DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
Center for Consumer Information & Insurance Oversight
200 Independence Avenue SW
Washington, DC 20201

September 11, 2019

Frequently Asked Questions (FAQs) Regarding Enhanced Direct Enrollment (EDE) Participation Requirements for Non-Issuer Users of Primary EDE Entity Environments Serving Consumers in States with Federally-facilitated Exchanges (FFEs) and State-based Exchanges on the Federal Platform (SBE-FPs)

These FAQs clarify the requirements for prospective upstream non-issuer users of an EDE environment discussed in the document *Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements* (EDE Guidelines) available at the following link: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf.

Any prospective hybrid, non-issuer upstream EDE Entity, as clarified in this FAQ, planning to participate in EDE for PYs 2019 and 2020 must notify CMS as soon as possible of its intent to submit an audit consistent with the processes detailed in this document. These FAQs do not address issuer upstream EDE entities.[1]

For any questions regarding these FAQs, please contact DE Support at directenrollment@cms.hhs.gov.

1. What is an upstream EDE Entity?

As noted in Section IV.B, "Providing an EDE Environment to Other Entities," of the EDE Guidelines, a primary EDE Entity is an entity that develops, designs, and hosts its own EDE environment for its own use or for use by others. An upstream EDE Entity is an entity that will use an EDE environment provided by a primary EDE Entity and only differs in terms of minor branding changes to the EDE environment. In these FAQs, CMS is further clarifying the use of an EDE environment by upstream EDE Entities and a unique category of upstream EDE Entity: the hybrid, non-issuer upstream EDE Entity.

[1] Issuer upstream entities are subject to the requirements for an upstream EDE Entity as defined in the EDE Guidelines if the issuer upstream entity is only making "minor branding changes." If an issuer upstream entity is adding systems or functionality, the upstream issuer may be subject to additional requirements related to the additional systems or functionality. Consistent with the processes defined in the EDE Guidelines, issuer upstream entities that are adding systems or functionality should contact DE Support at directenrollment@cms.hhs.gov. Issuer upstream entities should also refer to Section VII.g of the *Enhanced Direct Enrollment Agreement Between Enhanced Direct Enrollment Entity and the Centers for Medicare & Medicaid Services for the Individual Market Federally-facilitated Exchanges and the State-Based Exchanges on the Federal Platform* (EDE Business Agreement).

2. What are the types of non-issuer users of a primary EDE Entity's EDE environment?

In these FAQs, CMS recognizes two models for participating in EDE representing different types of non-issuer users of a primary EDE Entity's EDE environment.

The first model is a "white-label" user (Model 1: white-label users) for which a primary EDE Entity would enable the user to make "minor branding changes only" to the primary EDE Entity's EDE environment as defined in the EDE Guidelines (e.g., adding a user's logo or name to an EDE environment).[2] These white-label users may include downstream and delegated agents and brokers (as defined in Section IV.D, "Downstream Third-party Agent and Broker Arrangements" of the EDE Guidelines) and other non-issuer users. The users who fall within this classification have added no functionality or systems to the primary EDE Entity's EDE environment that constitute part of the overall EDE end-user experience. Accordingly, CMS requires that users of this model conduct all aspects of the pre-application, application, enrollment, and post-enrollment experience[3] and any data collected necessary for those steps or for the purposes of any Authorized Functions[4] within the confines of a primary EDE Entity's audited and approved EDE environment.[5]

The second model is a user of a primary EDE Entity's EDE environment that adds functionality or systems to the primary EDE Entity's EDE environment such that the overall EDE end-user experience is modified beyond minor branding changes. CMS will refer to these users as hybrid, non-issuer upstream EDE Entities (Model 2: hybrid, non-issuer upstream EDE Entities).[6]

Model 1 white-label users do not need to maintain a unique partner ID, sign an EDE Business Agreement, or complete an EDE privacy and security audit. Model 2 hybrid, non-issuer upstream users are required to maintain a unique partner ID, sign the EDE Business Agreement, and submit an EDE privacy and security audit (please refer to question 4 below).

In both models, consistent with the description of an upstream EDE Entity from the EDE Guidelines, CMS allows for unique white-label branding and logos within the primary EDE Entity's environment. Please refer to the EDE Entity-initiated change request process for details regarding any additional user interface customization (see question 8 below).

The remaining questions in these FAQs further elaborate on the requirements and specifics of these two types of users.

3. What are examples of hybrid, non-issuer upstream EDE Entity arrangements?

A hybrid, non-issuer upstream EDE Entity arrangement, for example, may be primarily characterized by the presence of additional functionality or systems as part of the overall EDE end-user experience. The hybrid, non-issuer upstream EDE Entity arrangement may have split control or authority for creating and/or maintaining the systems and functionality that comprise

---

[2] The white-label user model is defined in Section VII.f. of the EDE Business Agreement.
[3] Collectively, CMS considers these elements to constitute the overall EDE end-user experience whether the end-users are consumers or agents/brokers.
[4] For a list of Authorized Functions for which an EDE Entity may use consumer's personally identifiable information, please refer to Section III.a., "Authorized Functions," of the EDE Business Agreement.
[5] All subsequent references to "data" collected in this document are inclusive of the data elements delineated in Section III.a., "Authorized Functions," of the EDE Business Agreement.
[6] The hybrid, non-issuer upstream model is defined in Section VII.h. of the EDE Business Agreement.

the totality of the EDE environment or end-user experience. For example, additional functionalities or systems may include any redirect or connection to another entity's system or website (e.g., the hybrid, non-issuer upstream EDE Entity's system or website) as part of the EDE pre-application, application, plan shopping, plan selection, enrollment, or post-enrollment experience, including any data collection prior to initiating or after completing the Exchange application and/or submitting the qualified health plan (QHP) enrollment to the applicable Exchange.

One key criterion that CMS will consider in evaluating relationships between primary EDE Entities and potential hybrid, non-issuer upstream EDE Entities is the transference of a consumer's experience or a consumer's data outside of the boundaries of a primary EDE Entity's audited and approved environment. For example, CMS would consider any arrangement that sends a consumer or transmits a consumer's data—either collected from the consumer for application and QHP enrollment purposes or provided by the FFE pursuant to such activities—outside the system boundaries of a primary EDE Entity's audited and approved EDE environment to constitute a hybrid, non-issuer upstream EDE Entity arrangement. The following examples illustrate situations that CMS would consider constituting a hybrid, non-issuer upstream EDE Entity relationship with a primary EDE Entity:

- Example Scenario 1: A hybrid, non-issuer upstream EDE Entity collects initial data from a consumer on its system for the purposes of completing an Exchange eligibility application or to display QHPs (i.e., plan selection/shopping), and then may redirect the consumer and/or their data to the primary EDE Entity for completing the eligibility application or submitting the enrollment transaction to the applicable Exchange.
- Example Scenario 2: A hybrid, non-issuer upstream EDE Entity provides a plan selection and enrollment process separate from the primary EDE Entity's EDE environment. This may involve any exchange of applicable consumer data (pre-application or post-application) between the hybrid, non-issuer upstream EDE Entity and the primary EDE Entity's EDE environment to complete plan selection and enrollment. The consumer or the consumer's data may then be relayed back to the primary EDE Entity's EDE environment for further action, including enrollment, post-enrollment communications, and post-enrollment management action items.
- Example Scenario 3: A hybrid, non-issuer upstream EDE Entity retrieves, stores, transfers, or manages consumer data obtained or collected through the primary EDE Entity's EDE environment outside of that environment (e.g., data stored by customer relationship management software hosted or maintained outside of the primary EDE Entity's environment for the hybrid, non-issuer upstream EDE Entity's use).

This FAQ is intended to clarify that the scope of an EDE environment for a hybrid, non-issuer upstream EDE Entity extends through the EDE Entity's entire Exchange application and QHP enrollment experience. This includes any data collected or received from the FFE or Exchange consumers (directly or indirectly via an agent or broker), any implementation of the EDE requirements as defined in the EDE Guidelines and accompanying requirements, any preliminary QHP shopping or eligibility information or estimates, and the QHP selection and enrollment experience.

If a non-issuer entity only redirects a consumer from its website to a primary EDE Entity's EDE environment to complete the entire EDE end-user experience (the scope of which is described

above), and the entity does not exchange any data or provide any Exchange-related information relevant to the EDE end-user experience, then it would *not* be considered a hybrid, non-issuer upstream entity relationship; instead, it may be considered a white-label relationship if branding for the non-issuer upstream EDE entity appears on the primary EDE Entity's website after the redirect.

This FAQ does not provide examples of the full universe of possible hybrid, non-issuer upstream EDE Entity relationships or arrangements.[7] For example, any arrangement where a non-issuer upstream entity implements an EDE program requirement instead of the primary EDE Entity (e.g., privacy and security controls, business requirements, agent/broker identity proofing, etc.) would likely mean the entity is a hybrid, non-issuer upstream EDE Entity.

4. What audit requirements exist for hybrid, non-issuer upstream EDE Entities to be approved to use a primary EDE Entity's EDE environment?

A prospective hybrid, non-issuer upstream EDE Entity must complete an operational readiness review[8] that includes a privacy and security audit that has been conducted by an independent, third-party Auditor. This audit must be conducted in compliance with the relevant requirements defined in the EDE Guidelines for a primary EDE Entity conducting a privacy and security audit (see Section V, "Selection of an Auditor"; Section VII, "Privacy and Security Audit Requirements and Scope"; Section VIII, "Required Auditor and Prospective EDE Entity Training"; and Section X, "Approval Process and Audit Submission Window"). The Auditor must evaluate the prospective hybrid, non-issuer upstream EDE Entity's compliance with all applicable EDE privacy and security controls and requirements;[9] however, the Auditor does not need to independently evaluate the implementation of any inherited common controls implemented by the approved primary EDE Entity.[10] The Auditor must verify that all non-inherited controls[11] are fully implemented and document any controls that have not been implemented. The Auditor must document any related mitigation steps the prospective hybrid, non-issuer upstream EDE Entity has taken. These requirements are consistent with the instructions in the EDE System Security and Privacy Plan (SSP) workbook.[12]

For a list of all of the applicable privacy and security controls (including the ones that are inherited from the approved primary EDE Entity), please refer to Table 1 and Table 2 in the Appendix of this document.

After CMS approves a hybrid, non-issuer upstream EDE Entity, the EDE Entity must implement and maintain an information security and privacy continuous monitoring (ISCM) program for its systems to maintain ongoing CMS approval. The ISCM requirements are detailed in the EDE

---

[7] Primary EDE Entities or hybrid, non-issuer upstream EDE Entities that have questions regarding permissible arrangements and the hybrid, non-issuer upstream EDE Entity model should contact DE Support at directenrollment@cms.hhs.gov.

[8] See 45 C.F.R. 155.221(b)(4) and (e).

[9] For a list of privacy and security controls that the auditor must evaluate to ensure compliance by the hybrid, non-issuer upstream EDE Entity, please refer to Table 1 in the Appendix of this document.

[10] For a list of inheritable common controls, please refer to Table 2 in the Appendix of this document.

[11] Non-inherited controls include any inheritable common controls that have not been inherited through the approved primary EDE Entity's implementation of the EDE environment.

[12] See page iv of the SSP available on CMS zONE at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

Guidelines and the ISCM Strategy Guide (available on CMS zONE at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials).

In addition to the privacy and security audit details above, hybrid, non-issuer upstream EDE Entities must maintain the following with CMS:

- A unique Data Services Hub (DSH)-issued Partner ID for processing all EDE-related or EDE-generated transactions;
- A signed EDE Business Agreement with CMS; and
- Operational information regarding the arrangement between the approved primary EDE Entity and the hybrid, non-issuer upstream EDE Entity.

Hybrid, non-issuer upstream EDE Entities, depending on the additional functionality they are offering (e.g., a distinct plan selection and enrollment experience), may also need to onboard with CMS as a web-broker.[13]

Hybrid, non-issuer upstream EDE Entities must also comply with the business audit post-approval activities, as applicable (e.g., those described in Section XI, "Processes for Changes to an Audited or Approved EDE Environment," of the EDE Guidelines).

5. What process would a primary EDE Entity follow to permit a hybrid non-issuer upstream EDE Entity to use its EDE environment?

A primary EDE Entity would use the EDE Entity-initiated change request (CR) process. Any request to permit a hybrid, non-issuer upstream EDE Entity to use its EDE environment would be categorized as a category 3 CR and require an independent audit consistent with the requirements detailed above. This process is detailed in Section XI "Processes for Changes to an Audited or Approved EDE Environment," of the EDE Guidelines.

6. What is the timeline for a prospective hybrid, non-issuer upstream EDE Entity to submit the required documentation to seek approval to use an EDE environment?

CMS will only accept privacy and security audit submissions for hybrid, non-issuer upstream EDE Entities outside of the previously established audit submission window that ended June 30, 2019. CMS will accept these submissions on a rolling basis. There is no guarantee that every prospective EDE Entity that submits a complete audit will receive approval prior to the 2020 OEP or during the 2019 calendar year. No prospective EDE Entity will be approved unless and until the prospective EDE Entity meets all applicable program requirements.

7. What responsibilities exist for an approved primary EDE Entity that provides for white-label use of its EDE environment by non-issuer users?

For an approved primary EDE Entity that is providing its environment to a white-label user, consistent with the definition in the response to question 2, the white-label user does not need to maintain a unique Partner ID, execute an EDE Agreement, or obtain an EDE privacy and security audit. The entirety of the environment and the overall EDE end-user experience must be designed, developed, and hosted by the approved primary EDE Entity consistent with the

[13] Primary EDE Entities or hybrid, non-issuer upstream EDE Entities with any questions regarding the additional functionality or systems they plan to add to an approved EDE system should contact DE Support at directenrollment@cms.hhs.gov.

standards clarified in these FAQs. White-label users cannot add functionality or systems to the approved primary EDE Entity's EDE environment.

Web-brokers who are approved primary EDE Entities and provide this type of white-label user arrangement to agents and brokers must comply with the requirements in 45 C.F.R. § 155.220(c)(4).

8. What is the process for requesting variations or customizations to the audited and approved user interface for either the white-label Model 1 or the hybrid, non-issuer upstream EDE Entity Model 2 detailed above?

EDE Entities must follow the EDE Entity-initiated CR process, as detailed in the EDE Guidelines, to request any modifications to an approved EDE environment other than "minor branding changes" as described above. Please refer to Section XI.C, "Other EDE Entity-initiated Change Requests," of the EDE Guidelines for more information.

9. Can an approved hybrid, non-issuer upstream EDE Entity provide access to its EDE environment to an upstream issuer or another hybrid, non-issuer upstream EDE Entity?

Currently, no, CMS does not allow this arrangement. Consistent with the EDE Guidelines and these FAQs, only a primary EDE Entity can provide an EDE environment to a hybrid, non-issuer upstream EDE Entity or an upstream issuer.

Appendix: Privacy and Security Controls for EDE

The hybrid, non-issuer upstream EDE Entity's Auditor must evaluate the hybrid, non-issuer upstream EDE Entity's compliance with the EDE privacy and security controls documented in Table 1.

Table 1: Auditable (Non-Inheritable and Hybrid) Controls

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
Access Control (AC)			
AC-1	Access Control Policy and Procedures		X
AC-2	Account Management		X
AC-2(1)	Automated System Account Management		X
AC-2(2)	Removal of Temporary/Emergency Accounts		X
AC-2(3)	Disable Inactive Accounts		X
AC-2(4)	Automated Audit Actions		X
AC-2(7)	Role-Based Schemes		X
AC-2(10)	Shared / Group Account Credential Termination		X
AC-5	Separation of Duties		X
AC-18	Wireless Access	X	
AC-18(1)	Authentication and Encryption	X	
AC-19	Access Control for Mobile Devices	X	
AC-19(5)	Full-Device / Container-Based Encryption	X	
AC-20	Use of External Information Systems	X	
AC-20(1)	Limits on Authorized Use	X	
AC-20(2)	Portable Storage Devices	X	
AC-21	Information Sharing	X	
AC-22	Publicly Accessible Content	X	
Awareness and Training (AT)			
AT-1	Security Awareness and Training Policy and Procedures	X	
AT-2	Security Awareness Training	X	
AT-2(2)	Insider Threat	X	
AT-3	Role-Based Security Training	X	
AT-4	Security Training Records	X	

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
Audit and Accountability (AU)			
AU-1	Audit and Accountability Policy and Procedures	X	
AU-2	Audit Events		X
AU-2(3)	Reviews and Updates		X
AU-6	Audit Review, Analysis, and Reporting		X
AU-6(1)	Process Integration		X
AU-6(3)	Correlate Audit Repositories		X
AU-7	Audit Reduction and Report Generation		X
AU-7(1)	Automatic Processing		X
AU-8	Time Stamps		X
AU-8(1)	Synchronization with Authoritative Time Source		X
AU-9	Protection of Audit Information		X
Security Assessment and Authorization (CA)			
CA-1	Security Assessment and Authorization Policies and Procedures		X
CA-2	Security Assessments		X
CA-2(1)	Independent Assessors		X
CA-3(5)	Restrictions on External System Connections	X	
CA-5	Plan of Action and Milestones	X	
CA-6	Security Authorization		X
CA-7	Continuous Monitoring	X	
CA-7(1)	Independent Assessment	X	
CA-9	Internal System Connections	X	
Configuration Management (CM)			
CM-1	Configuration Management Policy and Procedures		X
CM-2	Baseline Configuration		X
CM-2(1)	Reviews and Updates		X
CM-2(3)	Retention of Previous Configurations		X
CM-3	Configuration Change Control	X	
CM-3(2)	Test/Validate/Document Changes	X	
CM-4	Security Impact Analysis	X	
CM-4(1)	Separate Test Environments	X	
CM-9	Configuration Management Plan		X

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
Contingency Planning (CP)			
CP-2	Contingency Plan		X
CP-2(1)	Coordinate with Related Plans	X	
CP-2(3)	Resume Essential Missions/Business Functions	X	
CP-2(8)	Identify Critical Assets	X	
CP-3	Contingency Training	X	
CP-4	Contingency Plan Testing	X	
CP-4(1)	Coordinate with Related Plans	X	
CP-8	Telecommunications Services		X
CP-8(1)	Priority of Service Provisions		X
CP-8(2)	Single Points of Failure		X
CP-9	Information System Backup	X	
CP-9(1)	Testing for Reliability/Integrity	X	
CP-10	Information System Recovery and Reconstitution		X
CP-10(2)	Transaction Recovery		X
Identification and Authentication (IA)			
IA-1	Identification and Authentication Policy and Procedures	X	
Incident Response (IR)			
IR-1	Incident Response Policy and Procedures	X	
IR-2	Incident Response Training	X	
IR-3	Incident Response Testing	X	
IR-3(2)	Coordination with Related Plans	X	
IR-4	Incident Handling	X	
IR-4(1)	Automated Incident Handling Processes	X	
IR-5	Incident Monitoring	X	
IR-6	Incident Reporting	X	
IR-6(1)	Automated Reporting	X	
IR-7	Incident Response Assistance	X	
IR-7(1)	Automation Support for Availability of Information/Support	X	
IR-8	Incident Response Plan	X	
IR-9	Information Spillage Response	X	
Media Protection (MP)			
MP-1	Media Protection Policy and Procedures		X

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
MP-2	Media Access		X
MP-3	Media Marking		X
MP-4	Media Storage		X
MP-5	Media Transport		X
MP-5(4)	Cryptographic Protection		X
MP-6	Media Sanitization		X
MP-7	Media Use		X
MP-7(1)	Prohibit Use Without Owner		X
Physical and Environmental Protection (PE)			
PE-1	Physical and Environmental Protection Policy and Procedures		X
PE-2	Physical Access Authorizations		X
PE-2(1)	Access by Position / Role		X
PE-3	Physical Access Control		X
PE-4	Access Control for Transmission Medium		X
PE-5	Access Control for Output Devices		X
PE-6	Monitoring Physical Access		X
PE-6(1)	Intrusion Alarms/Surveillance Equipment		X
PE-8	Visitor Access Records		X
Planning (PL)			
PL-1	Security Planning Policy and Procedures		X
PL-2	System Security Plan		X
PL-2(3)	Plan/Coordinate with Other Organizational Entities		X
PL-4	Rules of Behavior		X
PL-4(1)	Social Media and Networking Restrictions		X
PL-8	Information Security Architecture		X
Personnel Security (PS)			
PS-1	Personnel Security Policy and Procedures	X	
PS-2	Position Risk Designation	X	
PS-3	Personnel Screening	X	
PS-4	Personnel Termination	X	
PS-5	Personnel Transfer	X	
PS-6	Access Agreements	X	
PS-7	Third-Party Personnel Security	X	

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
PS-8	Personnel Sanctions	X	
Risk Assessment (RA)			
RA-1	Risk Assessment Policy and Procedure		X
RA-3	Risk Assessment		X
RA-5	Vulnerability Scanning		X
System and Services Acquisition (SA)			
SA-5	Information System Documentation		X
System and Communications Protection (SC)			
SC-28	Protection of Information at Rest	X	
SC-CMS-1	Electronic mail	X	
Accountability, Audit, and Risk Management (AR)			
AR-1	Governance and Privacy Program		X
AR-2	Privacy Impact and Privacy Program		X
AR-4	Privacy Monitoring and Auditing		X
AR-5	Privacy Awareness and Training	X	
AR-8	Accounting of Disclosures	X	
Data Quality and Integrity (DI)			
DI-1	Data Quality		X
DI-1(1)	Validate PII	X	
Data Minimization and Retention (DM)			
DM-3	Minimization of PII Used in Testing, Training, and Research		X
DM-3 (1)	Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques		X
Individual Participation and Redress (IP)			
IP-1	Consent		X
IP-2	Individual Access		X
IP-3	Redress		X
IP-4	Complaint Management		X
IP-4(1)	Complaint Management/Response Times		X
Security (SE)			
SE-1	Inventory of Personally Identifiable Information		X
SE-2	Privacy Incident Response		X
Transparency (TR)			
TR-1	Privacy Notice		X

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
TR-3	Dissemination of Privacy Program Information		X
Use Limitation (UL)			
UL-1	Internal Use	X	
UL-2	Information Sharing with Third Parties	X	

Table 2 reflects the Inheritable Common Controls that the hybrid, non-issuer upstream EDE Entity can potentially inherit from the primary EDE Entity. The hybrid, non-issuer upstream EDE Entity's Auditor does not need to independently evaluate the implementation of any inherited common controls implemented by the approved primary EDE Entity.

Table 2: Inheritable Common Controls

Control #	Security/Privacy Control Name
Access Control (AC)	
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-6	Least Privilege
AC-6(1)	Authorize Access to Security Functions
AC-6(2)	Non-Privileged Access for Non-Security Functions
AC-6(5)	Privileged Accounts
AC-6(9)	Auditing Use of Privileged Functions
AC-6(10)	Prohibit Non-Privileged Users from Executing Privileged Functions
AC-7	Unsuccessful Logon Attempts
AC-8	System Use Notification
AC-10	Concurrent Session Control
AC-11	Session Lock
AC-11(1)	Pattern-Hiding Displays
AC-12	Session Termination
AC-14	Permitted Actions Without Identification or Authentication
AC-17	Remote Access
AC-17(1)	Automated Monitoring/Control
AC-17(2)	Protection of Confidentiality/Integrity Using Encryption
AC-17(3)	Managed Access Control Points
AC-17(4)	Privileged Commands/Access
AC-17(9)	Disconnect / Disable Access
Audit and Accountability (AU)	
AU-3	Content of Audit Records
AU-3(1)	Additional Audit Information
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-5(1)	Audit Storage Capacity
AU-9(4)	Access by Subset of Privileged Users
AU-10	Non-Repudiation
AU-11	Audit Record Retention

Control #	Security/Privacy Control Name
AU-12	Audit Generation
Security Assessment and Authorization (CA)	
CA-3	System Interconnections
CA-8	Penetration Testing
CA-8(1)	Independent Penetration Agent or Team
Configuration Management (CM)	
CM-5	Access Restrictions for Change
CM-5(1)	Automated Access Enforcement/Auditing
CM-5(5)	Limit Production/Operational Privileges
CM-6	Configuration Settings
CM-6(1)	Automated Central Management/ Application/Verification
CM-7	Least Functionality
CM-7(1)	Periodic Review
CM-7(2)	Prevent Program Execution
CM-7(4)	Unauthorized Software/Blacklisting
CM-8	Information System Component Inventory
CM-8(1)	Updates During Installations/Removals
CM-8(3)	Automated Unauthorized Component Detection
CM-8(5)	No Duplicate Accounting of Components
CM-10	Software Usage Restrictions
CM-10(1)	Open Source Software
CM-11	User-Installed Software
Contingency Planning (CP)	
CP-1	Contingency Planning Policy and Procedures
CP-2(2)	Capacity Planning
CP-6	Alternate Storage Site
CP-6(1)	Separation from Primary Site
CP-6(3)	Accessibility
Identification and Authentication (IA)	
IA-2	Identification and Authentication (Organizational Users)
IA-2(1)	Network Access to Privileged Accounts
IA-2(2)	Network Access to Non-Privileged Accounts
IA-2(3)	Local Access to Privileged Accounts
IA-2(8)	Network Access to Privileged Accounts – Replay Resistant
IA-2(11)	Remote Access – Separate Device
IA-3	Device Identification and Authentication

Control #	Security/Privacy Control Name
IA-4	Identifier Management
IA-5	Authenticator Management
IA-5(1)	Password-Based Authentication
IA-5(2)	PKI-Based Authentication
IA-5(3)	In-Person or Trusted Third-Party Registration
IA-5(7)	No Embedded Unencrypted Static Authenticators
IA-5(11)	Hardware Token-Based Authentication
IA-6	Authenticator Feedback
IA-7	Cryptographic Module Authentication
IA-8	Identification and Authentication (Non-Organizational Users)
IA-8(2)	Acceptance of Third-Party Credentials
Maintenance (MA)	
MA-1	System Maintenance Policy and Procedures
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-3(1)	Inspect Tools
MA-3(2)	Inspect Media
MA-3(3)	Prevent Unauthorized Removal
MA-4	Nonlocal Maintenance
MA-4(1)	Auditing and Review
MA-4(2)	Document Nonlocal Maintenance
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
Risk Assessment (RA)	
RA-5(1)	Update Tool Capability
RA-5(2)	Update by Frequency/Prior to New Scan/When Identified
RA-5(5)	Privileged Access
System and Services Acquisition (SA)	
SA-1	System and Services Acquisition Policy and Procedures
SA-2	Allocation of Resources
SA-3	System Development Life Cycle
SA-4	Acquisition Process
SA-4(1)	Functional Properties of Security Controls
SA-4(2)	Design/Implementation Information for Security Controls
SA-4(9)	Functions/Ports/Protocols/Services in Use
SA-8	Security Engineering Principles

Control #	Security/Privacy Control Name
SA-9	External Information System Services
SA-10	Developer Configuration Management
SA-11	Developer Security Testing and Evaluation
SA-15	Development Process, Standards, and Tools
SA-17	Developer Security Architecture and Design
SA-22	Unsupported System Components
System and Communications Protection (SC)	
SC-1	System and Communications Protection Policy and Procedures
SC-2	Application Partitioning
SC-4	Information in Shared Resources
SC-5	Denial of Service Protection
SC-6	Resource Availability
SC-7	Boundary Protection
SC-7(3)	Access Points
SC-7(4)	External Telecommunications Services
SC-7(5)	Deny by Default/Allow by Exception
SC-7(7)	Prevent Split Tunneling for Remote Devices
SC-7(8)	Route Traffic to Authenticated Proxy Servers
SC-7(12)	Host-Based Protection
SC-7(13)	Isolation of Security Tools/Mechanisms/Support Components
SC-7(18)	Fail Secure
SC-8	Transmission Confidentiality and Integrity
SC-8(1)	Cryptographic or Alternate Physical Protection
SC-8(2)	Pre/Post Transmission Handling
SC-10	Network Disconnect
SC-12	Cryptographic Key Establishment and Management
SC-12(2)	Symmetric Keys
SC-13	Cryptographic Protection
SC-17	Public Key Infrastructure Certificates
SC-18	Mobile Code
SC-19	Voice Over Internet Protocol
SC-20	Secure Name/Address Resolution Service (Authoritative Source)
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22	Architecture and Provisioning for Name/Address Resolution Service
SC-23	Session Authenticity
SC-24	Fail in Known State

Control #	Security/Privacy Control Name
System and Information Integrity (SI)	
SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-2(2)	Automated Flaw Remediation Status
SI-2(3)	Time to Remediate Flaws / Benchmarks for Corrective Actions
SI-3	Malicious Code Protection
SI-3(2)	Automatic Updates
SI-4	Information System Monitoring
SI-4(1)	System-Wide Intrusion Detection System
SI-4(4)	Inbound and Outbound Communications Traffic
SI-4(5)	System-Generated Alerts
SI-5	Security Alerts, Advisories, and Directives
SI-6	Security Function Verification
SI-7	Software, Firmware, and Information Integrity
SI-7(1)	Integrity Checks
SI-7(7)	Integration of Detection and Response
SI-8	Spam Protection
SI-8(2)	Automatic Updates
SI-10	Information Input Validation
SI-11	Error Handling
SI-12	Information Handling and Retention
SI-16	Memory Protection
Authority and Purpose (AP	
AP-1	Authority to Collect
AP-2	Purpose Specification
Accountability, Audit, and Risk Management (AR)	
AR-7	Privacy-enhanced System Design and Development
Data Minimization and Retention (DM)	
DM-1	Minimization of Personally Identifiable Information
DM-1(1)	Minimization of PII/Locate/Remove/Redact/Anonymize PII
DM-2	Data Retention and Disposal
DM-2 (1)	Data Retention and Disposal/System Configuration