Framework (CRMF)

February 10, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

Revision History

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

Version	Draft Date	Summary of Changes
1.0	08/21/2019	Initial draft
1.1	2/7/2020	Updated to include Department cyber risk tolerance & appetite
1.2	2/12/2020	Reviewed for accuracy and timeliness,
1.3	3/19/2020	Updated Section 2.5 Authorize Information System
1.4	6/22/2020	Updated Section 3 (Policy Exceptions) Corrected Risk Appetite/Tolerance
1.5	2/2/2021	Underwent annual policy review for accuracy and timeliness and added in exceptions and waivers and updated Appendix A for NIST SP 800-53

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.10 19:02:20 -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 develop, document and implement an agencywide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Office of Management and Budget (OMB) Circular No. A-130, *Managing Information as a Strategic Resource*, requires agencies to ensure adequate security, commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. OMB A-130 also requires departments to establish a minimum set of controls to be included in federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.

The *Department of Education Life Cycle Management Framework ACS Directive OCIO 1-106* applies to the development, acquisition, implementation, maintenance and disposal of IT solutions regardless of cost, complexity and time constraints. A critical supporting component to the lifecycle of an information system operating in the Department's environment is cybersecurity risk management. Risk management recognizes that risk in complex IT systems cannot be eliminated, and that the owners and defenders of systems must decide what risks to remove, what is impractical to remove, and what must be managed. To do this, system owners must understand, assess and prioritize their risks.

The Risk Management Framework (RMF) is a set of information security policies and standards for the federal government developed by The National Institute of Standards and Technology (NIST). The RMF is covered specifically in the current, finalized versions of the following NIST publications:

- Special Publication 800-37 rev 2, *"A System Life Cycle Approach for Security and Privacy"*, describes the formal RMF assessment and authorization process.
- Special Publication 800-53 rev 4, *"Security and Privacy Controls for Federal Information Systems and Organizations"*, describes a structured process for integrating information security and risk management activities into system development from initiation to decommissioning. An organization will select system security and privacy controls and apply them organization-wide via an information security program, where the organization considers how to execute the framework at appropriate risk management levels.

This document establishes the Department standards for information technology (IT) systems across the Department of Education (ED), based upon the above guidance, to categorize the systems' risk impact, select security controls, implement security controls, assess risk, authorization to operate, and continuous monitoring within the Department's operational environment.

1.3 Scope

The methodology and processes that support cyber risk management 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 methodology is herein referred to as the ED CRMF. All cyber risk and system inventory information is maintained with the Department's system of record for FISMA reporting, Cyber Security Assessment and Management (CSAM) tool. Information systems that process, store, or disseminate 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.

The overarching objectives of the ED CRMF are to ensure that:

- Cybersecurity risks are identified and managed on an ongoing basis across the Department.
- ED Authorizing Officials (AO) and Department leadership are provided with the necessary information regarding cybersecurity risks to make efficient, cost-effective, risk management decisions about assets, systems, individuals, and processes that support their missions and business functions explicitly accepting the risks of operating the information system or service

1.4 Cybersecurity Framework Integration

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) in focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. The Framework consists of three parts:

- the Framework Core,
- the Implementation Tiers, and
- the Framework Profiles.

The CSF Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual and organizational risk profiles.

The Department's implementation of the CSF is reflected through policy and standards aligned to CSF Categories while CSF implementation status is reported through the ED CSF Risk Scorecard. The scorecard is used to define risk profiles to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerance/appetite, and resources. The risk levels within the scorecard provide a mechanism for Department stakeholders to view and understand the characteristics of their approach to managing cybersecurity risk. This is beneficial in prioritizing and achieving cybersecurity objectives across the Department.

1.5 Risk Management and the CSF

Risk Management, through the Cybersecurity Framework, is the ongoing process of identifying, assessing, and responding to risk. To manage risk, the Department assesses likelihood that an event will occur and the potential resulting impacts. With this information, executive leadership can determine the acceptable level of risk for achieving the Department's objectives and can express this as the organizational risk appetite.

With an understanding of risk appetite, the Department prioritizes cybersecurity activities, enabling leadership to make informed decisions about cybersecurity expenditures. The implementation of process in support of this standard provide the Department the ability to quantify and communicate adjustments to cybersecurity programs and establish appropriate procedures to mitigate risk, transfer risk, avoid the risk, or accept the risk, depending on the potential impact to the delivery of critical services. The CSF uses risk management processes, which enable leadership to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to allow the Department to select target states for cybersecurity activities that reflect desired outcomes.

2. STANDARDS

2.1 Information System Security Officer (ISSO) Appointments

For systems to ensure compliance to the directives established within this standard, the Department Information System Security Manager (ISSM) will formally appoint an Information System Security Officer (ISSO) to support risk management activities for each system. Dependent upon the size and complexity of the system and competing mission priorities, an Alternate-ISSO may also be appointed in support of the system. The Information System Owner (ISO) will work with the designated ISSO to ensure the information system is properly registered in CSAM.

2.2 System Registration

As established in *Standard ID.AM System Inventory*, the Department maintains a comprehensive system inventory in the CSAM system. CSAM is the authoritative source of the Department's system inventory, with accurate data describing information systems. All information systems must register in CSAM prior to the execution of ED CRMF activities to ensure the appropriate level of information is captured and understood at all operational and Principal Office levels.

The system information captured in CSAM must always reflect the current state of the information system throughout its lifecycle, in order to serve as a basis for near real-time risk decisions. The registration of the system in CSAM will trigger planning activities such as system security categorization, control selection, implementation, Independent Security Assessments, and common control authorizations, and continuous monitoring required to support an AO's decision to grant an ATO.

2.3 Categorize Information System

Prior to categorizing a system, the system must be registered in CSAM and the authorization boundary must be defined [1]. Principal Offices must use CSAM to conduct, document, track, and report security categorization. Based on that system boundary, all information types associated with the system must be identified and cataloged in CSAM. Information about the system and its mission, its roles and responsibilities as well as the system's operating environment, intended use and connections with other systems must be documented as they may affect the final security impact level determined for the

[1] Standard ID.AM System Inventory

information system. System categorization shall be determined in accordance with the current, finalized version of Federal Information Processing Standards (FIPS) Publications 199, *Standards for Security Categorization of Federal Information and Information Systems* and NIST special publication 800-60 as amended.

2.4 Select Security Controls

Security controls must be selected in accordance with baseline requirements, established within the current, finalized version of NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, as determined by the systems' security categorization. Security controls represent the management, operational and technical safeguards or countermeasures employed within an information system that protect the confidentiality, integrity and availability of the system and its information.

2.4.1 Common Control Providers

Common Control Providers (CCP), including cloud service providers, general support systems and programs, must document and provide security controls for inheritance within CSAM for all dependent systems, where the CCP has executed a Memorandum of Understanding or Service Level Agreement to provide the controls. Additionally, CCPs must create documentation regarding common controls that may be inherited by other information systems available to all ISOs for review, consideration, and incorporation into their respective System Security Plans (SSP). CCPs must obtain an ATO with the Department to ensure risk decisions can be made effectively and appropriately based upon security controls in place for the CCP, particularly when offered for inheritance.

Inherited common controls shall be explicitly identified and traceable from the dependent information system's security plan. ISOs must refer to and leverage the CCP's SSP and authorization package to ensure that the common control does, in fact, satisfy the need of a specific information system. Principal Offices should assign a hybrid status to security controls when one part of the control is common, and another part of the control is system specific.

2.4.2 System-Specific Controls

The security categorization of an information system establishes the baseline from which system-specific controls can be identified. ISOs and ISSOs must tailor system-specific controls to meet the needs of the business / mission process enabled by the information system. This may require the ISO and ISSO to identify additional controls and/or security control enhancements, as well as conduct risk analyses to determine whether hybrid controls or compensating controls are required to address any potential deficiencies in planned security control implementations.

The selection of system-specific security controls must be clearly documented as part of the SSP, with traceability to the requirements and supporting rationale for any selection decisions made. The description of security controls to be implemented must include sufficient detail to enable validation and assessment of the actual control implementation.

2.3 Implement Security Controls

The implementation of security controls must be integrated with a project or program's system and software engineering processes. It shall be accomplished in concert with the design and implementation of the overall system architecture with consideration for best practices and secure coding techniques, and in accordance with the Department's Enterprise Architecture (EA) and the Enterprise Program Management Review (EPMR) process.

2.4 Assess Security Controls

Assessing the security controls requires using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. Information systems within the Department's FISMA inventory must be assessed to determine the extent of operational risk posed to the organization and its mission in order to be granted an ATO from the system AO. Non-FISMA reportable subsystems are assessed under the ATO for the parent FISMA reportable system. Principal Offices must use CSAM to document, assess, and report on the status of required security controls. In order for a system to be assessed, the ISO must complete all required authorization documentation as established in the Department Standard *ID.GV Required Authorization Documentation*

Federal Shared Services provided by other agencies are not assessed within the Department in accordance with *ID.AM System Inventory Standard*. Federal Shared Services are authorized via an Inter-Agency Agreement (IAA) and no explicit Department ATO is issued.

2.4.1 Security Impact Analysis

In the event of a major system change, including infrastructure, use cases, security control changes and software modifications, a Security Impact Analysis (SIA) must be conducted by qualified system support staff (e.g. system administrators, developers) to determine the extent to which changes to the information system affect the security posture of the system. Because information systems are typically in a constant state of change, it is essential to understand the impact of changes on the functionality of existing security controls and in the context of the Department's risk appetite and tolerance. Security Impact Analyses shall be incorporated into the documented configuration management process for all information systems. The results of a SIA determine whether a change to an existing system is minor or significant and what residual risk, if any, needs to be treated as part of the change.

The assessment of the security impact must be conducted, analyzed and evaluated for adverse impact on security, prior to implementation, but also in the case of emergency / unscheduled changes. Once the changes are implemented and tested, a Security Control Assessment is performed to ensure that the changes have been implemented as approved, and to determine residual risks.

2.5 Authorize Information System

The explicit acceptance of risk is the responsibility of the designated AO and cannot be further delegated to other officials. The AO must consider many factors when deciding if the risk (security, privacy and supply chain) to the Principal Office and Department operations (including mission, functions, image, and reputation) and assets, individuals, other organizations, or the Nation, is acceptable. Balancing security and privacy considerations with mission and business needs is paramount to achieving an acceptable risk-based

authorization decision. Risks identified through risk assessments (both initial and ongoing) and continuous monitoring, must be catalogued and tracked in CSAM as Plans of Action and Milestones (POA&Ms). CSAM must be utilized to provide tracking and statuses for any failed controls identified during an assessment. Principal Offices must use CSAM to create, monitor, manage, track and report POA&Ms across enterprise-level initiatives and at the system level. CSAM must be used to document and report the status of the ATOs or Ongoing Security Authorization (OSA)[2] activities.

The respective AO must review the authorization boundary, security categorization results and decision, System Security Plan (SSP), assessment out briefs and reports, authorization package and POA&Ms, and determine whether the identified risks need to be mitigated prior to authorization. The AO should consult with the ISO, ISSO, and security and privacy control assessors and gain input from the Department's CISO and Senior Agency Official for Privacy (SAOP) prior to making the final authorization decision. The authorization decision shall be clearly identified in a formal authorization memorandum that is signed by the AO. Authorization decisions resulting from the risk assessment process shall be conveyed to the ISO and ISSO. Types of authorization decisions for ED systems and common control providers are detailed in the table below.

Authorization Decision	Description
Authorization to Operate (ATO)	Issued after an AO has determined the risk to Department operations and assets, individuals, other organizations, and the nation is acceptable. An ATO is issued for a specified period in accordance with the terms and conditions established by the AO. An authorization termination date is established by the AO as a condition of the ATO to indicate when the ATO expires. The authorization termination date may be adjusted at any time by the AO to reflect an increased level of concern regarding the security and privacy posture of the system. The AO may choose to include operating restrictions such as limiting logical and physical access to a minimum number of users; restricting system use time periods; employing enhanced or increased audit logging, scanning, and monitoring; or restricting the system functionality to include only the functions that require live testing. The AO considers results from the assessment of controls that are fully or partially implemented. Additionally, an adverse event could occur that triggers the need to review the authorization to operate. This includes major system changes and security posture impacts analyzed and reported through risk scoring as identified ongoing information security continuous monitoring (ISCM) activities.
Denial of Authorization	Issued for an information system in which the AO has determined the risk to Department operations (including image & reputation) and assets, individuals, and other organization is at an unacceptable level after reviewing the risk assessment and authorization package and any additional inputs provided. This means that the information system is not authorized to operate and cannot be placed into operation within the Department's operating environment. If the system is currently in operation, all activity is halted. A Denial of Authorization indicates that there are major weaknesses or

[2] Standard DE.CM Ongoing Security Authorization

Authorization Decision	Description
	deficiencies in the security controls employed within or inherited by the information system.

2.6 Continuous Monitoring and Ongoing Security Authorization

Following the issuance of an ATO, ISOs must conduct continuous monitoring activities to identify and remediate risks while monitoring changing conditions which could potentially affect the ability to conduct core missions and business functions. ISSOs shall coordinate with ISOs to address and remediate POA&M action items and track completion dates as required by the Department ISSM. POA&Ms shall be managed and maintained in CSAM. ISSOs shall review open POA&Ms regularly to determine which items require additional attention or resources and report to the AO any action item completion date not met.

Systems which have been evaluated by the Office of the Chief Information Officer (OCIO) as having sufficient combined manual and automated system-level continuous monitoring in place and adhere to the control assessment schedules, delivery of control artifacts, and requirements detailed within the Department's Ongoing Security Authorization Guidance may operate under an OSA[3]

2.7 Managing Risk – Risk Appetite and Tolerance

This standard memorializes the cybersecurity risk tolerance and risk appetite as it relates to the Department's Enterprise Risk Management (ERM) program. Risk appetite and tolerances are defined through the ED CSF Risk Scorecard ratings. Cyber risk is calculated through ongoing security & privacy assessments and monitoring using defined and proven methodologies both quantitative metrics and qualitative risk elements, as represented in the ED CSF Risk Scorecard. Cyber risk appetite and risk tolerance are determined through identifying and managing potential cyber risks, quantifying their potential impact, and used to prioritize risk management activities effectively.

The Department's cybersecurity risk appetite represents the target risk profile for a system, principle office and the extent to which the Department is comfortable with the accepting ongoing persistent cybersecurity risk. The risk appetite coincides with the calculated risk level of '2 – Low Risk' on a scale of '0-3' within the ED CSF Risk Scorecard. Therefore, systems are expected to maintain a minimum level of '2' as the risk appetite while the system is operational. Systems and system stakeholders must strive for level 3 by performing actions to mitigate risks and vulnerabilities.

The cyber risk tolerance represents the amount of cybersecurity risk the Department is prepared to accept in pursuit of its mission/business. For systems operating within the Department's IT environment, the risk tolerance coincides with the calculated risk level of one point on a scale from '0-3' within the ED CSF Risk Scorecard. Therefore, systems may temporarily perform at a '1 – Moderate/Low Risk' as mission and

[3] Standard DE.CM Ongoing Security Authorization

business necessity demand. The formal process for cyber risk tolerance acceptance is the Department's security authorization process for issuing and maintaining authorizations to operate (ATO.)

The Department's Cyber Risk program coordinates with the Department's ERM function to maintain awareness of the cyber risk of the organization. Tolerance and appetite information are provided to all levels of the organization through updates with a frequency determined by the Governance, Risk and Policy Branch in coordination with the Department's ERM function.

2.8 System Transfer or Merger

As established in *Standard ID.AM System Inventory*, in the event that an information system is transferred from one Principal Office to another Principal Office or merged with another existing system, a Memorandum for the Record (MFR) form must be completed to authorize the transfer and the completed form submitted to the ED CSAM Support Team to update the system in ED's FISMA System Inventory within CSAM.

2.9 System Disposition

As established in *Standard ID.AM System Inventory*, to remove an existing system(s) from ED's FISMA System Inventory within CSAM, a Disposal Plan and Disposal Checklist must be submitted to the EATI for review and approval. Requests to decommission a MAJ or GSS must also address actions for underlying SUBs/MINs. Decommissioned systems are not removed from CSAM for tracking purposes; instead the system status is updated to reflect retired.

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	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* -
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
8	NIST Cybersecurity Framework, Version 1.1, April 16, 2018 https://www.nist.gov/cyberframework/framework