Information Technology (IT) System and Services Acquisition (SA) Standard

January 26, 2024

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: 2024.01.26 17:02:24 -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.

Version	Date	Summary of Changes
1.0	1/21/2021	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	1/31/2022	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 EO.
1.2	1/31/2023	Updated to incorporate changes from annual review. Update broken links. Add footnote to HVA control reference in Section 2. Updates to SA-8 and SA-10 to address NIST SP 800-218 *Secure Software Development Framework, (SSDF)* requirements. Added SA-9 control overlay to address required actions from CISA BOD 23-01. Added control overlays SA-4 ED-01 and SA-4 ED-02.
5.3	1/26/2024	Aligned document major version number to align with NIST SP 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, Standards was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Inserted references to NIST SP 800-53B tailoring guidance. Updated Section 4, Acronyms as appropriate. Updated language in controls SA-01, SA-01 ED-01, and SA-03. Added controls SA-03(02), SA-04 ED-03, SA-04(08), SA-04(12), SA-09(01), SA-09(03), SA-09(05), SA-09(06), SA-09(08), SA-10(01), SA-10(03), SA-10(07), SA-11(01), SA-11(06), and SA-11(08). Added “leading zeros” to control identifiers in alignment with patch release of NIST SP 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays.

Table of Contents

1 INTRODUCTION

This governance document establishes U.S. Department of Education (ED or Department) information technology (IT) system and services acquisition standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders (EO), Emergency Orders, Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. 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 governance 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 (PUB) 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 amended, 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 system and services acquisition standards 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 and services acquisition 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 PUB 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 PUB 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 PUB 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). Systems that process federal tax information (FTI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[5], *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information.* Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines[6].

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) by using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to *APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY* for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

2.1 SA-01 Policy and Procedures (P, L, M, H, and Control Overlay)

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 ACSD-OCIO-004[7], Cybersecurity Policy, ACSD-OCIO-

[5] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf
[6] FedRAMP baselines https://www.fedramp.gov/baselines/
[7] Also known as OCIO: 3-112.

011[8], *Software Asset Management Acquisition Policy*, ACSD-OFO-006[9], *Acquisition Planning*, Acquisition Procedures Manual, and *Security and Privacy Requirements for IT Procurements*, a Department-level system and services acquisition policy (e.g., this document) that:

(a) addresses 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 ACSD-OCIO-004, *Cybersecurity Policy*.

The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) and Senior Procurement Executive or designee are designated to manage the development, documentation, and dissemination of the Department-level IT system and services acquisition 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.

Principal Office (PO) 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 this policy standard and associated system and services acquisition controls. The ISO and ISSO shall review system and services acquisition 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.

Control Overlay SA-1 ED-01 (P, L, M, H): This IT System and Services Acquisition (SA) Standard supplements ACSD-OCIO-011, *Software Asset Management Acquisition Policy*, ACSD-OFO-006, *Acquisition Planning*, Acquisition Procedures Manual, and *Security and Privacy Requirements for IT Procurements.*

[8] Also known as OCIO: 3-110.

[9] Also known as OFO-F: 2-107.

2.2 SA-02 Allocation of Resources (P, L, M, H)

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

2.3 SA-03 System Development Life Cycle (P, L, M, H)

a. Acquire, develop, and manage the system using ACSD-OCIO-007[10], *Lifecycle Management (LCM) Framework* and associated Enterprise Program Management Review (EPMR) Framework that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

2.3.1 SA-03(02) System Development Life Cycle | Use of Live or Operational Data

a. Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and

b. Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.

2.4 SA-04 Acquisition Process (P, L, M, H)

Include the following requirements, descriptions, and criteria, explicitly or by reference, using *Security and Privacy Requirements for IT Procurements* in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements.

[10] Also known as OCIO: 1-016.

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

Control Overlay SA-04 ED-01 (L, M, H): Ensure the Department CIO contract review process is performed before entering into a contract for IT or IT services or acquiring Internet of Things (IoT) devices(s) using a P-card or Simplified Acquisition Threshold purchase to assess device compliance with NIST IoT standards and guidelines.

Control Overlay SA-04 ED-02 (L, M, H): Prohibit using, procuring or obtaining an IoT device, or renewing a contract to procure or obtain an IoT device which does not comply with NIST IoT standards and guidelines unless the device(s) is necessary for national security, for research purposes, or is secured using alternative effective methods and a waiver of the prohibition on use or acquisition of the device in question is authorized.

Control Overlay SA-04 ED-03 (L, M, H): Ensure that all Department leveraged cloud service providers (CSPs) are Federal Risk and Authorization Management Program (FedRAMP) Authorized prior to being procured or placed into production.

2.4.1 SA-04(01) Acquisition Process | Functional Properties of Controls (M, H)

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

2.4.2 SA-04(02) Acquisition Process | Design and Implementation Information for Controls (M, H)

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design; low-level design; source code (only if applicable) or hardware schematics; and information and information sensitivity at level of detail necessary to permit analysis and testing.

Control Overlay SA-04(02) ED-01 (L, M, H): Obtain from software producers an acceptable self-attestation from software producers, consistent with NIST Guidance and OMB M-22-18, before using software.

a. Ensure the self-attestation includes the minimum requirements as documented in OMB M-22-18.

b. Require the software producer to identify those practices to which they cannot attest, practices they have in place to mitigate those risks and develop a Plan of Action & Milestones (POA&M). Take appropriate steps to ensure that such documentation is not posted publicly, either by the vendor or by the Department itself. If the software producer supplies that documentation and the Department finds it satisfactory, the Department may use the software despite the producer's inability to provide a complete self-attestation. Retain the self-attestation document unless the software producer posts it publicly and provides a link to the posting as part of its proposal response.

2.4.3 SA-04(05) Acquisition Process | System, Component, and Service Configurations (H)

Require the developer of the system, system component, or system service to:

a. Deliver the system, component, or service with ED approved security configurations consistent with the Department's baseline security and privacy configuration settings, as defined in the Information Technology (IT) Configuration Management (CM) Standard implemented; and

b. Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

2.4.4 SA-04(08) Acquisition Process | Continuous Monitoring Plan for Controls

Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.

2.4.5 SA-04(09) Acquisition Policy | Functions, Ports, Protocols, and Services in Use (M, H)

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

2.4.6 SA-04(10) Acquisition Policy | Use of Approved PIV Products (L, M, H)

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

2.4.7 SA-04(12) Acquisition Process | Data Ownership

a. Include organizational data ownership requirements in the acquisition contract; and

b. Require all data to be removed from the contractor's system and returned to the organization within 7 calendar days prior to contract termination.

2.5 SA-05 System Documentation (L, M, H)

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security and privacy functions and mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

   1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and;
   3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take action to create documentation if such documentation is essential to the effective implementation or operation of security controls in response; and

d. Distribute documentation to ISO and ISSO; in addition, distribute to other personnel with a need to know when required by contract or to provide system support.

2.6 SA-08 Security and Privacy Engineering Principles (L, M, H, and Control Overlay)

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: principles, concepts, activities, and tasks for engineering trustworthy secure systems contained within the current version of SP 800-160 Vol. 1 Rev. 1, *Engineering Trustworthy Secure Systems* and the NIST Secure Software Development Framework (SSDF) ED defined systems security and privacy engineering principles as documented in the ED Technical Security Architecture.

Control Overlay SA-08 ED-01 (L, M, H): Implement the security measures designated by NIST for all categories of critical software and critical software platforms.

2.6.1 SA-08(33) Security and Privacy Engineering Principles | Minimization (P)

Implement the privacy principle of minimization using processes consistent with applicable laws and policies which ensure systems only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and only maintain personally identifiable information for as long as is necessary to accomplish the purpose.

2.7 SA-09 External System Services (P, L, M, H and Control Overlay)

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: the ED-defined baseline security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Define and document organizational oversight and user roles and responsibilities regarding external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: as specified in Security and Privacy Requirements for IT Procurements document and applicable external system services documentation to include service level agreements (SLAs).

Control Overlay SA-09 ED-01 (L, M, H): Require Common Control Providers (CCP), including cloud service providers, to document and provide security controls for inheritance within the Cyber Security Assessment and Management (CSAM) system for all dependent systems, where the CCP has executed a Memorandum of Understanding (MOU) or Service Level Agreement (SLA) to provide the controls.

Control Overlay SA-09 ED-02 (L, M, H): Create documentation regarding common controls that may be inherited from CCP by other information systems and make the documentation available to all ISOs for review, consideration, and incorporation into their respective System Security Plans (SSP).

Control Overlay SA-09 ED-03 (L, M, H): Ensure CCPs must obtain an authorization to operate (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.

Control Overlay SA-09 ED-04 (L, M, H): Perform automated asset discovery and vulnerability enumeration across all discovered assets in accordance with DHS CISA BOD 23-01.

2.7.1 SA-09(01) External System Services | Risk Assessments and Organizational Approvals

a. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and

b. Verify that the acquisition or outsourcing of dedicated information security services is approved by a designated Department official.

2.7.2 SA-09(02) External System Services | Identification of Functions, Ports, Protocols, and Services (M, H)

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: all ED information systems and services which require an ATO.

2.7.3 SA-09(03) External System Services | Establish and Maintain Trust Relationship with Providers

Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: *Department Information Security and Privacy Requirements*, as amended.

2.7.4 SA-09(05) External System Services | Processing, Storage, and Service Location

Restrict the location of information or data and system services to the U.S. and its territories based on *Department Information Security and Privacy Requirements*, as amended.

2.7.5 SA-09(06) External System Services | Organization-controlled Cryptographic Keys

Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.

2.7.6 SA-09(08) External System Services | Processing and Storage Location — U.S. Jurisdiction

Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.

2.8 SA-10 Developer Configuration Management (M, H)

Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service design, development, implementation, operations, and disposal phases;

b. Document, manage, and control the integrity of changes to ED defined configuration management items to include but not limited to : the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the

object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation; software release files; and provenance data.

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to the ISO and ISSO.

2.8.1 SA-10(01) Developer Configuration Management | Software and Firmware Integrity Verification

Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

2.8.2 SA-10(03) Developer Configuration Management | Hardware Integrity Verification

Require the developer of the system, system component, or system service to enable integrity verification of hardware components.

2.8.3 SA-10(07) Developer Configuration Management | Security and Privacy Representatives

Require designated security and privacy representatives to be included in the configuration change management and control process.

2.9 SA-11 Developer Testing and Evaluation (P, M, H)

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security and privacy control assessments;

b. Perform unit, integration, system, and/or regression testing/evaluation as defined in the configuration management plan at a depth and coverage necessary to ensure that required security controls are implemented correctly and operating as intended;

c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during testing and evaluation.

2.9.1 SA-11(01) Developer Testing and Evaluation | Static Code Analysis

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

2.9.2 SA-11(06) Developer Testing and Evaluation | Attack Surface Reviews

Require the developer of the system, system component, or system service to perform attack surface reviews.

2.9.3 SA-11(08) Developer Testing and Evaluation | Dynamic Code Analysis

Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

2.10 SA-15 Development Process, Standards, and Tools (M, H)

a. Require the developer of the system, system component, or system service to follow a documented development process that:

   1. Explicitly addresses security and privacy requirements;
   2. Identifies the standards and tools used in the development process;
   3. Documents the specific tool options and tool configurations used in the development process; and
   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations at least annually (i.e., each fiscal year) to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: *Security and Privacy Requirements for IT Procurements*.

2.10.1 SA-15(03) Development Process, Standards, and Tools | Criticality Analysis (M, H)

Require the developer of the system, system component, or system service to perform a criticality analysis:

   a. At the following decision points in the system development life cycle: initially at the system design/architectural design phase of the EPMR and continuously through the entire lifecycle, including Operations and Maintenance (O&M) phase if there are significant system changes impacting criticality of system components; and
   b. At the following level of rigor: ED approved breadth and depth of criticality analysis.

2.11 SA-16 Developer-Provided Training (H)

Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: ED approved training to ensure the effectiveness of security controls implemented within ED information systems.

2.12 SA-17 Developer Security and Privacy Architecture and Design (H)

Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:

a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;

b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and

c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.

2.13 SA-21 Developer Screening (H)

Require that the developer of any information system, component, or service where the developer needs direct access to the ED managed environment:

a. Has appropriate access authorizations as determined by assigned ISO and ISSO; and

b. Satisfies the following additional personnel screening criteria: in accordance with ACSD-OFO-013[11], *Contractor Employee Personnel Security Screening*, and/or ED defined contractor personnel screening criteria as defined in *Information Technology (IT) System Personnel Security Standard*.

2.14 SA-22 Unsupported System Components (L, M, H, Control Overlay)

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components:

   1. Must be replaced unless extended support is obtained from either the component developer or third-party service supplier certified by the original component developer;

   2. Risk acceptance (exceptions and/or waivers) signed by the ED Authorizing Official (AO) are required for continued use of unsupported system components required to satisfy mission/business needs.

[11] Also known as OFO-O: 5-101.

Control Overlay SA-22 ED-01 (L, M, H): Require Enterprise Architecture Technology Insertion (EA(TI)) approval for all hardware and software for use on Department computers (laptop, desktop, server computers, and all other electronic devices) and networks before the hardware or software is executed or installed.

Control Overlay SA-22 ED-02 (L, M, H): Seek approval or obtain a waiver for unapproved software within 30 days of identification or discovery.

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 ACRONYMS

Acronym	Definition
ACSD	Administrative Communications System Directives
AO	Authorizing Official
ATO	Authorization to Operate
BOD	Binding Operational Directive
CCP	Common Control Provider
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CM	Configuration Management Family
CM.AW-P	Data Processing Awareness
CM-P	Communicate-P
CSAM	Cyber Security Assessment and Management
CSF	Cybersecurity Framework
CSP	Cloud Service Provider
CT.DP-P	Disassociated Processing
CT.PO-P	Data Processing Policies, Processes, and Procedures
CT-P	Control-P
DE	Detect
DE.CM	Security Continuous Monitoring
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
EA(TI)	Enterprise Architecture Technology Insertion
ED	U.S. Department of Education
EO	Executive Order
EPMR	Enterprise Program Management Review
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTRI	Federal Tax Return Information
GRP	Governance, Risk and Policy
GV.AT-P	Awareness and Training
GV.PO-P	Governance Policies, Processes, and Procedures
GV-P	Govern-P
H	High
HVA	High Value Asset
IAS	Information Assurance Services
ID	Identify
ID.AM	Asset Management
ID.BE	Business Environment
ID.DE-P	Data Processing Ecosystem Risk Management
ID.GV	Governance
ID.RA	Risk Assessment
ID.SC	Supply Chain Risk Management

Acronym	Definition
ID-P	Identify-P
IoT	Internet of Things
IRS	Internal Revenue Service
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
L	Low
LCM	Lifecycle Management
M	Moderate
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OCIO	Office of the Chief Information Officer
ODP	Organizationally Defined Parameters
OMB	Office of Management and Budget
P	Privacy
PF	Privacy Framework
PIV	Personal Identity Verification
PO	Principal Office
POA&M	Plan of Action & Milestones
PR	Protect
PR.AT	Awareness and Training
PR.DS	Data Security
PR.DS-P	Data Security
PR.IP	Information Protection Processes and Procedures
PR.PO-P	Data Protection Policies, Processes, and Procedures
PR-P	Protect-P
PUB	Publication
RAF	Risk Acceptance Form
SA	System and Services Acquisition Family
SAOP	Senior Agency Official for Privacy
SLA	Service Level Agreement
SP	Special Publication
SSDF	Secure Software Development Framework
SSP	System Security Plan

APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
SA-01	Policy and Procedures	X	X	X	X		
SA-02	Allocation of Resources	X	X	X	X	ID.GV, GV.PO-P	ID.GV-4, GV.PO-P2
SA-03	System Development Life Cycle	X	X	X	X	PR.IP, GV.PO-P, CT.PO-P	PR.IP-2, GV.PO-P2, CT.PO-P4
SA-03(01)	System Development Life Cycle | Manage Preproduction Environment					PR.IP, GV.PO-P, CT.PO-P	PR.IP-2, GV.PO-P2, CT.PO-P4
SA-03(02)	System Development Life Cycle | Use of Live or Operational Data					PR.IP, GV.PO-P, CT.PO-P	PR.IP-2, GV.PO-P2, CT.PO-P4
SA-03(03)	System Development Life Cycle | Technology Refresh					PR.IP, GV.PO-P, CT.PO-P	PR.IP-2, GV.PO-P2, CT.PO-P4
SA-04	Acquisition Process	X	X	X	X	ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-04(01)	Acquisition Process | Functional Properties of Controls			X	X	ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls			X	X	ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-04(03)	Acquisition Process | Development Methods, Techniques, and Practices					ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-04(05)	Acquisition Process | System, Component, and Service Configurations				X	ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-04(06)	Acquisition Process | Use of Information Assurance Products					ID.SC, PR.IP, DE.CM,	ID.SC-3, PR.IP-2, DE.CM-6,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
						ID.DE-P, CT.PO-P	ID.DE-P3, CT.PO-P4
SA-04(07)	Acquisition Process | NIAP-approved Protection Profiles					ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-04(08)	Acquisition Process | Continuous Monitoring Plan for Controls					ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-04(09)	Acquisition Process | Functions, Ports, Protocols, and Services in Use			X	X	ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-04(10)	Acquisition Process | Use of Approved PIV Products		X	X	X	ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-04(11)	Acquisition Process | System of Records					ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-04(12)	Acquisition Process | Data Ownership					ID.SC, PR.IP, DE.CM, ID.DE-P, CT.PO-P	ID.SC-3, PR.IP-2, DE.CM-6, ID.DE-P3, CT.PO-P4
SA-05	System Documentation		X	X	X	ID.RA	ID.RA-1
SA-08	Security and Privacy Engineering Principles		X	X	X	ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(01)	Security and Privacy Engineering Principles | Clear Abstractions					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
SA-08(02)	Security and Privacy Engineering Principles | Least Common Mechanism					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(03)	Security and Privacy Engineering Principles | Modularity and Layering					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(04)	Security and Privacy Engineering Principles | Partially Ordered Dependencies					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(05)	Security and Privacy Engineering Principles | Efficiently Mediated Access					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(06)	Security and Privacy Engineering Principles | Minimized Sharing					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(07)	Security and Privacy Engineering Principles | Reduced Complexity					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(08)	Security and Privacy Engineering Principles | Secure Evolvability					ID.BE, PR.IP,	ID.BE-5, PR.IP-2, CT.PO-P4,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
						CT.PO-P, CT.DP-P	CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(09)	Security and Privacy Engineering Principles | Trusted Components					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(10)	Security and Privacy Engineering Principles | Hierarchical Trust					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(11)	Security and Privacy Engineering Principles | Inverse Modification Threshold					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(12)	Security and Privacy Engineering Principles | Hierarchical Protection					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(13)	Security and Privacy Engineering Principles | Minimized Security Elements					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(14)	Security and Privacy Engineering Principles | Least Privilege					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
							CT.DP-P4, CT.DP-P5
SA-08(15)	Security and Privacy Engineering Principles | Predicate Permission					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(16)	Security and Privacy Engineering Principles | Self-reliant Trustworthiness					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(17)	Security and Privacy Engineering Principles | Secure Distributed Composition					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(18)	Security and Privacy Engineering Principles | Trusted Communications Channels					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(19)	Security and Privacy Engineering Principles | Continuous Protection					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(20)	Security and Privacy Engineering Principles | Secure Metadata Management					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
SA-08(21)	Security and Privacy Engineering Principles | Self-analysis					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(22)	Security and Privacy Engineering Principles | Accountability and Traceability					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(23)	Security and Privacy Engineering Principles | Secure Defaults					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(24)	Security and Privacy Engineering Principles | Secure Failure and Recovery					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(25)	Security and Privacy Engineering Principles | Economic Security					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(26)	Security and Privacy Engineering Principles | Performance Security					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(27)	Security and Privacy Engineering Principles | Human Factored Security					ID.BE, PR.IP,	ID.BE-5, PR.IP-2, CT.PO-P4,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
						CT.PO-P, CT.DP-P	CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(28)	Security and Privacy Engineering Principles | Acceptable Security					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(29)	Security and Privacy Engineering Principles | Repeatable and Documented Procedures					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(30)	Security and Privacy Engineering Principles | Procedural Rigor					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(31)	Security and Privacy Engineering Principles | Secure System Modification					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(32)	Security and Privacy Engineering Principles | Sufficient Documentation					ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5
SA-08(33)	Security and Privacy Engineering Principles | Minimization	X				ID.BE, PR.IP, CT.PO-P, CT.DP-P	ID.BE-5, PR.IP-2, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
							CT.DP-P4, CT.DP-P5
SA-09	External System Services	X	X	X	X	ID.AM, ID.SC, PR.AT, DE.CM, ID.DE-P, GV.AT-P	ID.AM-4, ID.SC-1, ID.SC-3, ID.SC-4, PR.AT-3, DE.CM-6, ID.DE-P1, ID.DE-P3, ID.DE-P5, GV.AT-P4
SA-09(01)	External System Services | Risk Assessments and Organizational Approvals					ID.AM, ID.SC, PR.AT, DE.CM, ID.DE-P, GV.AT-P	ID.AM-4, ID.SC-1, ID.SC-3, ID.SC-4, PR.AT-3, DE.CM-6, ID.DE-P1, ID.DE-P3, ID.DE-P5, GV.AT-P4
SA-09(02)	External System Services | Identification of Functions, Ports, Protocols, and Services			X	X	ID.AM, ID.SC, PR.AT, DE.CM, ID.DE-P, GV.AT-P	ID.AM-4, ID.SC-1, ID.SC-3, ID.SC-4, PR.AT-3, DE.CM-6, ID.DE-P1, ID.DE-P3, ID.DE-P5, GV.AT-P4
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers					ID.AM, ID.SC, PR.AT, DE.CM, ID.DE-P, GV.AT-P	ID.AM-4, ID.SC-1, ID.SC-3, ID.SC-4, PR.AT-3, DE.CM-6, ID.DE-P1, ID.DE-P3, ID.DE-P5, GV.AT-P4
SA-09(04)	External System Services | Consistent Interests of Consumers and Providers					ID.AM, ID.SC, PR.AT, DE.CM, ID.DE-P, GV.AT-P	ID.AM-4, ID.SC-1, ID.SC-3, ID.SC-4, PR.AT-3, DE.CM-6, ID.DE-P1, ID.DE-P3,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
							ID.DE-P5, GV.AT-P4
SA-09(05)	External System Services | Processing, Storage, and Service Location					ID.AM, ID.SC, PR.AT, DE.CM, ID.DE-P, GV.AT-P	ID.AM-4, ID.SC-1, ID.SC-3, ID.SC-4, PR.AT-3, DE.CM-6, ID.DE-P1, ID.DE-P3, ID.DE-P5, GV.AT-P4
SA-09(06)	External System Services | Organization-controlled Cryptographic Keys					ID.AM, ID.SC, PR.AT, DE.CM, ID.DE-P, GV.AT-P	ID.AM-4, ID.SC-1, ID.SC-3, ID.SC-4, PR.AT-3, DE.CM-6, ID.DE-P1, ID.DE-P3, ID.DE-P5, GV.AT-P4
SA-09(07)	External System Services | Organization-controlled Integrity Checking					ID.AM, ID.SC, PR.AT, DE.CM, ID.DE-P, GV.AT-P	ID.AM-4, ID.SC-1, ID.SC-3, ID.SC-4, PR.AT-3, DE.CM-6, ID.DE-P1, ID.DE-P3, ID.DE-P5, GV.AT-P4
SA-09(08)	External System Services | Processing and Storage Location — U.S. Jurisdiction					ID.AM, ID.SC, PR.AT, DE.CM, ID.DE-P, GV.AT-P	ID.AM-4, ID.SC-1, ID.SC-3, ID.SC-4, PR.AT-3, DE.CM-6, ID.DE-P1, ID.DE-P3, ID.DE-P5, GV.AT-P4
SA-10	Developer Configuration Management			X	X	PR.DS, PR.IP, CT.PO-P, PR.PO-P, PR.DS-P	PR.DS-8, PR.IP-1, PR.IP-2, PR.IP-3, CT.PO-P4, PR.PO-P1, PR.PO-P2, PR.DS-P8

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
SA-10(01)	Developer Configuration Management | Software and Firmware Integrity Verification					PR.DS, PR.IP, CT.PO-P, PR.PO-P, PR.DS-P	PR.DS-8, PR.IP-1, PR.IP-2, PR.IP-3, CT.PO-P4, PR.PO-P1, PR.PO-P2, PR.DS-P8
SA-10(02)	Developer Configuration Management | Alternative Configuration Management					PR.DS, PR.IP, CT.PO-P, PR.PO-P, PR.DS-P	PR.DS-8, PR.IP-1, PR.IP-2, PR.IP-3, CT.PO-P4, PR.PO-P1, PR.PO-P2, PR.DS-P8
SA-10(03)	Developer Configuration Management | Hardware Integrity Verification					PR.DS, PR.IP, CT.PO-P, PR.PO-P, PR.DS-P	PR.DS-8, PR.IP-1, PR.IP-2, PR.IP-3, CT.PO-P4, PR.PO-P1, PR.PO-P2, PR.DS-P8
SA-10(04)	Developer Configuration Management | Trusted Generation					PR.DS, PR.IP, CT.PO-P, PR.PO-P, PR.DS-P	PR.DS-8, PR.IP-1, PR.IP-2, PR.IP-3, CT.PO-P4, PR.PO-P1, PR.PO-P2, PR.DS-P8
SA-10(05)	Developer Configuration Management | Mapping Integrity for Version Control					PR.DS, PR.IP, CT.PO-P, PR.PO-P, PR.DS-P	PR.DS-8, PR.IP-1, PR.IP-2, PR.IP-3, CT.PO-P4, PR.PO-P1, PR.PO-P2, PR.DS-P8
SA-10(06)	Developer Configuration Management | Trusted Distribution					PR.DS, PR.IP, CT.PO-P, PR.PO-P, PR.DS-P	PR.DS-8, PR.IP-1, PR.IP-2, PR.IP-3, CT.PO-P4, PR.PO-P1, PR.PO-P2, PR.DS-P8
SA-10(07)	Developer Configuration Management | Security and Privacy Representatives					PR.DS, PR.IP, CT.PO-P,	PR.DS-8, PR.IP-1, PR.IP-2,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
						PR.PO-P, PR.DS-P	PR.IP-3, CT.PO-P4, PR.PO-P1, PR.PO-P2, PR.DS-P8
SA-11	Developer Testing and Evaluation	X		X	X	ID.RA, ID.SC, PR.IP, ID.DE-P, CT.PO-P	ID.RA-1, ID.SC-4, PR.IP-2, ID.DE-P5, CT.PO-P4
SA-11(01)	Developer Testing and Evaluation | Static Code Analysis					ID.RA, ID.SC, PR.IP, ID.DE-P, CT.PO-P	ID.RA-1, ID.SC-4, PR.IP-2, ID.DE-P5, CT.PO-P4
SA-11(02)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses					ID.RA, ID.SC, PR.IP, ID.DE-P, CT.PO-P	ID.RA-1, ID.SC-4, PR.IP-2, ID.DE-P5, CT.PO-P4
SA-11(03)	Developer Testing and Evaluation | Independent Verification of Assessment Plans and Evidence					ID.RA, ID.SC, PR.IP, ID.DE-P, CT.PO-P	ID.RA-1, ID.SC-4, PR.IP-2, ID.DE-P5, CT.PO-P4
SA-11(04)	Developer Testing and Evaluation | Manual Code Reviews					ID.RA, ID.SC, PR.IP, ID.DE-P, CT.PO-P	ID.RA-1, ID.SC-4, PR.IP-2, ID.DE-P5, CT.PO-P4
SA-11(05)	Developer Testing and Evaluation | Penetration Testing					ID.RA, ID.SC, PR.IP, ID.DE-P, CT.PO-P	ID.RA-1, ID.SC-4, PR.IP-2, ID.DE-P5, CT.PO-P4
SA-11(06)	Developer Testing and Evaluation | Attack Surface Reviews					ID.RA, ID.SC, PR.IP, ID.DE-P, CT.PO-P	ID.RA-1, ID.SC-4, PR.IP-2, ID.DE-P5, CT.PO-P4
SA-11(07)	Developer Testing and Evaluation | Verify Scope of Testing and Evaluation					ID.RA, ID.SC, PR.IP, ID.DE-P, CT.PO-P	ID.RA-1, ID.SC-4, PR.IP-2, ID.DE-P5, CT.PO-P4
SA-11(08)	Developer Testing and Evaluation | Dynamic Code Analysis					ID.RA, ID.SC, PR.IP, ID.DE-P, CT.PO-P	ID.RA-1, ID.SC-4, PR.IP-2, ID.DE-P5, CT.PO-P4

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
SA-11(09)	Developer Testing and Evaluation | Interactive Application Security Testing					ID.RA, ID.SC, PR.IP, ID.DE-P, CT.PO-P	ID.RA-1, ID.SC-4, PR.IP-2, ID.DE-P5, CT.PO-P4
SA-15	Development Process, Standards, and Tools			X	X	ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-15(01)	Development Process, Standards, and Tools | Quality Metrics					ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-15(02)	Development Process, Standards, and Tools | Security and Privacy Tracking Tools					ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-15(03)	Development Process, Standards, and Tools | Criticality Analysis			X	X	ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-15(05)	Development Process, Standards, and Tools | Attack Surface Reduction					ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-15(06)	Development Process, Standards, and Tools | Continuous Improvement					ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-15(07)	Development Process, Standards, and Tools | Automated Vulnerability Analysis					ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-15(08)	Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information					ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-15(10)	Development Process, Standards, and Tools | Incident Response Plan					ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-15(11)	Development Process, Standards, and Tools | Archive System or Component					ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-15(12)	Development Process, Standards, and Tools | Minimize Personally Identifiable Information					ID.SC, ID.DE-P, CT.PO-P	ID.SC-2, ID.DE-P2, CT.PO-P4
SA-16	Developer-provided Training				X		
SA-17	Developer Security and Privacy Architecture and Design				X	ID.AM, CT.PO-P, CT.DP-P, CM.AW-P	ID.AM-3, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
SA-17(01)	Developer Security and Privacy Architecture and Design | Formal Policy Model					ID.AM, CT.PO-P, CT.DP-P, CM.AW-P	ID.AM-3, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3
SA-17(02)	Developer Security and Privacy Architecture and Design | Security-relevant Components					ID.AM, CT.PO-P, CT.DP-P, CM.AW-P	ID.AM-3, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3
SA-17(03)	Developer Security and Privacy Architecture and Design | Formal Correspondence					ID.AM, CT.PO-P, CT.DP-P, CM.AW-P	ID.AM-3, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3
SA-17(04)	Developer Security and Privacy Architecture and Design | Informal Correspondence					ID.AM, CT.PO-P, CT.DP-P, CM.AW-P	ID.AM-3, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3
SA-17(05)	Developer Security and Privacy Architecture and Design | Conceptually Simple Design					ID.AM, CT.PO-P, CT.DP-P, CM.AW-P	ID.AM-3, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3
SA-17(06)	Developer Security and Privacy Architecture and Design | Structure for Testing					ID.AM, CT.PO-P, CT.DP-P, CM.AW-P	ID.AM-3, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3
SA-17(07)	Developer Security and Privacy Architecture and Design | Structure for Least Privilege					ID.AM, CT.PO-P, CT.DP-P, CM.AW-P	ID.AM-3, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3
SA-17(08)	Developer Security and Privacy Architecture and Design | Orchestration					ID.AM, CT.PO-P, CT.DP-P, CM.AW-P	ID.AM-3, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3
SA-17(09)	Developer Security and Privacy Architecture and Design | Design Diversity					ID.AM, CT.PO-P, CT.DP-P, CM.AW-P	ID.AM-3, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3
SA-20	Customized Development of Critical Components					ID.AM, ID.BE	ID.AM-5, ID.BE-4, ID.BE-5
SA-21	Developer Screening				X	PR.IP, PR.PO-P	PR.IP-11, PR.PO-P9

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
SA-22	Unsupported System Components		X	X	X		
SA-23	Specialization						