

FedRAMP Users Guide



FedRAMP

Datapipe Government Solutions
Federal Community Cloud Platform

Version 6.0

August 18, 2016

Controlled Unclassified Information

System Security Plan

Prepared by

Identification of Organization that Prepared this Document		
	Organization Name	Datapipe Government Solutions
	Street Address	1902 Campus Commons Drive
	Suite/Room/Building	Suite 510
	City, State Zip	Reston, VA 20191

Prepared for

Identification of Cloud Service Provider		
	Organization Name	Datapipe Government Solutions
	Street Address	1902 Campus Commons Drive
	Suite/Room/Building	Suite 510
	City, State Zip	Reston, VA 20191

Revision History

Date	Description	Version of SSP	Author
2/6/2015	Initial Document	1.0	DGS FCCP
2/26/2015	Updates to reflect SSP changes	2.0	DGS FCCP
5/5/2015	Updates to reflect SSP changes	3.0	DGS FCCP
8/18/2016	Update to reflect SSP v6.0	6.0	DGS FCCP

Table of Contents

1	CONTROLS.....	8
1.1	Access Control (AC).....	8
	AC-1 Access Control Policy and Procedures.....	8
	AC-2 Account Management.....	9
	AC-2 (1) Control Enhancement.....	10
	AC-2 (2) Control Enhancement.....	10
	AC-2 (3) Control Enhancement.....	10
	AC-2 (4) Control Enhancement.....	10
	AC-2 (5) Control Enhancement.....	10
	AC-2 (7) Control Enhancement.....	10
	AC-2 (9) Control Enhancement.....	11
	AC-2 (10) Control Enhancement.....	11
	AC-2 (12) Control Enhancement.....	11
	AC-5 Separation of Duties.....	11
	AC-6 Least Privilege.....	11
	AC-6 (1) Control Enhancement.....	11
	AC-6 (2) Control Enhancement.....	12
	AC 6 (5) Control Enhancement.....	12
	AC-6 (9) Control Enhancement.....	12
	AC-6 (10) Control Enhancement.....	12
	AC-7 Unsuccessful Login Attempts.....	13
	AC-8 System Use Notification.....	13
	AC-10 Concurrent Session Control.....	13
	AC-11 Session Lock.....	14
	AC-12 Session Termination.....	14
	AC-14 Permitted Actions without Identification or Authentication.....	14
	AC-17 Remote Access.....	14
	AC-19 Access Control for Portable and Mobile Systems.....	15
	AC-19 (5) Control Enhancement.....	15
	AC-20 Use of External Information Systems.....	15
	AC-20 (1) Control Enhancement.....	16
	AC-21 Information Sharing.....	16
	AC-22 Publicly Accessible Content.....	16
1.2	Awareness and Training (AT).....	17
	AT-1 Security Awareness and Training Policy and Procedures.....	17
	AT-2 Security Awareness.....	17
	AT-2 (2) Control Enhancement.....	17
	AT-3 Role-Based Security Training.....	17
	AT-4 Security Training Records.....	18
1.3	Audit and Accountability (AU).....	18
	AU-1 Audit and Accountability Policy and Procedures.....	18
	AU-2 Audit Events.....	18
	AU-2 (3) Control Enhancement.....	18
	AU-3 Content of Audit Records.....	19
	AU-3 (1) Control Enhancement.....	19
	AU-5 Response to Audit Processing Failures.....	19

AU-6 Audit Review, Analysis, and Reporting.....	19
AU-6 (1) Control Enhancement.....	19
AU-6 (3) Control Enhancement.....	20
AU-8 Time Stamps.....	20
AU-8 (1) Control Enhancement.....	20
AU-9 Protection of Audit Information.....	20
AU-9 (2) Control Enhancement.....	20
AU-11 Audit Record Retention.....	20
AU-12 Audit Generation.....	21
1.4 Security Assessment and Authorization (CA).....	21
CA-1 Certification, Authorization, Security Assessment Policy and Procedures.....	21
CA-2 Security Assessments.....	21
CA-2 (3) Control Enhancement.....	21
CA-3 System Interconnections.....	22
CA-3 (5) Control Enhancement.....	22
CA-5 Plan of Action and Milestones.....	22
CA-6 Security Authorization.....	22
CA-7 Continuous Monitoring.....	23
CA-7 (1) Control Enhancement.....	23
CA-8 Penetration Testing.....	24
CA-8 (1) Control Enhancement.....	24
1.5 Configuration Management (CM).....	24
CM-1 Configuration Management Policies and Procedures.....	24
CM-2 Baseline Configuration.....	24
CM-2 (1) Control Enhancement.....	25
CM-2 (2) Control Enhancement.....	25
CM-2 (3) Control Enhancement.....	25
CM-2 (7) Control Enhancement.....	25
CM-3 Configuration Change Control.....	26
CM-4 Security Impact Analysis.....	26
CM-5 Access Restrictions for Change.....	26
CM-5 (1) Control Enhancement.....	26
CM-5 (3) Control Enhancement.....	26
CM-6 Configuration Settings.....	27
CM-6 (1) Control Enhancement.....	27
CM-7 Least Functionality.....	27
CM-7 (2) Control Enhancement.....	27
CM-7 (5) Control Enhancement.....	28
CM-9 Configuration Management Plan.....	28
CM-10 Software Usage Restrictions.....	28
CM-10 (1) Control Enhancement.....	29
CM-11 User-Installed Software.....	29
1.6 Contingency Planning (CP).....	29
CP-1 Contingency Planning Policy and Procedures.....	29
CP-2 Contingency Plan.....	30
CP-2 (1) Control Enhancement.....	30
CP-2 (2) Control Enhancement.....	30
CP-2 (3) Control Enhancement.....	30
CP-2 (8) Control Enhancement.....	31
CP-3 Contingency Training.....	31
CP-4 Contingency Plan Testing.....	31
CP-4 (1) Control Enhancement.....	31
CP-9 Information System Backup.....	31

CP-10 Information System Recovery and Reconstitution	32
CP-10 (2) Control Enhancement	32
1.7 Identification and Authentication (IA)	32
IA-1 Identification and Authentication Policy and Procedures	32
IA-2 User Identification and Authentication	32
IA-2 (1) Control Enhancement	32
IA-2 (2) Control Enhancement	32
IA-2 (5) Control Enhancement	33
IA-2 (8) Control Enhancement	33
IA-2 (12) Control Enhancement	33
IA-4 Identifier Management	33
IA-4 (4) Control Enhancement	33
IA-5 Authenticator Management	34
IA-5 (1) Control Enhancement	34
IA-5 (2) Control Enhancement	35
IA-5 (4) Control Enhancement	35
IA-5 (6) Control Enhancement	35
IA-5 (7) Control Enhancement	35
IA-5 (11) Control Enhancement	35
IA-6 Authenticator Feedback	36
IA-8 Identification and Authentication (Non-Organizational Users)	36
IA-8 (1) Control Enhancement	36
IA-8 (2) Control Enhancement	36
IA-8 (4) Control Enhancement	36
1.8 Incident Response (IR)	36
IR-1 Incident Response Policy and Procedures	36
IR-2 Incident Response Training	36
IR-3 Incident Response Testing	37
IR-3 (2) Control Enhancement	37
IR-4 Incident Handling	37
IR-4 (1) Control Enhancement	37
IR-5 Incident Monitoring	37
IR-6 Incident Reporting	38
IR-6 (1) Control Enhancement	38
IR-7 Incident Response Assistance	38
IR-7 (1) Control Enhancement	38
IR-7 (2) Control Enhancement	38
IR-8 Incident Response Plan	39
IR-9 Information Spillage Response	40
IR-9 (1) Control Enhancement	40
IR-9 (2) Control Enhancement	40
IR-9 (3) Control Enhancement	40
IR-9 (4) Control Enhancement	40
1.9 Maintenance (MA)	41
MA-1 System Maintenance Policy and Procedures	41
MA-2 Controlled Maintenance	41
MA-3 Maintenance Tools	41
MA-4 Remote Maintenance	42
MA-4 (2) Control Enhancement	42
MA-5 Maintenance Personnel	42
MA-5 (1) Control Enhancement	43
1.10 Media Protection (MP)	43
MP-2 Media Access	43
MP-4 Media Storage	43

MP-5 Media Transport	43
MP-6 Media Sanitization and Disposal	43
MP-6 (2) Control Enhancement	44
1.11 Planning (PL)	44
PL-1 Security Planning Policy and Procedures	44
PL-2 System Security Plan	44
PL-2 (3) Control Enhancement	45
PL-4 Rules of Behavior	45
PL-4 (1) Control Enhancement	45
PL-8 Information Security Architecture	45
1.12 Personnel Security (PS)	46
PS-1 Personnel Security Policy and Procedures	46
PS-2 Position Categorization	46
PS-3 Personnel Screening	46
PS-3 (3) Control Enhancement	46
PS-4 Personnel Termination	47
PS-5 Personnel Transfer	47
PS-6 Access Agreements	47
PS-7 Third-Party Personnel Security	48
PS-8 Personnel Sanctions	48
1.13 Risk Assessment (RA)	49
RA-1 Risk Assessment Policy and Procedures	49
RA-3 Risk Assessment	49
RA-5 Vulnerability Scanning	49
RA-5 (8) Control Enhancement	49
1.14 System and Services Acquisition (SA)	50
SA-1 System and Services Acquisition Policy and Procedures	50
SA-2 Allocation of Resources	50
SA-3 System Development Life Cycle	50
SA-4 Acquisitions Process	50
SA-4 (8) Control Enhancement	50
SA-4 (9) Control Enhancement	51
SA-4 (10) Control Enhancement	51
SA-5 Information System Documentation	51
SA-8 Security Engineering Principles	52
SA-9 External Information System Services	52
SA-9 (1) Control Enhancement	52
SA-9 (2) Control Enhancement	52
SA-9 (4) Control Enhancement	52
SA-10 Developer Configuration Management	53
SA-10 (1) Control Enhancement	53
SA-11 Developer Security Testing and Evaluation	53
SA-11 (1) Control Enhancement	53
SA-11 (2) Control Enhancement	54
SA-11 (8) Control Enhancement	54
1.15 System and Communications Protection (SC)	54
SC-1 System and Communications Protection Policy and Procedures	54
SC-2 Application Partitioning	54
SC-5 Denial of Service Protection	54
SC-6 Resource Availability	55

SC-17 Public Key Infrastructure Certificates	55
SC-18 Mobile Code.....	55
SC-20 Secure Name / Address Resolution Service (Authoritative Source)	55
SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)	55
SC-22 Architecture and Provisioning for Name / Address Resolution Service.....	55
SC-23 Session Authenticity	56
1.16 System and Information Integrity (SI).....	56
SI-1 System and Information Integrity Policy and Procedures.....	56
SI-2 Flaw Remediation	56
SI-2 (3) Control Enhancement	56
SI-3 Malicious Code Protection.....	57
SI-3 (7) Control Enhancement	57
SI-4 Information System Monitoring.....	57
SI-4 (2) Control Enhancement	57
SI-4 (5) Control Enhancement	57
SI-6 Security Functionality Verification	57
SI-7 Software & Information Integrity.....	57
SI-7 (1) Control Enhancement	58
SI-7 (7) Control Enhancement	58
SI-10 Information Input Validation.....	58
SI-11 Error Handling	58
SI-12 Information Output Handling and Retention.....	58
SI-16 Memory Protection.....	58

Controls

This document was designed for those FCCP Customers who partner with Datapipe Government Solutions (DGS) Federal Community Cloud Platform (FCCP). DGS is responsible for the system infrastructure and partners with a provider who is responsible for the application and database. Each entity has a responsibility to document how NIST-mandated controls are implemented. In certain instances, there are only controls that apply to DGS, or the FCCP Customer, or both. Below is a list of shared controls. The FCCP Customer is expected to document its implementation in a manner such that each can be tested during Step 4 of the NIST SP 800-37, Revision 1 Risk Management Framework (RMF) process. Please refer to the FedRAMP web site: www.fedramp.gov for more information and templates.

1.1 ACCESS CONTROL (AC)

AC-1 Access Control Policy and Procedures

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

AC-2 Account Management

AC-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for identifying account types for their own users. System design only allows FCCP Customer access to the following: • Application access • Database access The FCCP Customer must identify account types for its users in the FCCP Customer's SSP.
Part b	The FCCP Customer is responsible for defining in its SSP how account managers are assigned for the database and application.
Part c	The FCCP Customer is responsible for establishing its own group membership protocols for the application and database. How conditions are established for group membership for the FCCP Customer's customer will be addressed in the FCCP Customer's SSP.
Part d	The FCCP Customer is responsible for identifying authorized users of the IS and specifying access privileges for the application and database. How the FCCP Customer identifies authorized users of the information system and specifies access privileges is described in the FCCP Customer's SSP.
Part e	The FCCP Customer is required to obtain appropriate approvals for requests to establish accounts for the application and database environment. The process for obtaining appropriate approvals for requests to establish accounts is described in the FCCP Customer's SSP
Part f	The FCCP Customer is responsible for notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes for application and database accounts. The process of establishing, activating, modifying, disabling, and removing accounts is described in the FCCP Customer's SSP.
Part g	The FCCP Customer is responsible for issuing a temporary, guest, or anonymous account at their discretion for the application and database. How the FCCP Customer specifically authorizes and monitors the use of guest/anonymous and temporary accounts is described in its SSP
Part h	The FCCP Customer Program Manager is responsible for contacting the DGS FCCP Program Manager if an FCCP Customer employee is terminated, transferred, or information system usage or need-to-know/need-to-share changes. How the FCCP Customer notifies account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes is described in FCCP Customer's SSP and included in their FedRAMP submission.
Part i	The FCCP Customer is responsible for granting access to the application and database based on a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions.
Part j	The FCCP Customer is responsible for reviewing accounts for the application and database.
Part k	The FCCP Customer is responsible for establishing a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group for the application and database.

AC-2 (1) Control Enhancement

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

The FCCP Customer is responsible for automating management of accounts for the application and database.

AC-2 (2) Control Enhancement

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

The FCCP Customer is responsible for automatically terminating temporary and emergency accounts for the application and database users.

AC-2 (3) Control Enhancement

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

The FCCP Customer is responsible for disabling inactive user and nonuser accounts in accordance with their own policies and procedures.

AC-2 (4) Control Enhancement

AC-2 (4) What is the solution and how is it implemented?

The FCCP Customer is responsible for automatically auditing account creation, modification, disabling, and termination actions for the application and database.

AC-2 (5) Control Enhancement

AC-2 (5) What is the solution and how is it implemented?

The FCCP Customer will describe in its SSP how time periods of expected inactivity are defined for the database and application

AC-2 (7) Control Enhancement

AC-2 (7) What is the solution and how is it implemented?

Part a	The FCCP Customer is responsible for establishing and administering privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles for the application and database.
Part b	The FCCP Customer is responsible for tracking and monitoring privileged role assignments for the application and database.
Part c	The FCCP Customer is responsible for disabling accounts associated with privileged role assignments when those assignments are no longer appropriate for the application and database.

AC-2 (9) Control Enhancement

AC-2 (9) What is the solution and how is it implemented?
The FCCP Customer is responsible for describing in its SSP the conditions that permit the use of shared/group accounts for the database and application.

AC-2 (10) Control Enhancement

AC-2 (10) What is the solution and how is it implemented?
The FCCP Customer will describe in its SSP how shared/group account credentials are terminated when members leave the group for the database and application.

AC-2 (12) Control Enhancement

AC-2 (12) What is the solution and how is it implemented?	
Part a	The FCCP Customer will describe in its SSP how it monitors information system accounts for the database and application.
Part b	The FCCP Customer will describe in its SSP how atypical usage of information accounts are reported for the database and application.

AC-5 Separation of Duties

AC-5 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for separating duties of individuals as necessary for the application and database, to prevent malevolent activity without collusion.
Part b	The FCCP Customer is responsible for documenting separation of duties for the application and database users and administrators.
Part c	The FCCP Customer is responsible for implementing separation of duties through assigned information system access authorizations for the application and database.

AC-6 Least Privilege

AC-6 What is the solution and how is it implemented?
The FCCP Customer is responsible for employing the concept of least privilege, allowing only authorized access for users of the application and database (and processes acting on behalf of users), which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

AC-6 (1) Control Enhancement

AC-6 (1) What is the solution and how is it implemented?
The FCCP Customer is responsible for explicitly authorizing access to list of security functions for the application and database.

AC-6 (2) Control Enhancement

1

AC-6 (2) What is the solution and how is it implemented?
The FCCP Customer is responsible for requiring that users of information system accounts, or roles, with access to security functions or security-relevant information for the application and database, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.

AC 6 (5) Control Enhancement

1

AC-6 (5) What is the solution and how is it implemented?
The FCCP Customer is responsible for explaining which roles it restricts privileged accounts for the database and application. A list of user assigned authorizations with user privileges. The DGS FCCP AC Policies and Procedures. Related control to AC-3. A list of personnel. Security system accounts (Centrify, Splunk, FirePOWER, Trend Micro and Nessus) are restricted to people assigned the System Engineer role Server operating system administrative accounts are restricted to people assigned the System Administrator role Network device accounts (firewalls, routers switches, load balancers) are restricted to people assigned the Network Administrator role VMWare administrator accounts are restricted to people assigned the Virtualization Administrator role Active Directory administrator accounts are restricted to people assigned the Domain Administrator role

AC-6 (9) Control Enhancement

2

AC-6 (9) What is the solution and how is it implemented?
The FCCP Customer will describe in its SSP how the database and application audits privileged access.

AC-6 (10) Control Enhancement

1

AC-6 (10) What is the solution and how is it implemented?
The FCCP Customer is responsible for describing in its SSP how it prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

AC-7 Unsuccessful Login Attempts

AC-7 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for enforcing a limit of consecutive invalid login attempts to the application or database by a user within a specific time period.
Part b	The FCCP Customer is responsible for configuring the application and database to automatically lock the account for a specific time period, lock the account until released by an administrator, or delays the next login prompt when the maximum number of unsuccessful attempts into the application or database is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

AC-8 System Use Notification

AC-8 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for displaying an approved system use notification message or banner before granting access to the application or database that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording.
Part b	The FCCP Customer is responsible for retaining the notification message or banner on the screen until users take explicit actions to log on to or further access the information system.
Part c	For applications and databases that are part of a publicly accessible systems, the FCCP Customer is responsible for: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

AC-8 What is the solution and how is it implemented?	
Req. 1	The FCCP Customer is responsible for determining elements of the application and database within cloud environment that require the System Use Notification control.
Req. 2	The FCCP Customer is responsible for ensuring the application and database display the most recent Warning Banner and indicate the percentage of items requiring the banner setting.
Req. 3	The FCCP Customer is responsible for providing results of verification and the necessary periodicity of the application and database baseline configuration review.

AC-10 Concurrent Session Control

AC-10 What is the solution and how is it implemented?	
The FCCP Customer is responsible for limiting the number of concurrent sessions for each application and database account.	

AC-11 Session Lock

AC-11 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for preventing further access to the application and database by initiating a session lock.
Part b	The FCCP Customer is responsible for retaining the session lock until the application or database user reestablishes access using established identification and authentication procedures.

AC-12 Session Termination

AC-12 What is the solution and how is it implemented?	
The FCCP Customer describes in its SSP how the database and application automatically terminates a user session.	

AC-14 Permitted Actions without Identification or Authentication

AC-14 What is the solution and how is it implemented?	
Part a	The FCCP Customer describes in its SSP what user actions, if any, that can be accomplished within the customer environment without identification and authentication.
Part b	The FCCP Customer describes in its SSP what user actions, if any, that can be accomplished within the customer environment without identification and authentication.

AC-17 Remote Access

AC-17 What is the solution and how is it implemented?	
Part a	Since the FCCP CPM Customer Administrator is an authorized privileged role, the FCCP CPM Administrator accesses the management zone using the same process as the DGS FCCP System Administrators, DGS FCCP Domain Administrators, DGS FCCP Network Administrators, DGS FCCP Virtualization Administrators, and DGS FCCP Security Engineers. The FCCP CPM Customer Administrator would need to gain remote access to the FCCP system before granting access to its users to the application and database. The FCCP CPM Customer is responsible for describing how its users gain remote access in its SSP.

AC-19 Access Control for Portable and Mobile Systems

AC-19 What is the solution and how is it implemented?	
1 2 Part a	The FCCP Customer is responsible for documenting in its SSP how it establishes usage restrictions, configuration requirements, connecting requirements, and implementation guidance for FCCP Customer-controlled mobile devices.
Part b	The FCCP Customer does not authorize the direct connection of mobile devices to systems in the FCCP accreditation boundary. It is the email correspondence from customers in the FCCP environment which may be sent and received to and from mobile devices. For this correspondence only mobile devices with encryption enabled via passcode, biometric finger scan, or unique pattern are authorized.

AC-19 (5) Control Enhancement

AC-19 (5) What is the solution and how is it implemented?	
—	The FCCP Customer is responsible for describing in its SSP the type of encryption to protect the confidentiality and integrity of information on organization-defined mobile devices.

AC-20 Use of External Information Systems

AC-20 What is the solution and how is it implemented?	
1 Part a	The FCCP Customer will describe in its SSP how it establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.
Part b	The FCCP Customer will describe in its SSP how it establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store, and/or transmit organization-controlled information using the external information systems.

AC-20 (1) Control Enhancement

AC-20 (1) What is the solution and how is it implemented?	
Part a	If the FCCP Customer requests an interconnection to be made, the DGS Customer will provide security relevant information for DGS consideration via the Change Advisory Board. DGS will assess the proposed change, attain formal approval via internal Change Advisory and FedRAMP prior to implementing the change. If FCCP Customer allows external connections, the FCCP Customer will describe in its SSP how it can verify the implementation of required security controls on the external system as specified in the FCCP Customer's information security policy and security plan.
Part b	If the FCCP Customer requests an interconnection to be made, the DGS Customer will provide security relevant information for DGS consideration via the Change Advisory Board. DGS will assess the proposed change, attain formal approval via internal Change Advisory and FedRAMP prior to implementing the change. If FCCP Customer allows external connections, the FCCP Customer will describe in its SSP how it has approved information system connection or processing agreements with the organizational entity hosting the external information system.

AC-21 Information Sharing

AC-21 What is the solution and how is it implemented?	
Part a	The FCCP Customer will describe in its SSP how it facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments.
Part b	The FCCP Customer will describe in its SSP how it employs rule-based access control (RuBAC), access control matrix, content-dependent access control, and context-dependent access control mechanisms for the database and application.

AC-22 Publicly Accessible Content

AC-22 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for designating individuals associated with the application and database authorized to post information onto an organizational information system that is publicly accessible.
Part b	The FCCP Customer is responsible for training authorized individuals to ensure that publicly accessible information from the application or database does not contain non-public information.
Part c	The FCCP Customer is responsible for reviewing the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system.
Part d	The FCCP Customer is responsible for reviewing the content on the publicly accessible organizational information system for non-public information and removing nonpublic information from the publicly accessible organizational information system, if discovered.

1.2 AWARENESS AND TRAINING (AT)

AT-1 Security Awareness and Training Policy and Procedures

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

AT-2 Security Awareness

AT-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for providing basic security awareness training to all information system users of the application and database (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes.
Part b	The FCCP Customer is responsible for providing basic security awareness training to all information system users of the application and database (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes.
Part c	The FCCP Customer is responsible for providing basic security awareness training to all information system users of the application and database (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes.

AT-2 (2) Control Enhancement

AT-2 (2) What is the solution and how is it implemented?
The FCCP Customer is responsible for explaining in its SSP how it includes security awareness training on recognizing and reporting potential indicators of insider threat.

AT-3 Role-Based Security Training

AT-3 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for providing role-based security-related training for the application and database before authorizing access to the system.
Part b	The FCCP Customer is responsible for providing role-based security-related training for the application and database when required by system changes.
Part c	The FCCP Customer will describe in its SSP how role-based security training to personnel assigned security roles and responsibilities at least annually.

AT-4 Security Training Records

AT-4 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for documenting and monitoring individual information system security training activities for the application and database including basic security awareness training and specific information system security training; and retaining individual training records for at least one year.
Part b	The FCCP Customer is responsible for documenting in its SSP the retention period for FCCP Customer staff training records.

1.3 AUDIT AND ACCOUNTABILITY (AU)

AU-1 Audit and Accountability Policy and Procedures

AU-1 What is the solution and how is it implemented?	
hPart 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.

AU-2 Audit Events

AU-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for auditing the following for web applications and database: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. The capabilities to configure auditing for web applications and database auditable events will vary for each web application and database. DGS FCCP Domain Administrator, DGS FCCP System Administrator, DGS FCCP Network Administrator, and DGS FCCP Security Engineer would not have direct access to these web applications and database auditable events.
Part b	The FCCP Customer is responsible for coordinating the security audit function with the CPM Government System Owner and other organizational entities for the application and database requiring audit related information to enhance mutual support and to help guide the selection of auditable events. For selecting application and database auditable events, the FCCP Customer would not require participation from DGS FCCP.
Part c	The FCCP Customer is responsible for providing a rationale, in its SSP, why the list of auditable events for the application and database are deemed to be adequate to support after-the-fact investigations of security incidents.
Part d	The FCCP Customer is responsible for determining, based on current threat information and ongoing assessment of risk, that the following subset of events from AU-2 are to be audited for the application and database.

AU-2 (3) Control Enhancement

AU-2 (3) What is the solution and how is it implemented?	
The FCCP Customer is responsible for reviewing and updating the list of auditable events for the application and database annually or whenever there is a change in the threat environment.	

AU-3 Content of Audit Records

3

AU-3 What is the solution and how is it implemented?	
The FCCP Customer is responsible for producing audit records for the application and database that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	

AU-3 (1) Control Enhancement

1

AU-3 (1) What is the solution and how is it implemented?	
The FCCP Customer is responsible for notifying the DGS FCCP Security engineer on which application logs should be collected by FCCP log collection tools. FCCP Customer is responsible for documenting detailed information in the audit records for audit events identified by type, location, or subject for the application and database.	

AU-5 Response to Audit Processing Failures

1

1

AU-5 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for alerting designated organizational officials in the event of a database or application audit processing failure.
Part b	The FCCP Customer is responsible for taking additional actions in the event of a database or application audit processing failure. FCCP Customer can make a change request to make required changes to FCCP firewalls per DGS FCCP and FCCP Customer's change control process to enable audit processing failure alerting.

AU-6 Audit Review, Analysis, and Reporting

1

1

AU-6 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for reviewing and analyzes information system audit records for the application and database for indications of inappropriate or unusual activity, and reports findings to designated organizational officials.
Part b	The FCCP Customer is responsible for adjusting the level of audit review, analysis, and reporting within the application and database when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

AU-6 (1) Control Enhancement

1

AU-6 (1) What is the solution and how is it implemented?	
The FCCP Customer is responsible for integrating audit review, analysis, and reporting within the application and database to support organizational processes for investigation and response to suspicious activities.	

AU-6 (3) Control Enhancement

AU-6 (3) What is the solution and how is it implemented?

1 The FCCP Customer is responsible for analyzing and correlating audit records across different repositories within the application and database to gain organization-wide situational awareness. In addition, the FCCP Customer may request application and database logs that are captured by Splunk from the DGS FCCP Security Engineer. The FCCP Customer may choose to receive the logs in the following formats: Raw Events, CSV, XML, or JSON.

AU-8 Time Stamps

AU-8 (1) Control Enhancement

AU-8 (1) What is the solution and how is it implemented?

1 **Part a** The FCCP Customer is responsible for configuring database time settings to synchronize with the operating system or domain controller on at least an hourly basis.

~~**Part b**~~ The FCCP Customer is responsible for configuring database time settings to synchronize with the operating system or domain controller on at least an hourly basis.

AU-8 (1) What is the solution and how is it implemented?

1 **Req. 1** The FCCP Customer is responsible for configuring database time settings to synchronize with the operating system or domain controller which are synched against time.nist.gov (Gaithersburg, MD) and nist1-lnk.binary.net (Lincoln, Nebraska).

~~**Req. 2**~~ The FCCP Customer is responsible for configuring database time settings to synchronize with the operating system or domain controller, which are synched against time.nist.gov (Gaithersburg, MD) and nist1-lnk.binary.net (Lincoln, Nebraska).

AU-9 Protection of Audit Information

AU-9 What is the solution and how is it implemented?

— The FCCP Customer is responsible for protecting audit information and audit tools for the application and database from unauthorized access, modification, and deletion.

AU-9 (2) Control Enhancement

AU-9 (2) What is the solution and how is it implemented?

1 The FCCP Customer is responsible for backing up audit records for the application and database at onto a different system or media than the system being audited.

AU-11 Audit Record Retention

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

— The FCCP Customer is responsible for retaining application and database audit records online to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

AU-12 Audit Generation

AU-12 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for providing audit record generation capability for the application and database for the list of auditable events defined in AU-2.
Part b	The FCCP Customer is responsible for allowing designated organizational personnel to select, which auditable events are to be audited by the application and database.
Part c	The FCCP Customer is responsible for generating audit records for the list of audited events defined in AU-2 with the content as defined in AU-3 for the application and database.

1.4 SECURITY ASSESSMENT AND AUTHORIZATION (CA)

CA-1 Certification, Authorization, Security Assessment Policy and Procedures

CA-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.

CA-2 Security Assessments

CA-2 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for developing a security assessment plan that describes the scope of the assessment for the application and database including: • Security controls and control enhancements under assessment; • Assessment procedures to be used to determine security control effectiveness; and • Assessment environment, assessment team, and assessment roles and responsibilities.
Part b	The FCCP Customer is responsible for assessing the security controls for the application and database to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Part c	The FCCP Customer is responsible for producing a security assessment report that documents the results of the assessment for the application and database.
Part d	The FCCP Customer is responsible for producing a security assessment report that documents the results of the assessment for the application and database.

CA-2 (3) Control Enhancement

CA-2 (3) What is the solution and how is it implemented?
The FCCP Customer will describe in its SSP how assessments for the database and applications meet the conditions of a P-ATO in the FedRAMP Secure Repository.

CA-3 System Interconnections

CA-3 What is the solution and how is it implemented?	
Part c	The FCCP Customer is responsible for explaining in its SSP how it monitors the information system connections on an ongoing basis verifying enforcement of security requirements.

CA-3 (5) Control Enhancement

CA-3 (5) What is the solution and how is it implemented?	
The FCCP Customer will describe in its SSP how they employ policies for allowing database and applications to connect to external systems.	

CA-5 Plan of Action and Milestones

CA-5 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for developing a plan of action and milestones for the application and database to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.
Part b	The FCCP Customer is responsible for updating existing plan of action and milestones for the application and database based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-6 Security Authorization

CA-6 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for assigning a senior-level executive or manager to the role of authorizing official for the application and database.
Part b	The FCCP Customer is responsible for ensuring that the authorizing official authorizes the application and database for processing before commencing operations.
Part c	The FCCP Customer is responsible for updating the application and database's security authorization.

CA-7 Continuous Monitoring

CA-7 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for developing a continuous monitoring strategy and implements a continuous monitoring program that includes establishing metrics to be monitored
Part b	The FCCP Customer is responsible for documenting in its SSP its established frequencies for monitoring and assessments supporting such monitoring.
Part c	The FCCP Customer is responsible for describing in its SSP how it develops a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy.
Part d	The FCCP Customer is responsible for describing in its SSP how it develops a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.
Part e	The FCCP Customer is responsible for describing in its SSP how it develops a continuous monitoring strategy and implements a continuous monitoring program that includes correlation and analysis of security-related information generated by assessments and monitoring.
Part f	The FCCP Customer is responsible for describing in its SSP how it develops a continuous monitoring strategy and implements a continuous monitoring program that includes response actions to address results of the analysis of security-related information.
Part g	The FCCP Customer is responsible for describing in its SSP how it develops a continuous monitoring strategy and implements a continuous monitoring program that includes reporting the security status of organization and the information system to meet federal and FedRAMP requirements monthly

CA-7 What is the solution and how is it implemented?	
Req. 2	The FCCP Customer is responsible for documenting in its SSP monthly database and web application scans.
Req. 3	The FCCP Customer will be expected to hire a 3PAO to perform scans for the databases and applications that run on DGS FCCP.

CA-7 (1) Control Enhancement

CA-7 (1) What is the solution and how is it implemented?	
The FCCP Customer will describe in its SSP for the database and application how it employs assessors or assessment teams with its organization-defined level of independence to monitor the security controls in the information system on an ongoing basis.	

CA-8 Penetration Testing

CA-8 What is the solution and how is it implemented?	
The FCCP Customer describes in its SSP the frequency with which the independent 3PAO performs penetration testing on the database and application.	

CA-8 (1) Control Enhancement

CA-8 (1) What is the solution and how is it implemented?	
The FCCP Customer describes in its SSP the frequency with which the independent 3PAO performs penetration testing on the database and application.	

1.5 CONFIGURATION MANAGEMENT (CM)

CM-1 Configuration Management Policies and Procedures

CM-1 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for explaining in its SSP how it develops, documents, and disseminates to organization-defined personnel or roles: (1) A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls
Part b	The FCCP Customer is responsible for explaining in its SSP how frequently it reviews and updates the current: (1) Configuration management policy at least every 3 years; and (2) Configuration management procedures at least annually.

CM-2 Baseline Configuration

CM-2 What is the solution and how is it implemented?	
The FCCP Customer is responsible for developing, documenting, and maintaining under configuration control, a current baseline configuration of the application and database.	

CM-2 (1) Control Enhancement

CM-2 (1) What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for reviewing and updating the baseline configuration for the application and database.
Part b	The FCCP Customer is responsible for reviewing and updating the baseline configuration for the application and database when required by the JAB.
Part c	The FCCP Customer is responsible for reviewing and updating the baseline configuration for the application and database as an integral part of information system component installations and upgrades.

CM-2 (2) Control Enhancement

CM-2 (2) What is the solution and how is it implemented?	
The FCCP Customer describes in its SSP how it employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the database and application.	

CM-2 (3) Control Enhancement

CM-2 (3) What is the solution and how is it implemented?	
The FCCP Customer is responsible for retaining older versions of the baseline configurations for the application and database to support rollback.	

CM-2 (7) Control Enhancement

CM-2 (7) What is the solution and how is it implemented?	
Part a	The FCCP Customer will work with the CPM Government System Owner to address this control.
Part b	The FCCP Customer will work with the CPM Government System Owner to address this control.

CM-3 Configuration Change Control

CM-3 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for determining the types of changes to the application and database that are configuration controlled.
Part b	The FCCP Customer is responsible for approving configuration-controlled changes to the application and database with explicit consideration for security impact analyses
Part c	The FCCP Customer is responsible for documenting approved configuration-controlled changes to the application and database.
Part d	The FCCP Customer is responsible for describing in its SSP how it implements approved configuration-controlled changes to the information system for the database and application.
Part e	The FCCP Customer is responsible for retaining and reviewing records of configuration-controlled changes to the application and database.
Part f	The FCCP Customer is responsible for auditing activities associated with configuration-controlled changes to the system.
Part g	The FCCP Customer is responsible for coordinating and providing oversight for configuration change control activities for the application and database.

CM-4 Security Impact Analysis

CM-4 What is the solution and how is it implemented?
The FCCP Customer is responsible for analyzing changes to the information system to determine potential security impacts prior to change implementation.

CM-5 Access Restrictions for Change

CM-5 What is the solution and how is it implemented?
The FCCP Customer is responsible for defining, documenting, approving, and enforcing physical and logical access restrictions associated with changes to the application and database.

CM-5 (1) Control Enhancement

CM-5 (1) What is the solution and how is it implemented?
The FCCP Customer is responsible for defining, documenting, approving, and enforcing physical and logical access restrictions associated with changes to the application and database.

CM-5 (3) Control Enhancement

CM-5 (3) What is the solution and how is it implemented?
The FCCP Customer will describe in its SSP how it prevents the installation of unauthorized software and firmware components for the database and application without verification that the component has been digitally signed using a certificate that is recognized and approved.

CM-6 Configuration Settings

CM-6 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for establishing and documenting mandatory configuration settings for the application and database that reflect the most restrictive mode consistent with the sensitivity level.
Part b	The FCCP Customer is responsible for implementing the configuration settings for the application and database.
Part c	The FCCP Customer is responsible for identifying, documenting, and approving exceptions from the mandatory configuration settings for individual components within the application and database based on explicit operational requirements.
Part d	The FCCP Customer is responsible for monitoring and controlling changes to the configuration settings for the application and database in accordance with organizational policies and procedures.

CM-6 (1) Control Enhancement

CM-6 (1) What is the solution and how is it implemented?	
The FCCP Customer is responsible for employing automated mechanisms to centrally manage, apply, and verify configuration settings for the application and database.	

CM-7 Least Functionality

CM-7 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for configuring the database and application to provide only essential capabilities.
Part b	The FCCP Customer is responsible for documenting in their SSP how the database and application prohibits or restricts the use of the following functions, ports, protocols, and/or services.

CM-7 (2) Control Enhancement

CM-7 (2) What is the solution and how is it implemented?	
The FCCP Customer works with DGS FCCP Program Manager and DGS FCCP Network Administrator to have any authorized software application added to the whitelist on the firewall. In addition, the FCCP Customer is responsible for providing organization-defined policies regarding software program usage and restrictions as well as rules authorizing the terms and conditions of software program usage.	

CM-7 (5) Control Enhancement

CM-7 (5) What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for explaining in its SSP how it identifies software programs related to the database and application that are authorized to execute on the information system
Part b	The FCCP Customer is responsible for explaining in its SSP how it employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs related to the database and application on the information system
Part c	The FCCP Customer is responsible for explaining in its SSP how it reviews and updates the list of authorized software programs related to the database and application at least annually or when there is a change.

CM-9 Configuration Management Plan

CM-9 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for addressing roles, responsibilities, and configuration management processes and procedures for the application and database.
Part b	The FCCP Customer is responsible for establishing the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
Part c	The FCCP Customer is responsible for defining the configuration items for the application and database and when in the system development life cycle the configuration items are placed under configuration management.
Part d	The FCCP Customer is responsible for defining in its SSP how its configuration management plan is protected from unauthorized disclosure and modification.

CM-10 Software Usage Restrictions

CM-10 What is the solution and how is it implemented?	
Part a	The FCCP Customer will describe in its SSP how it uses software and associated documentation in accordance with contract agreements and copyright laws for the database and application.
Part b	The FCCP Customer will describe in its SSP how it tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution for the database and application.
Part c	The FCCP Customer will describe in its SSP how they control and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work for the database and application.

CM-10 (1) Control Enhancement

1

CM-10 (1) What is the solution and how is it implemented?	
	The FCCP Customer will describe in its SSP how it establishes the restrictions on the use of open source database and application software.

CM-11 User-Installed Software

1 {
-
-
-

CM-11 What is the solution and how is it implemented?	
Part a	The FCCP Customer is responsible for describing in its SSP how it establishes policies for the database and application that govern the installation of software by users.
Part b	The FCCP Customer is responsible for describing in its SSP the methods it uses to enforce software installation policies for the database and application.
Part c	The FCCP Customer is responsible for describing in its SSP how it monitors policy compliance for the database and application continuously.

1.6 CONTINGENCY PLANNING (CP)

CP-1 Contingency Planning Policy and Procedures

2

CP-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.