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

January 31, 2022

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

APPROVAL

_____

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	Draft 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 the EO.

Table of Contents

1 INTRODUCTION

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.

This governance document establishes Department information technology (IT) system and services acquisition 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.

1.2 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 control standards.

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 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 (P) baseline controls are required.

---

[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/sites/whitehouse.gov/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

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 SA-1 System and Services Acquisition 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 OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy*, OCIO: 3-110/ACSD-OCIO-011, *Software Asset Management Acquisition Policy*, OFO-F: 2-107/ACSD-OFO-006, *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 OCIO: 3-112/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 Systems Services and Acquisitions (SA) Standard supplements ACSD-OCIO-011, Software Asset Management Acquisition Policy, OFO-F: 2-107/ACSD-OFO-006, *Acquisition Planning*, Acquisition Procedures Manual, and Security and Privacy Requirements for IT Procurements.

2.2   SA-2 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-3 System Development Life Cycle (P, L, M, H)

a. Acquire, develop, and manage the system using OCIO: 1-016/ACSD-OCIO-007*, 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.

2.4   SA-4 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.

 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.

2.4.1 SA-4(1) 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-4(2) 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.

2.4.3 SA-4(5) 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) System 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-4(9) Acquisition Process | 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.

2.4.5 SA-4(10) Acquisition Process | 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.

2.5 SA-5 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-8 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:

ED defined systems security and privacy engineering principles as documented in the ED Technical Security Architecture.

Control Overlay SA-8 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-8(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-9 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-9 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-9 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-9 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.

2.7.1   SA-9(2) 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.

2.8   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.

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.

2.9   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.

2.10 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(3) 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 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 OFO-O: 5-101/ACSD-OFO-013, *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 and 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.

Control Overlay SA-22 ED-01 (L, M, H): Require Enterprise Architecture Technology Insertion (EATI) 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

ACS	Administrative Communications System
AO	Authorizing Official
ATO	Authorization to Operate
CCP	Common Control Provider
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COR	Contracting Officer's Representative
CSAM	Cyber Security Assessment and Management
DHS	Department of Homeland Security
EATI	Enterprise Architecture Technology Insertion
ED	Department of Education
EDSOC	ED Security Operations Center
EPMR	Enterprise Program Management Review
EO	Executive Officer
FIPS	Federal Information Processing Standard
IAS	Information Assurance Services
ISA	Interconnection Security Agreement
ISO	Information System Owner
ISSO	Information Systems Security Officer
IT	Information Technology
LCM	Lifecycle Management
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
PIV	Personal Identity Verification
PO	Principal Office
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy

SLA   Service Level Agreement

SSP   System Security Plan

SP   Special Publication

5 APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below along with the designation when the control is offered to Principal Office information systems for inheritance. NIST SP 800-53 controls that are not applicable to any control baseline are shaded in gray.

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
SA-1	Policy and Procedures	x	x	x	x		
SA-2	Allocation of Resources	x	x	x	x	ID.GV, GV.PO-P	ID.GV-4, GV.PO-P2
SA-3	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-3(1)	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-3(2)	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-3(3)	System Development Life Cycle | Technology Refresh					PR.IP, GV.PO-P, CT.PO-P	PR.IP-2, GV.PO-P2, CT.PO-P4
SA-4	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-4(1)	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-4(2)	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-4(3)	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-4(5)	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-4(6)	Acquisition Process | Use of Information Assurance Products					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

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
SA-4(7)	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-4(8)	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-4(9)	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-4(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-4(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-4(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

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
SA-5	System Documentation		x	x	x	ID.RA	ID.RA-1
SA-8	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-8(1)	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
SA-8(2)	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-8(3)	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-8(4)	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

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
SA-8(5)	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-8(6)	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-8(7)	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-8(8)	Security and Privacy Engineering Principles | Secure Evolvability					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-8(9)	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-8(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-8(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

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
SA-8(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-8(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-8(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, CT.DP-P4, CT.DP-P5
SA-8(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-8(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-8(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-8(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-8(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

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
SA-8(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
SA-8(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-8(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-8(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-8(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-8(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-8(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-8(27)	Security and Privacy Engineering Principles | Human Factored 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

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
SA-8(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-8(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-8(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-8(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-8(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-8(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, CT.DP-P4, CT.DP-P5
SA-9	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-9(1)	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,

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
							ID.DE-P3, ID.DE-P5, GV.AT-P4
SA-9(2)	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-9(3)	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-9(4)	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, ID.DE-P5, GV.AT-P4
SA-9(5)	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-9(6)	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-9(7)	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,

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
							ID.DE-P5, GV.AT-P4
SA-9(8)	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
SA-10(1)	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(2)	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(3)	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(4)	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(5)	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

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
SA-10(6)	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(7)	Developer Configuration Management | Security and Privacy Representatives					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-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(1)	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(2)	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(3)	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(4)	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(5)	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(6)	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(7)	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(8)	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
SA-11(9)	Developer Testing and Evaluation | Interactive Application Security Testing					ID.RA, ID.SC, PR.IP,	ID.RA-1, ID.SC-4, 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 Privacy Category	CSF and Privacy Subcategory
						ID.DE-P, CT.PO-P	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(1)	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(2)	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(3)	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(5)	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(6)	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(7)	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(8)	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		

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
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
SA-17(1)	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(2)	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(3)	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(4)	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(5)	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(6)	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(7)	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(8)	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

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
SA-17(9)	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
SA-22	Unsupported System Components		x	x	x		
SA-23	Specialization						