

CP-2 Contingency Plan

CP-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for developing a contingency plan for the application and database system that: Identifies essential missions and business functions and associated contingency requirements; provides recovery objectives, restoration priorities, and metrics; addresses contingency roles, responsibilities, assigned individuals with contact information; addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and is reviewed and approved by designated officials within the organization.
Part b	The FCCP Customer is responsible for distributing copies of the contingency plan to key personnel for the application or database.
Part c	The FCCP Customer is responsible for coordinating contingency planning activities with incident handling activities for the application and database.
Part d	The FCCP Customer is responsible for reviewing the contingency plan for the application and database.
Part e	The FCCP Customer is responsible for revising the contingency plan to address changes to the application, database, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
Part f	The FCCP Customer is responsible for communicating contingency plan changes to key contingency roles for the application and database.
Part g	The FCCP Customer is responsible for protecting the Contingency Plan from unauthorized disclosure and modification for the application and database.

CP-2 (1) Control Enhancement

CP-2 (1) What is the solution and how is it implemented?
The FCCP Customer is responsible for coordinating contingency plan development for the application and database with organizational elements responsible for related plans.

CP-2 (2) Control Enhancement

CP-2 (2) What is the solution and how is it implemented?
The FCCP Customer is responsible for conducting capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations for the application and database.

CP-2 (3) Control Enhancement

CP-2 (3) What is the solution and how is it implemented?
The FCCP Customer Administrator works in concert with DGS FCCP ITCP staff planning for the resumption of essential missions and business functions within 4 hours of contingency plan activation.

CP-2 (8) Control Enhancement

CP-2 (8) What is the solution and how is it implemented?	
The FCCP Customer works with the DGS FCCP Program Manager and Government System Owner to identify critical information system assets supporting essential missions and business functions.	

CP-3 Contingency Training

CP-3 What is the solution and how is it implemented?	
The FCCP Customer is responsible for training personnel in their contingency roles and responsibilities with respect to the application and database, and provides refresher training.	

CP-4 Contingency Plan Testing

CP-4 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for tests and/or exercises the contingency plan for the information system to determine the plan's effectiveness and the organization's readiness to execute the plan.
Part b	The FCCP Customer is responsible for reviewing the contingency plan test/exercise results.
Part c	The FCCP Customer is responsible for initiating corrective actions for the database and application as part of the lessons learned from the results of the Contingency Plan Test.

CP-4 (1) Control Enhancement

CP-4 (1) What is the solution and how is it implemented?	
The FCCP Customer is responsible for coordinating contingency plan testing and/or exercises for the application and database with organizational elements responsible for related plans.	

CP-9 Information System Backup

CP-9 What is the solution and how is it implemented?	
Part b	The FCCP Customer is responsible for conducting backups of system-level information contained in the application and database.
Part c	The FCCP Customer is responsible for conducting backups of application and database documentation including security-related documentation.
Part d	The FCCP Customer will describe in its SSP how it protects the confidentiality, integrity, and availability of backup information at storage locations for the database and application.

CP-10 Information System Recovery and Reconstitution

CP-10 (2) Control Enhancement

CP-10 (2) What is the solution and how is it implemented?

The FCCP Customer is responsible for explaining in its SSP how it implements transaction recovery for systems that are transaction-based.

1.7 IDENTIFICATION AND AUTHENTICATION (IA)

IA-1 Identification and Authentication Policy and Procedures

IA-1 What is the solution and how is it implemented?
--

Part a	The FCCP Customer is responsible for having policies for this control family.
---------------	---

Part b	The FCCP Customer is responsible for having procedures for this control family.
---------------	---

IA-2 User Identification and Authentication

IA-2 What is the solution and how is it implemented?
--

The FCCP Customer is responsible for uniquely identifying and authenticating organizational users for the application and database (or processes acting on behalf of organizational users).

IA-2 (1) Control Enhancement

IA-2 (1) What is the solution and how is it implemented?
--

The FCCP CPM Customer Administrator is responsible for following the same steps mentioned above. Network Access to all servers and network devices are required to be made from a single remote desktop server (FCCP Jump Box), provided the user has access privileges defined in AD. To access the Jump Box, user must establish a Cisco AnyConnect VPN Client (TLS Version 1.2) connection using two-factor authentication. Two-factor authentication is achieved using a combination of a unique pin and randomly generated passcode from the RSA hardware token. DGS FCCP Domain Administrators assign the FCCP CPM Customer Administrator hardware tokens.
--

IA-2 (2) Control Enhancement

IA-2 (2) What is the solution and how is it implemented?
--

The FCCP Customer is responsible for using multifactor authentication for network access to non-privileged accounts for the application and database.

IA-2 (5) Control Enhancement

IA-2 (5) What is the solution and how is it implemented?	
The FCCP Customer will describe in its SSP how it requires individuals to be authenticated with an individual authenticator when a group authenticator is employed for the database and application.	

IA-2 (8) Control Enhancement

IA-2 (8) What is the solution and how is it implemented?	
The FCCP Customer is responsible for using replay-resistant authentication mechanisms for network access to privileged accounts for the application and database. The mechanisms are approved and accepted by the JAB.	

IA-2 (12) Control Enhancement

IA-2 (12) What is the solution and how is it implemented?	
The FCCP Customer works with the Government System Owner to gather their specific requirements for a PIV, CAC, or HSPD-12 implementation and communicates these requirements to the DGS FCCP Program Manager, DGS FCCP System Administrator, and DGS FCCP Network Administrator to configure appropriately.	

IA-4 Identifier Management

IA-4 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for receiving authorization from a designated organizational official to assign a user or device identifier for the application and database.
Part b	The FCCP Customer is responsible for selecting an identifier that uniquely identifies an individual attempting to access the application and database.
Part c	The FCCP Customer is responsible for assigning the user identifier to the intended party for the application and database.
Part d	The FCCP Customer is responsible for preventing reuse of user identifiers for the application and database.
Part e	The FCCP Customer is responsible for disabling the user identifier for the application and database. The time period is approved and accepted by JAB.

IA-4 (4) Control Enhancement

IA-4 (4) What is the solution and how is it implemented?	
The FCCP Customer is responsible for managing user identifiers by uniquely identifying the user of the application and database using a particular status.	

IA-5 Authenticator Management

IA-5 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator for the application and database.
Part b	The FCCP Customer is responsible for establishing initial authenticator content for authenticators defined by the organization.
Part c	The FCCP Customer is responsible for ensuring that authenticators for the application and database have sufficient strength of mechanism for their intended use.
Part d	The FCCP Customer is responsible for establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators for the application and database.
Part e	The FCCP Customer is responsible for changing default content of authenticators for the application and database upon information system installation.
Part f	The FCCP Customer is responsible for establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators for the application and database. Minimum password lifetime must be 1 day, and maximum password lifetime must be 60 days.
Part g	The FCCP Customer is responsible for Changing/refreshing authenticators for the application and database after an organization-defined time period.
Part h	The FCCP Customer is responsible for protecting authenticator content for the application and database from unauthorized disclosure and modification.
Part i	The FCCP Customer is responsible for requiring application and database users to take, and having devices implement, specific measures to safeguard authenticators.
Part j	The FCCP Customer is responsible for changing authenticators for group/role accounts when membership to those accounts changes for the database and application.

IA-5 (1) Control Enhancement

IA-5 (1) What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for enforces minimum password complexity for the application and database.
Part b	The FCCP Customer is responsible for enforcing an organization-defined number of character changes for application and database passwords when new passwords are created.
Part c	The FCCP Customer is responsible for encrypting application and database passwords in storage and in transmission.
Part d	The FCCP Customer is responsible for enforcing password minimum and maximum lifetime restrictions for the application and database.
Part e	The FCCP Customer is responsible for prohibiting password reuse for the application and database.
Part f	The FCCP Customer is responsible for describing in its SSP whether it allows the use of temporary password and how it enforces an immediate change to a permanent password for the database and application.

IA-5 (2) Control Enhancement

IA-5 (2) What is the solution and how is it implemented?	
2 2 1 1 Part a	The FCCP Customer is responsible for describing in its SSP how its applications and databases validate certificates by constructing a certification path with status information from an accepted trust anchor. The FCCP Customer will receive certificates for any services requiring the use of certificates within the DGS FCCP private network. For any public-facing services that require certificates, the FCCP Customer would use a third-party certificate authority.
Part b	The FCCP Customer is responsible for describing in its SSP how its applications and databases enforce authorized access to the private key. This process will be the same for the FCCP Customer as it is described for the DGS FCCP, however it will apply to public-facing services that require certificates, and the FCCP Customer would use a third-party certificate authority.
Part c	The FCCP Customer is responsible for describing in its SSP how its applications and databases map the authenticated identity to the user account for its users. This process will be the same for the FCCP Customer as it is described for the DGS FCCP, however it will apply to public-facing services that require certificates, and the FCCP Customer would use a third-party certificate authority.
Part d	The FCCP Customer is responsible for describing in its SSP how it implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network for public certificates related to the database and application.

IA-5 (4) Control Enhancement

IA-5 (4) What is the solution and how is it implemented?
1 The FCCP Customer is responsible for describing in its SSP how it employs automated tools to determine if password authenticators are sufficiently strong to satisfy FedRAMP password complexity requirements for the database and application.

IA-5 (6) Control Enhancement

IA-5 (6) What is the solution and how is it implemented?
1 The FCCP Customer is responsible for protecting authenticators commensurate with the classification or sensitivity of the information accessed in the application and database.

IA-5 (7) Control Enhancement

IA-5 (7) What is the solution and how is it implemented?
— The FCCP Customer is responsible for explaining in their SSP how they ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys for use in the application and database.

IA-5 (11) Control Enhancement

IA-5 (11) What is the solution and how is it implemented?
1 The FCCP Customer will describe in its SSP how it implements hardware token based authentication mechanisms to satisfy organization-defined token quality requirements.

IA-6 Authenticator Feedback

1

IA-6 What is the solution and how is it implemented?	
	The FCCP Customer is responsible for system obscuring feedback of authentication information during the authentication process for the application and database to protect the information from possible exploitation/use by unauthorized individuals.

IA-8 Identification and Authentication (Non-Organizational Users)

IA-8 (1) Control Enhancement

1

IA-8 (1) What is the solution and how is it implemented?	
	The FCCP Customer will describe in its SSP how databases and applications accept and electronically verify Personal Identity Verification (PIV) credentials from other federal agencies. <i>not</i>

IA-8 (2) Control Enhancement

1

IA-8 (2) What is the solution and how is it implemented?	
	The FCCP Customer will describe in its SSP how its databases and applications accepts only FICAM-approved third-party credentials.

IA-8 (4) Control Enhancement

1

IA-8 (4) What is the solution and how is it implemented?	
	The FCCP Customer will describe in its SSP how it conforms to FICAM-issued profiles for the database and application.

Rani & Tim

1.8 INCIDENT RESPONSE (IR)

IR-1 Incident Response Policy and Procedures

IR-1 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for having policies for this control family.
Part b	The FCCP Customer is responsible for having procedures for this control family.

IR-2 Incident Response Training

IR-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for training personnel in their incident response roles and responsibilities with respect to the application and database.
Part b	The FCCP Customer is responsible for providing refresher incident response training for those with IR roles and responsibilities.
Part c	The FCCP Customer is responsible for providing refresher incident response training for those with IR roles and responsibilities for the database and application at least annually thereafter.

IR-3 Incident Response Testing

IR-3 What is the solution and how is it implemented?	
The FCCP Customer is responsible for testing and/or exercising the incident response capability for the application and database to determine the incident response effectiveness and documents the results.	

IR-3 (2) Control Enhancement

IR-3 (2) What is the solution and how is it implemented?	
The FCCP Customer coordinates incident response testing with the following organizational elements responsible for related plans:	
• FCCP Customer Program Manager • FCCP Customer Administrator • Government System Owner (optional)	

IR-4 Incident Handling

IR-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for implements an incident handling capability for application and database security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
Part b	The FCCP Customer is responsible for coordinating incident handling activities with contingency planning activities for the database and application.
Part c	The FCCP Customer is responsible for incorporating lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

IR-4 (1) Control Enhancement

IR-4 (1) What is the solution and how is it implemented?	
The FCCP Customer is responsible for employing automated mechanisms to support the incident handling process for the application and database.	

IR-5 Incident Monitoring

IR-5 What is the solution and how is it implemented?	
The FCCP Customer is responsible for tracking and documenting application and database security incidents.	

IR-6 Incident Reporting

IR-6 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for reporting suspected security incidents to the organizational incident response capability and DGS FCCP SIRT Team Leader via phone or email within an organization-defined time period.
Part b	The FCCP Customer is responsible for reporting security incident information to designated authorities.

IR-6 (1) Control Enhancement

IR-6 (1) What is the solution and how is it implemented?
The FCCP Customer is responsible for employing automated mechanisms to assist in the reporting of security incidents.

IR-7 Incident Response Assistance

IR-7 What is the solution and how is it implemented?
The FCCP Customer is responsible for providing an incident response support resource for the application and database, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

IR-7 (1) Control Enhancement

IR-7 (1) What is the solution and how is it implemented?
The FCCP Customer is responsible for employing automated mechanisms to increase the availability of incident response related information and support for the application and database.

IR-7 (2) Control Enhancement

IR-7 (2) What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for establishing a direct, cooperative relationship between its incident response capability and external providers of information system protection capability for the application and database.
Part b	The FCCP Customer is responsible for identifying organizational incident response team members for the application and database to the external providers.

IR-8 Incident Response Plan

IR-8 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for developing an incident response plan for the application and database that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization. 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and is reviewed and approved by designated officials within the organization.
Part b	The FCCP Customer is responsible for distributing copies of the incident response plan to all application and database personnel with IR responsibilities.
Part c	The FCCP Customer is responsible for reviewing the incident response plan for the application and database.
Part d	The FCCP Customer is responsible for revising the incident response plan to address application/database changes or problems encountered during plan implementation, execution, or testing.
Part e	The FCCP Customer is responsible for communicating incident response plan changes for the application and database to all personnel with IR responsibilities.
Part f	The FCCP Customer is responsible for describing in its SSP how it protects the incident response plan from unauthorized disclosure and modification for the database and application.

IR-9 Information Spillage Response

IR-9 What is the solution and how is it implemented?	
Part a	The FCCP Customer will describe in its SSP how it identifies other information systems or system components that may have been subsequently contaminated in the database and application.
Part b	The FCCP Customer will describe in its SSP any additional organization-defined actions to be taken in the event of an information spill related to the database and application.
Part c	The FCCP Customer will describe in its SSP how it identifies other information systems or system components that may have been subsequently contaminated in the database and application.
Part d	The FCCP Customer will describe in its SSP any additional organization-defined actions to be taken in the event of an information spill related to the database and application.
Part e	The FCCP Customer will describe in its SSP how it identifies other information systems or system components that may have been subsequently contaminated in the database and application.
Part f	The FCCP Customer will describe in its SSP any additional organization-defined actions to be taken in the event of an information spill related to the database and application.

IR-9 (1) Control Enhancement

IR-9 (1) What is the solution and how is it implemented?
The FCCP Customer will identify in its SSP the assigned role with responsibility for responding to information spills on the database and application.

IR-9 (2) Control Enhancement

IR-9 (2) What is the solution and how is it implemented?
The FCCP Customer will describe in its SSP how they provide information spillage response training for the database and application.

IR-9 (3) Control Enhancement

IR-9 (3) What is the solution and how is it implemented?
The FCCP Customer will describe in its SSP how they implement responses to incidents to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions in the database and application.

IR-9 (4) Control Enhancement

IR-9 (4) What is the solution and how is it implemented?
This control is designed for federal government employees. As contractors we comply with this security safeguard and other federal mandates by signing Non-Disclosure Agreements (NDA), Memorandum of Understanding (MOU), Rules of Behavior, Confidentiality Agreements, and any Acceptable Use Policies. The federal agency is responsible for specific actions that should be taken if personnel are exposed to information not within assigned access authorizations.

1.9 MAINTENANCE (MA)

MA-1 System Maintenance Policy and Procedures

MA-1 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for having policies for this control family.
Part b	The FCCP Customer is responsible for having procedures for this control family.

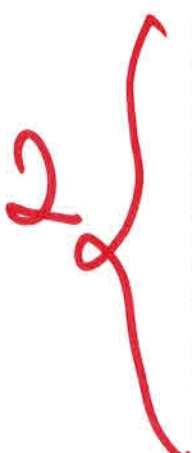
MA-2 Controlled Maintenance

MA-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for scheduling, performing, documenting, and reviewing records of maintenance and repairs on application and database components in accordance with manufacturer or vendor specifications and/or organizational requirements.
Part b	The FCCP Customer is responsible for controlling all maintenance activities for the application and database, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.
Part c	The FCCP Customer is responsible for requiring that a designated official explicitly approve the removal of the information system or system components, pertaining to the application and database, from organizational facilities for off-site maintenance or repairs.
Part e	The FCCP Customer is responsible for checking all potentially impacted security controls to verify that the controls, applicable to the application and database, are still functioning properly following maintenance or repair actions.
Part f	The FCCP Customer describes in its SSP which maintenance-related information is included in the maintenance record for the database and application.

MA-3 Maintenance Tools

MA-3 What is the solution and how is it implemented?	
The FCCP Customer is responsible for approving, controlling, monitoring the use of, and maintains on an ongoing basis, information system maintenance tools for the application and database.	

MA-4 Remote Maintenance



MA-4 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for authorizing, monitoring, and controlling non-local maintenance and diagnostic activities for the application and database.
Part b	The FCCP Customer is responsible for allowing the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the application and database.
Part c	The FCCP Customer is responsible for employing strong identification and authentication techniques for the application and database in the establishment of non-local maintenance and diagnostic sessions.
Part d	The FCCP Customer is responsible for maintaining records for non-local maintenance and diagnostic activities for the application and database.
Part e	The FCCP Customer is responsible for terminating all sessions and network connections when non-local maintenance for the application and database is completed.

MA-4 (2) Control Enhancement



MA-4 (2) What is the solution and how is it implemented?	
The FCCP Customer is responsible for documenting in its security plan the the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections for the database and application, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	

MA-5 Maintenance Personnel



MA-5 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for establishing a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel for the application and database.
Part b	The FCCP Customer is responsible for ensuring that personnel performing maintenance on the application and database have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.
Part c	The FCCP Customer is responsible for ensuring that personnel performing maintenance on the application and database have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

MA-5 (1) Control Enhancement

MA-5 (1) What is the solution and how is it implemented?	
1 1 Part a	The FCCP Customer will describe in its SSP how it implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens that include the following requirements.
Part b	The FCCP Customer will describe in its SSP how it develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. These would typically include database views, constrained interfaces, restricted user interfaces, and application partitioning.

1.10 MEDIA PROTECTION (MP)

MP-2 Media Access

MP-2 What is the solution and how is it implemented?	
—	The FCCP Customer would describe the security mechanisms it employs to restrict access to non-digital media to authorized individuals in its SSP.

MP-4 Media Storage

MP-4 What is the solution and how is it implemented?	
— 1 Part a	The FCCP Customer will describe in its SSP how non-digital media is physically protected and secured.
Part b	The FCCP Customer will describe in its SSP how it Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

MP-5 Media Transport

MP-5 What is the solution and how is it implemented?	
— — Part a	The FCCP Customer will describe in its SSP how it protects and controls non-digital media during transport outside of control areas.
Part d	The FCCP Customer will describe in its SSP how it Restricts the activities associated with transport of such media to authorized personnel.

MP-6 Media Sanitization and Disposal

MP-6 What is the solution and how is it implemented?	
1 1 Part a	The FCCP Customer will describe in its SSP how it sanitizes non-digital information system media, prior to disposal, release out of organizational control, or release for reuse.
Part b	The FCCP Customer describes in its SSP how it employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

MP-6 (2) Control Enhancement

1

MP-6 (2) What is the solution and how is it implemented?	
	The FCCP Customer will describe in its SSP how it tests sanitization equipment and procedures to verify that the intended sanitization is being achieved in the database and application.

1.11 PLANNING (PL)

PL-1 Security Planning Policy and Procedures

IA-1 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for having policies for this control family.
Part b	The FCCP Customer is responsible for having procedures for this control family.

PL-2 System Security Plan

2

PL-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for developing an SSP for the application and database that: • Is consistent with the organization's enterprise architecture; • Explicitly defines the authorization boundary for the system; • Describes the operational context of the information system in terms of missions and business processes; • Provides the security categorization of the information system including supporting rationale; • Describes the operational environment for the information system; • Describes relationships with or connections to other information systems ; • Provides an overview of the security requirements for the system; • Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and • Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
Part b	The FCCP Customer is responsible for explaining how it distributes copies of the security plan and communicates subsequent changes to the plan to organization-defined personnel or roles.
Part c	The FCCP Customer is responsible for reviewing the security plan for the application and database.
Part d	The FCCP Customer is responsible for updating the plan to address changes to the application or database, or problems identified during plan implementation or security control assessments.
Part e	The FCCP Customer is responsible for describing in its SSP how it protects the security plan from unauthorized disclosure and modification.

PL-2 (3) Control Enhancement

PL-2 (3) What is the solution and how is it implemented?	
The FCCP Customer will describe in its SSP how they plan and coordinate security-related activities affecting the information system with its organization-defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities.	

PL-4 Rules of Behavior

PL-4 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for establishing and making readily available to all application and database users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage. The FCCP Customer is responsible for communicating any changes to their RoB to all application and database users.
Part b	The FCCP Customer is responsible for receiving signed acknowledgment from application and database users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the application and database.
Part c	The FCCP Customer is responsible for reviewing and updating the rules of behavior for the database and application support
Part d	The FCCP Customer is responsible for requiring individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

PL-4 (1) Control Enhancement

PL-4 (1) What is the solution and how is it implemented?
The FCCP Customer includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

PL-8 Information Security Architecture

PL-8 What is the solution and how is it implemented?	
Part a	The FCCP Customer will describe in its SSP how they 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services.
Part b	The FCCP Customer will describe in its SSP how they review and update the information security architecture at least annually or when a significant change occurs to reflect updates in the enterprise architecture.
Part c	The FCCP Customer will describe in its SSP how they ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

1.12 PERSONNEL SECURITY (PS)

PS-1 Personnel Security Policy and Procedures

PS-1 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for having policies for this control family.
Part b	The FCCP Customer is responsible for having procedures for this control family.

PS-2 Position Categorization

PS-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for assigning a risk designation to all positions associated with the application and database.
Part b	The FCCP Customer is responsible for establishes screening criteria for individuals filling positions to manage the application and database.
Part c	The FCCP Customer is responsible for reviewing and revising position risk designations for application and database stakeholders.

PS-3 Personnel Screening

PS-3 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for screening individuals prior to authorizing access to the application and database.
Part b	The FCCP Customer is responsible for rescreening individuals for the application and database.

PS-3 (3) Control Enhancement

PS-3 (3) What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for ensuring its employees have valid access authorizations that are demonstrated by assigned official government duties.
Part b	The FCCP Customer is responsible for ensuring its employees satisfy personnel-screening criteria in support of government contracts.

PS-4 Personnel Termination

PS-4 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for the following when terminating an employee with roles and responsibilities associated with the database and application: (a) Terminates information system access; (b) Conducts exit interviews; (c) Retrieves all security-related organizational information system-related property; and (d) Retains access to organizational information and information systems formerly controlled by terminated individual
Part b	The FCCP Customer is responsible for terminating/revoking any authenticators/credentials associated with the individual for the database and application.
Part c	The FCCP Customer is responsible conducting and documenting exit interviews for application and database administrators.
Part d	The FCCP Customer is responsible for retrieving all security-related and application and database system-related property.
Part e	The FCCP Customer is responsible for retaining access to application and database information formerly controlled by terminated individual.
Part f	The FCCP Customer is responsible for notifying HR/Legal departments when an individual is terminated for the database and application.

PS-5 Personnel Transfer

PS-5 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for reviewing and confirming ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization.
Part b	The FCCP Customer is responsible for initiating organization-defined transfer or reassignment actions] within organization-defined time period following the formal transfer action.
Part c	The FCCP Customer is responsible for modifying access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
Part d	The FCCP Customer is responsible for notifying organization-defined personnel or roles within 5 days of the time period following the formal transfer action.

PS-6 Access Agreements

PS-6 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for developing and documenting access agreements for the application and database.
Part b	The FCCP Customer is responsible for reviewing/updating the access agreements for the application and database.
Part c	The FCCP Customer is responsible for ensuring individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.

PS-7 Third-Party Personnel Security

PS-7 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for establishing requirements including security roles and responsibilities for the database and application
Part b	The FCCP Customer is responsible for requiring third-party providers to comply with established personnel security policies and procedures for the database and application.
Part c	The FCCP Customer is responsible for documenting personnel security requirements for the database and application.
Part d	The FCCP Customer is responsible for requiring third-party providers notify organization-defined personnel of any personnel transfers or terminations of third-party personnel who possess organizational credentials/badges of database and application privileges within a week.
Part e	The FCCP Customer is responsible for monitoring compliance for third-party providers as part of the annual audit under Continuous Monitoring for the database and application.

PS-8 Personnel Sanctions

PS-8 What is the solution and how is it implemented?	
Part a	The FCCP Customer describes in its SSP how it employs a formal sanctions process for personnel failing to comply with established information security policies and procedures for the database and application.
Part b	The FCCP Customer is responsible for notifying organization-defined personnel or roles within organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction for the database and application.

1.13 RISK ASSESSMENT (RA)

RA-1 Risk Assessment Policy and Procedures

RA-1 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for having policies for this control family.
Part b	The FCCP Customer is responsible for having procedures for this control family.

RA-3 Risk Assessment

RA-3 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for conducting an assessment of risk for the application and database, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
Part b	The FCCP Customer is responsible for documenting the application and database risk assessment results.
Part c	The FCCP Customer is responsible for reviewing the application and database risk assessment results.
Part d	The FCCP Customer is responsible for documenting the application and database risk assessment results.
Part e	The FCCP Customer is responsible for updating the risk assessment whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

RA-5 Vulnerability Scanning

RA-5 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for scanning for vulnerabilities for the web application and database and when new vulnerabilities potentially affecting the system/applications are identified and reported.

RA-5 (8) Control Enhancement

RA-5 (8) What is the solution and how is it implemented?	
The FCCP Customer will describe in its SSP how it reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited for the database and application.	

1.14 SYSTEM AND SERVICES ACQUISITION (SA)

SA-1 System and Services Acquisition Policy and Procedures

SA-1 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for having policies for this control family.
Part b	The FCCP Customer is responsible for having procedures for this control family.

SA-2 Allocation of Resources

SA-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for including a determination of information security requirements for the application in mission/business process planning.
Part b	The FCCP Customer is responsible for determining, documenting, and allocating the resources required to protect the application and database as part of its capital planning and investment control process.
Part c	The FCCP Customer is responsible for establishing a discrete line item for information security in organizational programming and budgeting documentation.

SA-3 System Development Life Cycle

SA-3 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for managing the application and database using a system development life cycle methodology that Includes information security considerations.
Part b	The FCCP Customer is responsible for defining and documenting application and database security roles and responsibilities throughout the system development life cycle.
Part c	The FCCP Customer is responsible for identifying individuals having information system security roles and responsibilities.
Part d	The FCCP Customer is responsible for integrating the organization information security risk management process into System Develop Life Cycle activities for the database and application.

SA-4 Acquisitions Process

SA-4 (8) Control Enhancement

SA-4 (8) What is the solution and how is it implemented?
The FCCP Customer will describe in its SSP how it requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness for the database and application.

SA-4 (9) Control Enhancement

SA-4 (9) What is the solution and how is it implemented?

The FCCP Customer is responsible for identifying early in the system development lifecycle, the functions, ports, protocols, and services for the database and application.

SA-4 (10) Control Enhancement

SA-4 (10) What is the solution and how is it implemented?

The FCCP Customer is responsible for employing only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

SA-5 Information System Documentation

SA-5 What is the solution and how is it implemented?

Part a	The FCCP Customer is responsible for obtaining, protecting as required, and making available to authorized personnel, administrator documentation for the application and database that describes: Secure configuration, installation, and operation of the information system; Effective use and maintenance of security features/functions; and Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
Part b	The FCCP Customer is responsible for obtaining, protecting as required, and making available to authorized personnel, user documentation for the application and database that describes: User-accessible security features/functions and how to effectively use those security features/functions; Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and User responsibilities in maintaining the security of the information and information system; and Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.
Part c	The FCCP Customer is responsible for documenting in its SSP how it documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response
Part d	The FCCP Customer is responsible for documenting in its SSP how it protects documentation as required, in accordance with the risk management strategy.
Part e	The FCCP Customer is responsible for documenting in its SSP how it distributes documentation to organization-defined personnel or roles

SA-8 Security Engineering Principles

SA-8 What is the solution and how is it implemented?	
The FCCP Customer is responsible for applying application and database security engineering principles in the specification, design, development, implementation, and modification of the information system.	

SA-9 External Information System Services

SA-9 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for requiring that external information system services comply with FCCP security requirement and employs security controls in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards and guidance.
Part b	The FCCP Customer is responsible for defining and documenting government oversight and user roles and responsibilities with regard to external information system services.
Part c	The FCCP Customer is responsible for monitoring security control compliance by external service providers.

SA-9 (1) Control Enhancement

SA-9 (1) What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for conducting an organizational assessment of risk on the application and database prior to the acquisition or outsourcing of dedicated information security services.
Part b	The FCCP Customer is responsible for ensuring that the acquisition or outsourcing of dedicated information security services for the application and database is approved.

SA-9 (2) Control Enhancement

SA-9 (2) What is the solution and how is it implemented?	
The FCCP Customer will explain in its SSP how it identifies the functions, ports, protocols, and other services required for the use of such services for all external systems where Federal information is processed or stored.	

SA-9 (4) Control Enhancement

SA-9 (4) What is the solution and how is it implemented?	
The FCCP Customer will describe in its SSP how it employs safeguards to ensure that the interests of all external systems where Federal information is processed or stored are consistent with and reflect organizational interests in the database and application.	

SA-10 Developer Configuration Management

SA-10 What is the solution and how is it implemented?	
Part a	The FCCP Customer will describe in its SSP how it performs application and database configuration management during design, development, implementation, and operation.
Part b	The FCCP Customer will describe in its SSP how it manages and controls changes to the application and database.
Part c	The FCCP Customer will describe in its SSP how it implements only organization-approved changes.
Part d	The FCCP Customer will describe in its SSP how it documents approved changes to the application and database.
Part e	The FCCP Customer will describe in its SSP how it tracks security flaws and flaw resolution for the application and database.

SA-10 (1) Control Enhancement

SA-10 (1) What is the solution and how is it implemented?	
	The FCCP Customer must explain in its SSP how it requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

SA-11 Developer Security Testing and Evaluation

SA-11 What is the solution and how is it implemented?	
Part a	The FCCP Customer will describe in its SSP how it creates and implements a security test and evaluation plan for the application and database.
Part b	The FCCP Customer will describe in its SSP how it implements a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process.
Part c	The FCCP Customer describes in its SSP how it documents the results of the security testing/evaluation and flaw remediation processes for the application and database.
Part d	The FCCP Customer describes in its SSP how it implements a verifiable flaw remediation process for the application and database.
Part e	The FCCP Customer describes in its SSP how it corrects flaws identified during testing/evaluation for the application and database.

SA-11 (1) Control Enhancement

SA-11 (1) What is the solution and how is it implemented?	
	The FCCP Customer will describe in its SSP how it submits a code analysis report as part of the authorization package, updates the report in any reauthorization actions, and documents in the Continuous Monitoring Plan, how newly-developed code for the information system is reviewed.

SA-11 (2) Control Enhancement

1

SA-11 (2) What is the solution and how is it implemented?	
	The FCCP Customer is responsible for performing threat and vulnerability analyses and subsequent testing/evaluation of the database and application.

SA-11 (8) Control Enhancement

2

SA-11 (8) What is the solution and how is it implemented?	
	The FCCP Customer will describe in its SSP how it requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis in the database and application.

1.15 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

SC-1 System and Communications Protection Policy and Procedures

SC-1 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for having policies for this control family.
Part b	The FCCP Customer is responsible for having procedures for this control family.

SC-2 Application Partitioning

1

SC-2 What is the solution and how is it implemented?	
	The FCCP Customer must describe user functionality associated with their application. FCCP Customer must separate user functionality (including user interface services) from information system management functionality and describe in the FCCP Customer SSP how this is achieved for the application and database.

SC-5 Denial of Service Protection

2

SC-5 What is the solution and how is it implemented?	
	The FCCP Customer is responsible for protecting the application and database against or limits the effects of different types of denial of service attacks by implementing secure coding best practices such as input validation and bounds checking to prevent application and database DoS attacks such as buffer overflows. For additional guidance, the FCCP Customer can reference the following: https://www.owasp.org/index.php/Application_Denial_of_Service The list of denial of service attacks is accepted and approved by JAB.

SC-6 Resource Availability

SC-6 What is the solution and how is it implemented?

The FCCP Customer is responsible for limiting the use of resources by priority for the application and database.

SC-17 Public Key Infrastructure Certificates

SC-17 What is the solution and how is it implemented?

The DGS FCCP customer is responsible for obtaining public key certificates from an approved third-party certificate authority.

SC-18 Mobile Code

SC-18 What is the solution and how is it implemented?

Part a	The FCCP Customer is responsible for defining acceptable and unacceptable mobile code and mobile code technologies for the application and database.
Part b	The FCCP Customer is responsible for establishing usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.
Part c	The FCCP Customer is responsible for authorizing, monitoring, and controlling the use of mobile code within the application and database.

SC-20 Secure Name / Address Resolution Service (Authoritative Source)

SC-20 What is the solution and how is it implemented?

Part a	The FCCP Customer will describe in its SSP how it provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.
---------------	--

SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)

SC-21 What is the solution and how is it implemented?

The FCCP Customer will describe in its SSP how it performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

SC-22 Architecture and Provisioning for Name / Address Resolution Service

SC-22 What is the solution and how is it implemented?

The FCCP Customer will describe in its SSP how the information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

SC-23 Session Authenticity

SC-23 What is the solution and how is it implemented?

3 The FCCP Customer must document and implement authenticity to provide protection against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. This requirement should focus on communications protection for the application session rather than for the network packet and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Depending on the required degree of confidentiality and integrity, web services/SOA should require the use of SSL/TLS Version 1.2 mutual authentication (two-way/bidirectional).

1.16 SYSTEM AND INFORMATION INTEGRITY (SI)

SI-1 System and Information Integrity Policy and Procedures

SI-1 What is the solution and how is it implemented?

Part a	The FCCP Customer is responsible for having policies for this control family.
Part b	The FCCP Customer is responsible for having procedures for this control family.

SI-2 Flaw Remediation

SI-2 What is the solution and how is it implemented?

1

Part a	The FCCP Customer is responsible for identifying, reporting, and correcting application and database flaws.
Part b	The FCCP Customer is responsible for testing software updates related to flaw remediation for effectiveness and potential side effects on the application and database before installation.
Part c	The FCCP Customer is responsible for installing security-relevant software and firmware for the application and database within 30 days of the release of the update. <i>were slower; not enough capacity</i>
Part d	The FCCP Customer is responsible for incorporating flaw remediation into the organizational configuration management process for the application and database.

SI-2 (3) Control Enhancement

SI-2 (3) What is the solution and how is it implemented?

1

Part a	The FCCP Customer will describe in its SSP how it measures the time between flaw identification and flaw remediation for the database and application.
Part b	The FCCP Customer will describe in its SSP how it establishes benchmarks for taking corrective actions in the database and application.

SI-3 Malicious Code Protection

SI-3 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for automatically configuring the scan for removable media to check for malicious code, and not allow access to perform any executable functions on it until the malicious code on the removable media has been quarantined or removed.

SI-3 (7) Control Enhancement

SI-3 (7) What is the solution and how is it implemented?	
The FCCP Customer will describe in its SSP how it implements nonsignature-based malicious code detection mechanisms into the information system for the database and application.	

SI-4 Information System Monitoring

SI-4 (2) Control Enhancement

SI-4 (2) What is the solution and how is it implemented?	
The FCCP Customer is responsible for employing automated tools to support near real-time analysis of events for the application and database.	

SI-4 (5) Control Enhancement

SI-4 (5) What is the solution and how is it implemented?	
The FCCP Customer is responsible for providing near real-time alerts when indications of compromise or potential compromise occurs in accordance with the incident response plan.	

SI-6 Security Functionality Verification

SI-6 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for verifying correct security operations for the application and database.
Part b	The FCCP Customer is responsible for performing this verification for the application and database.

SI-7 Software & Information Integrity

SI-7 What is the solution and how is it implemented?	
The FCCP Customer is responsible for detecting unauthorized changes to software and information for the application and database.	

SI-7 (1) Control Enhancement

SI-7 (1) What is the solution and how is it implemented?

The FCCP Customer is responsible for reassessing the integrity of software and information by performing integrity scans of the application and database.

SI-7 (7) Control Enhancement

SI-7 (7) What is the solution and how is it implemented?

The FCCP Customer is responsible for describing in its SSP how it incorporates the detection of unauthorized changes to any database or application component into its incident response capability.

SI-10 Information Input Validation

SI-10 What is the solution and how is it implemented?

The FCCP Customer is responsible for checking the validity of information inputs for the application and database. DGS is responsible for the OS and infrastructure. Input accuracy mechanisms are hard-coded into the OS; therefore, these are addressed by Microsoft, Cisco, Linux, etc.

SI-11 Error Handling

SI-11 What is the solution and how is it implemented?

Part a The FCCP Customer is responsible for generating error messages for the application and database that provide information necessary for corrective actions without revealing in error logs and administrative messages that could be exploited by adversaries. The FCCP Customer implementation must also include how the system prevents revelation of content related to sensitive financial data or internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes and settings).

Part b The FCCP Customer is responsible for revealing error messages only to authorized personnel for the application and database.

Review of current messages

SI-12 Information Output Handling and Retention

SI-12 What is the solution and how is it implemented?

The FCCP Customer is responsible for handling and retaining both information within and output from the application and database in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

SI-16 Memory Protection

SI-16 What is the solution and how is it implemented?

The FCCP Customer will describe in its SSP how the information system implements safeguards to protect its memory from unauthorized code execution for the database and application.