Information Technology (IT) System Security Assessment and Authorization (CA) Standard

January 31, 2023

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 **IAS_Governance@ed.gov.**

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2023.01.30 15:20:35 -05'00'

Steven Hernandez

Director, IAS/Chief Information Security Officer (CISO)

Revision History

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

Table 1: Revision History

Version	Date	Summary of Changes
1.0	12/22/2021	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/14/2022	Update to incorporate feedback from Information Assurance Services (IAS), Governance, Risk and Policy (GRP) Team.
1.2	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with the EO.
1.3	1/31/2023	Annual Review. Minor format changes. Addition of Control Overlays CA-2 ED-08, CA-2 ED-09, and CA-8 ED-06. Control Overlay CA-7 ED-02 clarified. Appendix B updated to include Ongoing Authorization to Operate (OATO). Clarified Ongoing Security Authorization (OSA) entrance and exit criteria in Appendix C.

Contents

1 INTRODUCTION

This governance document establishes Department information technology (IT) system maintenance controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders, Emergency Orders, Binding Operational Directives, and Department Administrative Communications System (ACS) directives and policies. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing regulation Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as baseline information system controls.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these maintenance control standards.

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2 STANDARDS

The Department standards for IT system security assessment and authorization controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS 199 categorization level (e.g., Low (L), Moderate (M) and High (H)) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS 199 impact-level or privacy baseline. In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA).

This standard directly supports the Department's integration of the NIST Cyber Security 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. Refer to Appendix A for a summary of controls by baseline and corresponding NIST CSF categories and subcategories.

2.1 CA-1 Policy and Procedures (P, L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy* a Department-level security assessment and authorization policy (e.g., this document) that:

a. address's purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

c. authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as OCIO: 3-112/ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) are designated to manage the development, documentation, and dissemination of the Department-level IT system security assessment and authorization policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws,

executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

The Office of the Chief Information Officer (OCIO), Information Assurance Services (IAS) manage the development, documentation, and dissemination of the Department-level IT system security assessment and authorization standard operating procedures in support of this standard. IAS Branch Chiefs shall review security assessment and authorization procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office personnel including Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of the Department's security assessment and authorization policy and the associated controls. The ISO and ISSO shall review security assessment and authorization procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

2.2 CA-2 Control Assessments (P, L, M, H and Control Overlay)

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted

b. Develop a control assessment plan that describes the scope of the assessment including:

    1. Controls and control enhancements under assessment
    2. Assessment procedures to be used to determine control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities

c. Ensure the control assessment plan is reviewed and approved by the Authorizing Official (AO) or designated representative prior to conducting the assessment

d. Assess the controls in the system and its environment of operation at least annually (i.e., each fiscal year) using independent assessors, self-assessments or ongoing security control monitoring/ongoing security authorization processes to determine the extent to which the

controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to Chief Information Security Officer (CISO), AO, Chief Privacy Officer/Senior Agency Official for Privacy (CPO/SAOP), ISO, and ISSO.

Control Overlay CA-2 ED-01 (L, M, H): Assess information systems within the Department's FISMA inventory to determine the extent of operational risk posed to the organization and its mission in order to be granted an Authorization to Operate (ATO) from the AO.

Control Overlay CA-2 ED-02 (L, M, H): Include non-FISMA reportable subsystems in the assessment of the parent FISMA reportable system.

Control Overlay CA-2 ED-03 (L, M, H): Use the Cyber Security Assessment and Management (CSAM) tool to review, assess, maintain, track and report on the status (e.g., implemented, not implemented) of required controls (e.g., baseline controls and control overlays).

Control Overlay CA-2 ED-04 (L, M, H): Complete all required authorization documentation as established in the Information Technology System Planning (PL) Standard prior to assessing a system.

Control Overlay CA-2 ED-05 (L, M, H): Reuse existing FedRAMP third party assessment organization (3PAO) reports available from the FedRAMP Program Management Office to assess FedRAMP authorized cloud service providers

Control Overlay CA-2 ED-06 (L, M, H): Leverage FedRAMP tailored test cases specific for FedRAMP Tailored when conducting an assessment or self-assessment of FedRAMP Tailored Low Impact-Software as a Service (LI-SaaS) cloud service providers.

Control Overlay CA-2 ED-07 (L, M, H): Accept Inter-Agency Agreement (IAA) in lieu of performing an assessment of ED Shared Services.

Control Overlay CA-2 ED-08 (L, M, H): Execute a self-assessment of all controls within the control baseline prior to obtaining an initial ATO and record the self-assessment results in CSAM. Capture any weaknesses identified during the self-assessment within a POA&M which is associated to the vulnerable control.

Control Overlay CA-2 ED-09 (L, M, H): Execute a self-assessment within 90 days of any controls to be assessed by the Department's authorized assessor and record the self-assessment results in CSAM. Capture any weaknesses identified during the self-assessment within a POA&M which is associated to the vulnerable control.

2.2.1 CA-2(1) Control Assessments | Independent Assessors (M, H)

Employ independent assessors or assessment teams to conduct control assessments.

2.2.2 CA-2(2) Control Assessments | Specialized Assessments (H)

Include as part of control assessments, annual (i.e., each fiscal year), announced, penetration testing and other forms of security assessments to include but not be limited to the following: in-depth monitoring; malicious user testing; vulnerability scanning; insider threat assessment; performance/load testing.

2.3 CA-3 Information Exchange (L, M, H)

a. Approve and manage the exchange of information between the system and other systems using interconnection security agreements (ISA); memorandum of understanding (MOU); interagency agreements (IAA); service level agreements (SLA);

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements at least annually (i.e., each fiscal year).

2.3.1 CA-3(6) Information Exchange | Transfer Authorizations (H)

Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

2.4 CA-5 Plan of Action and Milestones (POA&M) (P, L, M, H and Control Overlay)

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones monthly, at minimum, based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Control Overlay CA-5 ED-01 (L, M, H): Create, monitor, manage, track and report enterprise-level and system-level POA&Ms in CSAM in accordance with the current version of the Department's POA&M Standard Operating Procedures (SOP).

Control Overlay CA-5 ED-02 (L, M, H): Document a user-defined criticality in CSAM for all new POA&Ms created and injected as well as for all open POA&M(s) in accordance with the current version of the Department's POA&M SOP.

Control Overlay CA-5 ED-03 (L, M, H): Receive approval from CSP vendors at the time of authorization to inject POA&M information into CSAM; when approval is not obtained, then the maximum CSF Risk Scorecard score will be limited.

Control Overlay CA-5 ED-04 (L, M, H): Inject FedRAMP Cloud Service Provider (CSP) POA&M information into CSAM, when Principal Offices sponsor a Department ATO for the CSP and direct approval from the CSP vendor to inject the CSP POA&Ms into CSAM is received.

2.5 CA-6 Authorization (P, L, M, H and Control Overlay)

a. Assign a senior official as the AO for the system.

b. Assign a senior official as the AO for common controls available for inheritance by organizational systems.

c. Ensure that the AO for the system, before commencing operations:

    1. Accepts the use of common controls inherited by the system; and

    2. Authorizes the system to operate.

d. Ensure that the AO for common controls authorizes the use of those controls for inheritance by organizational systems.

e. Update the authorizations in accordance with the terms and conditions established by the AO.

Control Overlay CA-6 ED-01 (L, M, H): Designate the ED CIO as the defacto AO for all ED systems unless specifically delegated otherwise.

Control Overlay CA-6 ED-02 (L, M, H): Identify in a formal authorization memo signed by the AO the authorization decision as defined in Appendix B: Authorization Decision. Document and report the status of the ATO or Ongoing Security Authorization (OSA) in CSAM.

Control Overlay CA-6 ED-03 (L, M, H): Take actions required to register into the Department's FISMA inventory and then shut down, migrate, or authorize any information systems and services discovered processing, storing, transmitting, or disseminating information on behalf of the Department or Principal Operating Component (POC) without a valid ATO.

Control Overlay CA-6 ED-04 (L, M, H): Ensure the CSF Risk Scorecard maintains a score of "0.00" for all unauthorized information systems and services operating without an ATO until the system or service is authorized in accordance with the Department's policies. Systems scored as "0.00" negatively impact POC scores and are briefed to Department senior leadership at least monthly. Score unauthorized systems/services that adhere to OCIO requirements for achieving an ATO as a "1.00" for a safe harbor period specified by the CISO or delegate and based on system impact levels. Based upon an assessment of risk, the respective AO may render a Denial of Authorization decision.

Control Overlay CA-6 ED-05 (L, M, H): Based upon an assessment of risk, the respective AO may explicitly accept the risk for the operation of the system and grant an ATO to systems/services which are pursuing migration or authorization and are 1) registered in CSAM as operational; 2)

scheduled for assessment; and 3) are actively working to complete required assessment and authorization processes defined within the Department's policies, standards, and processes.

Control Overlay CA-6 ED-06 (L, M, H): Authorize Federal Shared Services via an Inter-Agency Agreement (IAA).

2.6 CA-7 Continuous Monitoring (P, L, M, H and Control Overlay)

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: including, at minimum, metrics defined in the current version of the IAS Information System Continuous Monitoring (ISCM) Roadmap

b. Establishing at least monthly for monitoring and annually (i.e., each fiscal year) for assessment of control effectiveness or in accordance with OSA assessment schedule and in conjunction with the Continuous Diagnostics and Mitigation (CDM) Program

c. Ongoing control assessments in accordance with the continuous monitoring strategy

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy

e. Correlation and analysis of information generated by control assessments and monitoring

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to CISO, AO, CPO/SAOP monthly.

Control Overlay CA-7 ED-01 (L, M, H): Conduct continuous monitoring activities following the issuance of an ATO to identify and remediate risks while monitoring changing conditions which could potentially affect the ability to conduct core missions and business functions.

Control Overlay CA-7 ED-02 (L, M, H): Enroll all information systems, including common control providers, into the Department (OSA) program within 90 days of satisfying the entrance criteria; see Appendix C for OSA program entry and exit criteria. Eligible systems not enrolled with 90 days are required to track non-compliance with a POA&M.

2.6.1 CA-7(1) Continuous Monitoring | Independent Assessment (M, H)

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

2.6.2 CA-7(4) Continuous Monitoring | Risk Monitoring (P, L, M, H and Control Overlay

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

a. Effectiveness monitoring

b. Compliance monitoring, and

c. Change monitoring.

Control Overlay CA-7(4) ED-01 (L, M, H): Determine adherence to established risk appetite and tolerance, as it relates to the Department's Enterprise Risk Management (ERM) program, through the ED CSF Risk Scorecard ratings.

Control Overlay CA-7(4) ED-02 (L, M, H): Use results of ongoing security and privacy assessments and monitoring using defined and proven methodologies, both quantitative metrics and qualitative risk elements, to monitor cyber risk, as represented in the ED CSF Risk Scorecard.

Control Overlay CA-7(4) ED-03 (L, M, H): Use ED CSF Risk Scorecard to evaluate adherence to established cyber risk appetite and risk tolerance. The Department's cybersecurity risk appetite represents the target risk profile for a system, Principal 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 '2.00' on a scale of '0.00-3.00' within the ED CSF Risk Scorecard. Therefore, systems are expected to maintain a minimum level of '2.00' as the risk appetite while the system is operational. Systems and system stakeholders must strive for level 3.00 by performing actions to mitigate risks and vulnerabilities.

The cyber risk tolerance represents the amount of cybersecurity risk the Department is prepared to temporarily 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 '1.00' point on a scale from '0.00 – 3.00' within the ED CSF Risk Scorecard. Therefore, systems may temporarily perform down to a '1.00' as mission and business necessity demand. The formal process for cyber risk tolerance acceptance is the Department's security authorization process for issuing and maintaining an ATO.

Control Overlay CA-7(4) ED-04 (L, M, H): Coordinate the Department's Cyber Risk program with the Department's ERM function to maintain awareness of the cyber risk of the organization. Provide tolerance and appetite information 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.

2.7 CA-8 Penetration Testing (H and Control Overlay)

Conduct penetration testing at least annually (i.e., each fiscal year) on all FIPS 199 High impact and HVA information systems.

Control Overlay CA-8 ED-01 (H): Ensure the penetration test methodology used for all penetration testing performed aligns with this policy and the current version of NIST SP 800-115: *Technical Guide to Information Security Testing and Assessment*.

Control Overlay CA-8 ED-02 (H): Develop a penetration test plan which describes the scope and methodology of the testing, rules of engagement, test schedule, logistics including all equipment, tools, and software/applications used, communication strategy, and the documents actions taken to comply with Department requirements.

Control Overlay CA-8 ED-03 (H): Limit or prevent adverse impacts to the ED operations and information system as a result of penetration testing performed; require all authorized penetration testers to retain/provide evidence of the following:

a. A digital forensic image of each testing machine (this includes virtual machine images used for remote testing) prior to the start of testing and signed attestation that all penetration testing equipment, software, and services are free from indications of compromise at the time the forensic image was taken.

b. Results of industry standard vulnerability scans for each testing machine to determine if any vulnerabilities exist and to verify that all patching is up-to-date and signed attestation stating its testing equipment, software and services are free from all vulnerabilities as noted in the national vulnerability database. Any exceptions are noted and the reasoning as to why the vulnerability cannot be addressed.

c. Description of antivirus software installed on each testing machine and verification that it is up to date with the most recent definitions.

d. The Federal Information Processing Standards certification numbers identifying the encryption standards used on each testing machine for all encryption.When assessors are furnished with ED government furnished equipment and services (GFES) deployed with the Department authorized Virtual Private Network (VPN) software, only the GFES may be used to establish a “tunnel” to access the Department’s network for any non-government furnished equipment (non-GFES) testing machines.

e. When drone virtual machines are used to conduct remote assessments, the drones will be configured to make use of a secure outbound connection to the internet. The connection is established via FIPS-140-2/3 validated (certificate provided as noted in “d”) Public Key infrastructure with an AES256 cypher being used. PKI connection keys must be established by or provided to ED SOC for appropriate monitoring and analysis of the encrypted traffic.

Control Overlay CA-8 ED-04 (H): Limit the use of whitelisting of testing equipment; when it is required to conduct testing of specific development environments, whitelisting should be documented and restricted to a specific target range of internet protocol and system access.

Control Overlay CA-8 ED-05 (H): Ensure the AO or designated representative reviews and approves the penetration test plan, including the rules of engagement, prior to initiating any penetration testing activities.

Control Overlay CA-8 ED-06 Conduct penetration testing at least annually (i.e., each fiscal year) on all FIPS 199 Moderate impact information systems

2.7.1 CA-8(1) Penetration Testing | Independent Penetration Testing Agent or Team (H and Control Overlay)

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

Control Overlay CA-8(1) ED-01 (H): Enable and support penetration testing performed by DHS.

2.8 CA-9 Internal System Connections (L, M, H)

a. Authorize internal connections of all components or classes of components to the system.

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated.

c. Terminate internal system connections after determining it no longer provides support for organizational missions or business functions or when conditions meet one or more of the following:

    1. Zero trust architecture standards, guidance, and memorandums from Cybersecurity and Infrastructure Security Agency (CISA), Office of Management and Budget (OMB) or NIST
    2. Targeted responses to certain types of incidents
    3. Time-of-day restrictions on system use, if implemented, or
    4. Thirty (30) minutes of session inactivity. System-level activities, established by a virtual private network (VPN) connection, are authorized to continue after strict user interactions have ended to support remote system patching; and

d. Review at least annually (i.e., each fiscal year) the continued need for each internal connection.

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: ACRONYMS

Table 2: Acronyms

Acronym	Definition
3PAO	Third Party Assessment Organization
ACS	Administrative Communication System
AO	Authorizing Official
ATO	Authorization to Operate
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CSAM	Cyber Security Assessment and Management tool
CSP	Cloud Service Provider
DATO	Denial of Authorization to Operate
DHS	Department of Homeland Security
ED	Department of Education
ERM	Enterprise Risk Management
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
GFES	Government Furnished Equipment or Services
HVA	High Value Asset
IAA	Inter Agency Agreement
IAS	Information Assurance Services

ISA	Interconnection Security Agreement
ISCM	Information System Continuous Monitoring
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
LI-SaaS	Low Impact-Software as a Service
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OATO	Ongoing Authorization to Operate
OSA	Ongoing Security Authorization
PO	Principal Office
POA&M	Plan of Action & Milestones
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy
SLA	Service Level Agreement
SSP	System Security Plan
VPN	Virtual Private Network

APPENDIX B: BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below. NIST SP 800-53 controls that are not applicable to any control baseline are shaded in gray and notated with an asterisk.

Table 3: Baseline Control Parameter Summary

Control Identifier	Control/Control Enhancement Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
CA-1	Policy and Procedures	x	x	x	x	DE.DP, RS.AN	DE.DP-2, RS.AN-5
CA-2	Control Assessments	x	x	x	x	ID.RA, ID.SC, PR.IP, DE.DP, RS.AN, RS.MI, ID.DE-P, GV.MT-P, CT.DM-P, PR.PO-P	ID.RA-1, ID.RA-5, ID.SC-4, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-5, RS.MI-3, ID.DE-P5, GV.MT-P3, CT.DM-P9, PR.PO-P5
CA-2(1)	Control Assessments Independent Assessors			x	x	ID.RA, ID.SC, PR.IP, DE.DP, RS.AN, RS.MI, ID.DE-P, GV.MT-P, CT.DM-P, PR.PO-P	ID.RA-1, ID.RA-5, ID.SC-4, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-5, RS.MI-3, ID.DE-P5, GV.MT-P3, CT.DM-P9, PR.PO-P5
CA-2(2)	Control Assessments Specialized Assessments				x	ID.RA, ID.SC, PR.IP, DE.DP, RS.AN, RS.MI, ID.DE-P, GV.MT-P, CT.DM-P, PR.PO-P	ID.RA-1, ID.RA-5, ID.SC-4, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-5, RS.MI-3, ID.DE-P5, GV.MT-P3,

Control Identifier	Control/Control Enhancement Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							CT.DM-P9, PR.PO-P5
*CA-2(3)	Control Assessments | Leveraging Results from External Organizations					ID.RA, ID.SC, PR.IP, DE.DP, RS.AN, RS.MI, ID.DE-P, GV.MT-P, CT.DM-P, PR.PO-P	ID.RA-1, ID.RA-5, ID.SC-4, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-5, RS.MI-3, ID.DE-P5, GV.MT-P3, CT.DM-P9, PR.PO-P5
CA-3	Information Exchange		x	x	x	ID.AM, DE.AE	ID.AM-3, DE.AE-1
CA-3(6)	Information Exchange | Transfer Authorizations				x	ID.AM, DE.AE	ID.AM-3, DE.AE-1
*CA-3(7)	Information Exchange | Transitive Information Exchanges					ID.AM, DE.AE	ID.AM-3, DE.AE-1
CA-5	Plan of Action and Milestones	x	x	x	x	ID.RA, ID.RA-P, GV.MT-P	ID.RA-1, ID.RA-6, ID.RA-P5, GV.MT-P4
*CA-5(1)	Plan of Action and Milestones | Automation Support for Accuracy and Currency					ID.RA, ID.RA-P, GV.MT-P	ID.RA-1, ID.RA-6, ID.RA-P5, GV.MT-P4
CA-6	Authorization	x	x	x	x	ID.RM. ID.GV	ID.RM-1, ID.GV-2
*CA-6(1)	Authorization | Joint Authorization — Intra-organization						
*CA-6(2)	Authorization | Joint Authorization — Inter-organization						
CA-7	Continuous Monitoring	x	x	x	x	ID.RA, ID.SC, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, ID.DE-P,	ID.RA-1, ID.RA-5, ID.SC-4, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2,

Control Identifier	Control/Control Enhancement Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						GV.MT-P, CT.DM-P, PR.PO-P	DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, ID.DE-P5, GV.MT-P1, GV.MT-P3, CT.DM-P9, PR.PO-P5, PR.PO-P6
CA-7(1)	Continuous Monitoring | Independent Assessment			x	x	ID.RA, ID.SC, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, ID.DE-P, GV.MT-P, CT.DM-P, PR.PO-P	ID.RA-1, ID.RA-5, ID.SC-4, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, ID.DE-P5, GV.MT-P1, GV.MT-P3, CT.DM-P9, PR.PO-P5, PR.PO-P6
*CA-7(3)	Continuous Monitoring | Trend Analyses					ID.RA, ID.SC, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, ID.DE-P, GV.MT-P, CT.DM-P, PR.PO-P	ID.RA-1, ID.RA-5, ID.SC-4, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1,

Control Identifier	Control/Control Enhancement Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, ID.DE-P5, GV.MT-P1, GV.MT-P3, CT.DM-P9, PR.PO-P5, PR.PO-P6
CA-7(4)	Continuous Monitoring | Risk Monitoring	x	x	x	x	ID.RA, ID.SC, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, ID.DE-P, GV.MT-P, CT.DM-P, PR.PO-P	ID.RA-1, ID.RA-5, ID.SC-4, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, ID.DE-P5, GV.MT-P1, GV.MT-P3, CT.DM-P9, PR.PO-P5, PR.PO-P6
*CA-7(5)	Continuous Monitoring | Consistency Analysis					ID.RA, ID.SC, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, ID.DE-P, GV.MT-P, CT.DM-P, PR.PO-P	ID.RA-1, ID.RA-5, ID.SC-4, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5,

Control Identifier	Control/Control Enhancement Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							RS.AN-1, RS.MI-3, ID.DE-P5, GV.MT-P1, GV.MT-P3, CT.DM-P9, PR.PO-P5, PR.PO-P6
*CA-7(6)	Continuous Monitoring | Automation Support for Monitoring					ID.RA, ID.SC, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, ID.DE-P, GV.MT-P, CT.DM-P, PR.PO-P	ID.RA-1, ID.RA-5, ID.SC-4, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, ID.DE-P5, GV.MT-P1, GV.MT-P3, CT.DM-P9, PR.PO-P5, PR.PO-P6
CA-8	Penetration Testing				x	ID.RA, PR.IP, PR.PO-P	ID.RA-1, PR.IP-7, PR.PO-P5
CA-8(1)	Penetration Testing | Independent Penetration Testing Agent or Team				x	ID.RA, PR.IP, PR.PO-P	ID.RA-1, PR.IP-7, PR.PO-P5
*CA-8(2)	Penetration Testing | Red Team Exercises					ID.RA, PR.IP, PR.PO-P	ID.RA-1, PR.IP-7, PR.PO-P5
*CA-8(3)	Penetration Testing | Facility Penetration Testing					ID.RA, PR.IP, PR.PO-P	ID.RA-1, PR.IP-7, PR.PO-P5
CA-9	Internal System Connections		x	x	x	ID.AM	ID.AM-3
*CA-9(1)	Internal System Connections | Compliance Checks					ID.AM	ID.AM-3

APPENDIX C: AUTHORIZATION DECISION

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 (e.g., security, privacy and supply chain) when deciding if the risk 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 POA&Ms.

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 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.

Table 4: Authorization Decision

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 may be 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 ATO. This includes major system

Authorization Decision	Description
	changes and security posture impacts analyzed and reported through risk scoring as identified ongoing information security continuous monitoring (ISCM) activities.
Ongoing Authorization to Operate (OATO)	Issued after an AO has determined the risk to Department operations and assets, individuals, other organizations, and the nation is acceptable and OSA entrance criteria are satisfied. Ongoing authorization is defined as the subsequent (follow-on) risk determinations and risk acceptance decisions taken at agreed-upon and documented frequencies in accordance with the Department's mission/business requirements and organizational risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process. The authorizing official is provided with the necessary information regarding the near real-time security and privacy posture of the system to determine whether the mission/business risk of continued system operation or the provision of common controls is acceptable. The authorization termination decision is event driven and the AO may determine that the system's OATO is rescinded based on a risk-based determination. 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 OATO decision. 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 (DATO)	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

Authorization Decision	Description
	halted. A Denial of Authorization indicates that there are major weaknesses or deficiencies in the security controls employed within or inherited by the information system.

APPENDIX D: ONGOING SECURITY AUTHORIZATION CRITERIA

The OSA entrance criteria conditions in table below must be satisfied to enter into the Department's OSA program. The OSA Exit Criteria events are triggers that may result in a system's unenrollment from the OSA program.

Table 5: OSA Entrance Criteria

OSA ENTRANCE CRITERIA	
Event	**Description**
ATO Granted	An independent assessment of risk has been completed (Baseline Assessment). AND OSA MOU signed and on file within CSAM. AND Ongoing Authority to Operate (OATO) Memo signed and on file within CSAM.
Privacy Assessment	The information system has a valid, up-to-date Privacy Threshold Analysis (PTA) and, if required, Privacy Impact Assessment (PIA) based upon determinations from the Department's Privacy Office.

Table 6: OSA Exit Criteria

OSA EXIT CRITERIA	
Event	**Description**
Past Due POA&Ms	Past Due POA&M risk factor score is less than a three (3) in the system level CSF Scorecard
CSF Risk Scorecard Overall Score	Overall Score < 1, which is below the established Department Risk Appetite
Secure Baseline Configuration (STIG) Compliance	Remediation of non-compliant secure baseline configuration findings not completed within two weeks of OSA entrance or OSA assessment remediation period
Critical and High Vulnerabilities	All identified critical and high vulnerabilities have not been remediated within the Department's established timelines in accordance with *Information Technology (IT)*

OSA EXIT CRITERIA	
	System Risk Assessment (RA) Standard
Significant System Change	If significant system changes occur, including planned or unplanned major upgrades or system migration
System information is inaccurate and/or outdated in CSAM	System is identified on the CSAM Data Discrepancies report for inaccuracies or missing information