Tennessee Consolidated Retirement System (TCRS)

Cybersecurity Requirements

February 06, 2024
Version 0.1

Table of Contents

Introduction

Purpose

The following tables list TCRS's cybersecurity requirements for the Pension Administration System.

Requirements have been broken into three Flexibility Types based upon degree of flexibility TCRS has:

1) Mandatory,
2) Desired, and
3) Optional.

Respondents must confirm that they meet all mandatory technical requirements defined in this document. This confirmation is to be provided in the Respondents' response to Item A.14 of RFP Attachment 6.2 – Section A— Mandatory Requirement Items. These requirements align to NIST 800.53 best practices. If the proposed PAS solution does not meet a particular technical requirement defined as Desired, the Respondent must provide details explaining what aspects of the functionality are not supported, along with any alternate solutions that can be employed to achieve the required results. These details are to be provided in the Respondent's response to the question posed in Item C.7 of RFP Attachment 6.2 – Section C (Technical Qualifications, Experience & Approach Items).

Flexibility Types

The following table describes TCRS's definitions of these priorities and the specific implementation rules.

- The Respondent must include in their fixed price bid all requirements denoted with a Flexibility Rating of 1 or 2.
- The Respondent must provide line item optional pricing for each requirement denoted with a Flexibility Rating of 3.

Flexibility Rating	Flexibility Type	Comments
1	**Mandatory**	TCRS must have this requirement. Respondents failure to meet these requirements will cause their proposal to be considered non-responsive and rejected.
2	**Desired**	TCRS highly desires this requirement. Respondent will be evaluated on their ability to satisfy these requirements.
3	**Optional**	TCRS considers this requirement to be a "nice to have." Respondent will be evaluated on their ability to satisfy these requirements.

The tables in the following sections reference different flexibility levels.

Each technical requirement category is identified by a number and name. There is nothing to be implied from the category identification numbers and/or the technical requirement ID numbers other than simple identification. The individual requirements listed are numbered as an extension to the category number. Please do not alter the technical requirement ID numbers.

Instructions to Vendors

For all requirements, indicate the Degree of Customization Required in the applicable field:

A. **Configuration**. Existing system functionality will be configured to deliver the requirement. This includes setting of parameter values, updates to factor and value tables, updating rules engines, and selection from any available configuration options within the existing software release. Configuration changes would not be expected to have any impact on future software updates.

B. **Minor Customization**. To meet the requirement, existing functionality will be modified to incorporate unique TCRS customizations not within the existing software release. This includes customization within well-defined exit/entry points within the system, interface file format definitions, custom formulas, custom SQL or SQR code for queries or reports, and addition / modification of data fields. Minor Customizations would not be expected to have an impact on future software updates.

C. **Major Customization**. Existing functionality to meet the requirement does not currently exist within an existing module, feature, or system component. This includes TCRS-specific extensions / enhancements / customizations to existing functionality, TCRS-specific APIs, protocols, or standards, and back-porting features from another version of the system. These are customizations that would not normally be reviewed or tested by the Contractor as part of their general System release testing and validation. Special care would be required to ensure compatibility with future software updates.

D. **Other** (describe in comments). Existing functionality to meet the requirement does not currently exist and would require either a new functionality be added to the System, e.g., a new module, feature, or system component, the use of third-party technology specifically to meet TCRS' requirement, or the requirement will be met outside of the System either manually or with a standalone tool.

Vendors Response to Requirements

C-01 Access Control

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
01.01	Policy and Procedures	The Proposed Vendor shall follow access control policies aligned to TCRS' security program requiring approvals for user and privileged accounts.	1	N
01.02	Account Management	The proposed solution shall establish and manage user accounts, relying upon operating system or other software controls to ensure Role Based Access Control (RBAC) is implemented appropriately.	1	N
01.03	Account Management	The proposed solution shall ensure all individual accounts are managed. Types of individual accounts may include but are not limited to: • User • Auditor • Super-User (Elevate End User Privilege) • System Administrator	1	N
01.04	Account Management	System and service level accounts must be managed.	1	N
01.05	Account Management	The proposed solution shall ensure that group, or shared, accounts are not permitted under any condition.	1	N
01.06	Account Management	All vendor personnel changes shall result in an immediate notification to TCRS to ensure the realignment of privileges within 24 hours.	1	N
01.07	Information Flow Enforcement	Systems that have interconnections with the Proposed Solution hosted environment shall have agreements for that interconnectivity, including security controls that specify the maintenance of the privacy of the information exchanged. TCRS System owners shall approve all interconnected systems.	1	Y

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
01.08	Separation of Duties	Oversight and management shall be performed over system administrators to ensure that those involved in making any privileged changes to the Proposed Solution are reviewed and monitored.	1	N
01.09	Separation of Duties	Designed system roles shall ensure a functional and/or administrative separation of duties to mitigate risks associated with user accounts being able to perform functions of significant criticality or sensitivity that should be controlled by more than one individual.	1	N
01.10	Least Privilege	The Proposed Solution shall predefine roles for server administrator logins that provide only the access required to perform required maintenance functions.	1	N
01.11	Least Privilege	Assigned user privileges are defined with the least amount of rights / privileges that will enable the user to perform the tasks they are required to perform.	1	N
01.12	Least Privilege	Remote Desktop Services is reserved solely for system administration purposes and only available to authorized system administrative accounts.	1	Y
01.13	Unsuccessful Login Attempts	The Proposed Solution shall ensure that configurations include a configurable setting for password attempts and temporary account locking based on TCRS policy.	2	N
01.14	Unsuccessful Login Attempts	After a configurable number of attempts (i.e., 5 attempts) within thirty (30) minutes, user account locking occurs until unlocked by a TCRS administrator.	2	N
01.15	Session Lock	The Proposed Solution shall permit a maximum of fifteen (15) minutes idle time before logout / disconnect – this time shall be configurable to allow for changes to TCRS' security posture.	2	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
01.16	Session Lock	The proposed solution shall allow for TCRS to establish a session lock capability through configuration settings. If a session is locked, the user must reauthenticate to reestablish processing.	2	N
01.17	Session Lock	The Proposed Solution shall allow for external applications (e.g., the Employer Portal) to have an alternative session lock time setting which must also be configurable.	2	N
01.18	Session Termination	The Proposed Solution shall require all servers to terminate the session based on a configurable time defined by TCRS. The user is prompted to (re)authenticate to continue system use prior to session termination.	2	N
01.19	Permitted Actions Without Identification or Authentication	No actions shall be performed without following the identification and authentication requirements contained herein.	2	N
01.20	Simultaneous logins	The proposed solution shall not allow more than 2 simultaneous logins.		N

C-02 Awareness and Training

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
02.01	Security Awareness and Training Policy and Procedures	The Proposed Vendor shall perform formal annual security awareness and training in support of the TCRS environment, making updates to the materials based upon the latest best practices. The proposed training shall include, at a minimum: • Handling of Personally Identifiable Information (PII) • Health Information Portability and Accountability Act (HIPAA) and Protected Health Information (PHI) • Social Engineering for Security Awareness • Phishing / Vishing Awareness Training, and • General Security Training (To include the requirements contained herein)	1	Y

C-03 Audit and Accountability

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
03.01	Audit and Accountability Policy and Procedures	If the proposed solution is hosted, the Proposed Vendor shall describe their audit and accountability approach to log management.	1	Y
03.02	Audit Events	The Proposed Solution shall ensure all capturable events are subject to inclusion in audit logs to support near-real-time and after-the-fact reviews of system activity.	1	N

03.03	Audit Events	The minimum set of events that is required to be audited includes system (both application and on the server infrastructure) events, process tracking and all privileged user actions, including: • Successful and unsuccessful account logon events – Capturing all logon events support the nonrepudiation aspects of determining which user performed what action on which server. Unusual activity may indicate specific user accounts under attack. • Account management events – Can include such activities as enabling / disabling accounts, changing group memberships, or enabling / disabling access privileges. • Object access – Can include all changes to the proposed system's objects. Additionally, excessive attempts to access certain objects may indicate configuration issues or inappropriate / unauthorized access attempts. • Policy Change – Changes in account policy can have varied effects, such as a reduction in visibility over system activities or opening directories to unmonitored alteration. Some changes will take effect only with the next system restart, causing a gap between the time at which the change is created and the time at which it takes effect. • Privilege functions – Includes such activities as broadening user permissions, changing the catalog of users permitted to access, modifying, or deleting files within a directory or group of directories. • Process tracking – Monitoring processes allow for the capture of unauthorized activity not necessarily tied to a specific user.	1	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
		• System events – System-level events can indicate corrupted or failed operations that may signify a threat to system integrity and weaken the ability to restore a system to a known state.		
03.04	Content of Audit Records	The Proposed Solution shall support configuration of network device and server operating system settings to support creating audit records that meeting basic forensics. This may include but is not limited to: • What event occurred, • When it occurred, • The location where it occurred (at minimum, a source IP address), • Who initiated the event (unless a system-initiated event which will be indicated), and • Whether the event succeeded or failed.	1	N
03.05	Content of Audit Records	The logs shall be stored in a secured, non-modifiable storage area with the capability of sharing TCRS specified logs with an external log management service.	1	N
03.06	Response to Audit Processing Failures	The Proposed Solution shall be capable of triggering an alert if log recording fails to operate normally.	1	N
03.07	Audit Review, Analysis, and Reporting	The Proposed Vendor shall perform periodic review and analysis of audit records for indications of inappropriate or unusual activity and report any findings of said activity immediately to TCRS for review.	1	Y
03.08	Audit Review, Analysis, and Reporting	The Proposed Solution shall demonstrate the use of automated tool(s) for aggregation reduction and report generation to analyze and report activity in a form necessary to support investigation and response to suspicious activities.	1	Y

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
03.09	Time Stamps	The Proposed Solution shall synchronize timestamps using internal system clocks to corroborate entries across diverse servers using the NIST Network Time Protocol (NTP) to generate time stamps for audit records that are stored internally in UTC-compatible format.	1	N
03.10	Protection of Audit Information	The Proposed Vendor shall restrict access to audit logs and audit tools only to authorized personnel including TCRS Administrators when applicable.	1	N
03.11	Audit Record Retention	The Proposed Solution shall address audit log record retention and at the minimum include one (1) year of retention and/or align with TCRS data retention policies.	1	N
03.12	Audit Record Retention	TCRS' record retention requirements shall be configurable to ensure flexibility in meeting legislative requirements.	1	N

C-04 System Authorization and Security Assessment

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N
04.01	Security Assessments	The Proposed Vendor shall perform formal security assessments upon all hosted information systems and provide SOC2 and bridge letter results to TCRS for review.	1	Y
04.02	System Interconnections	The Proposed Vendor shall ensure the performance of independent security assessments upon all hosted systems.	1	Y
04.03	System Interconnections	The Proposed Solution shall document the interconnections to other information systems and ensure connections are defaulted to a “deny all, allow-by-exception” security posture. Allowed exceptions must be approved by TCRS where applicable.	1	N
04.04	Plan of Action and Milestones	The Proposed Vendor shall develop a Plan of Action and Milestones (POAM) post-assessment to address how critical, high, and medium priority risks are to be resolved for the hosted solution.	2	Y
04.05	Security Authorization	A senior official of TCRS will be designated as the Authorizing Official (AO). The AO shall provide authorization prior to system operation.	2	N
04.06	Continuous Monitoring	The Proposed Solution shall ensure continuous monitoring of the hosted environment.	2	Y

C-05 Configuration Management

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
05.01	Configuration Management Policies and Procedures	The Proposed Vendor shall denote that it has a formal security configuration management process that aligns to ITIL Best Practices and it addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance applied to all organizational entities with access to the Proposed Solution.	1	N
05.02	Baseline Configuration	Proposed Vendor shall develop, document, and maintain baseline configuration documentation aligned to a standard (i.e., CIS) to support the system implementation and ensure it conforms to the baseline.	1	Y
05.03	Configuration Change Control	The Proposed Vendor's Information Security Policy and associated Procedures shall ensure changes to the Proposed Solution environment would be approved by authorized TCRS personnel. All public facing systems must have a risk assessment performed to obtain TCRS approval.	1	N
05.04	Configuration Change Control	Changes shall not be promulgated to the Proposed Solution unless approved by TCRS as part of the configuration management program.	1	N
05.05	Access Restrictions for Change	The Proposed Vendor's Information Security Policy and associated Procedures shall ensure that only authorized system administrators can make approved changes to the Proposed Solution systems, either on-site or remotely via VPN.	1	N
05.06	Configuration Settings	The Proposed Vendor's Information Security Policy and associated Procedures shall ensure CIS or industry best practice guidelines are followed to harden the operating system and network components to the most restrictive settings consistent with Moderate Risk while permitting system operation.	1	Y

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
05.07	Least Functionality	The Proposed Vendor's Information Security Policy and associated Procedures shall ensure that all ports, protocols and/or services are prohibited by default.	1	Y
05.08	Least Functionality	The Proposed Vendor shall provide all functions, ports, protocols and/or services required to be allowed-by-exception for system operability for approval by TCRS.	1	Y
05.09	Least Functionality	Under all conditions the following, at a minimum, must be restricted: • Telnet • FTP • SSH version 1 • Terminal Services • Port 1433 for SQL Server • Adobe Flash • SMB v1	1	N

C-06 Contingency Planning

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
06.01	Contingency Planning Policy and Planning	The Proposed Vendor shall ensure backup and recovery procedures address Proposed Solution formal contingency plan processes.	1	N
06.02	Contingency Planning Policy and Planning	The formal documented contingency plan policy and procedures addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance applied to all organizational entities with access to the Proposed Solution.	1	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
06.03	Contingency Plan	The disaster recovery plan should, at minimum, accomplish the following: 1. Identifies essential missions and business functions with associated contingency requirements to continue delivering TCRS retirement plan participant information. 2. Defines Recovery Time Objective (RTO) and Recovery Point Objective (RPO) objectives, priorities, and metrics for the Proposed Solution as identified herein. 3. Defines roles, specific responsibilities and assigned individuals supporting the successful implementation of the Contingency Plan including contact methods and communication protocols. 4. Discusses the methods for maintaining essential business missions and functions during system disruption, compromise or failure including the method to determine whether to maintain operations-in-place or transfer operations to an alternate datacenter. 5. Includes ultimate restoration to normal operations within the original security framework and internal recertification procedures. 6. Provides for annual review, update, approval and testing to ensure effectiveness.	1	N
06.04	Contingency Plan Testing	An annual test of the Contingency Plan shall be conducted to ensure that the plan, assigned personnel and resources are prepared and capable to perform required tasks to continue or restore services and system functionality.	2	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
06.05	Contingency Plan Testing	The plan shall test leveraging controlled failover events in conjunction with TCRS approval and participation.	2	N
06.06	Alternate Storage Site (Hosted Solution Only)	The disaster recovery procedures shall have automated backup processes that replicate content to an alternate processing site for use in restoring the system.	1	Y
06.07	Alternate Storage Site (Hosted Solution Only)	In addition to provisioning copies of operating systems and application software refreshed after every update, daily and weekly backup processes ensure minimal data loss in the event the contingency plan must be invoked.	1	Y
06.08	Alternate Storage Site (Hosted Solution Only)	The Proposed Solution's disaster recovery procedures shall ensure backups are replicated through the Primary Datacenter's backbone to the recovery site	1	Y
06.09	Alternate Storage Site (Hosted Solution Only)	The disaster recovery procedures shall ensure the Alternate Datacenter location is situated to minimize the risk of a regional disruption or disaster scenario that affects both the Primary and Recovery Datacenters.	1	Y
06.10	Alternate Storage Site (Hosted Solution Only)	The disaster recovery procedures shall maintain an alternate recovery site with equivalent configurations including all security, safety and infrastructure established at the primary datacenter.	1	Y
06.11	Alternate Storage Site (Hosted Solution Only)	TCRS has identified the Proposed Solution as a Critical Application and requires an RTO of 4 hours and RPO of 15 minutes or less.	1	Y

C-07 Identification and Authentication

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
07.01	User Identification and Authentication	The Proposed Vendor's security policy and associated Procedures shall address formal identification and authentication processes for the Proposed Solution. All local accounts require authentication using the same password complexity as network accounts.	1	N
07.02	User Identification and Authentication	The technique for identification and authentication includes user IDs and passwords, tokens for VPN, or any combination of methods that the system can trust to always work effectively.	1	N
07.03	User Identification and Authentication	The solution shall have the capability to leverage identity verification services such as Lexis-Nexis identity verification protocols.	1	N
07.04	User Identification and Authentication	The solution shall have the capability to enforce multi-factor authentication for access within the trusted TCRS Local Area Network and shall require multi-factor authentication for remote access, VPN, and external portals.	1	N
07.05	User Identification and Authentication	Each privileged user is required to have, at minimum, a unique user ID and password to access any system.	1	N
07.06	User Identification and Authentication	The Proposed Vendor shall implement replay-resistant techniques on the Proposed Solution's hosted environment.	1	Y
07.07	User Identification and Authentication	Privileged users would have to log in with their regular (non-privileged) user account to establish VPN connection and then log in separately with their privileged user account credentials to perform administrative functions.	1	N
07.08	Identifier Management	Application Users are uniquely identified by user ID. Disabled accounts are retained for a minimum of two years before re-use is permitted.	1	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
07.09	Identifier Management	User identifiers are automatically disabled after a configurable number of days of inactivity.	1	N

07.10	Authenticator Management	Authenticators must have sufficient strength by satisfying the following configurable criteria based on TCRS policy:
		• Password must not match the prior twelve (12) passwords or three (3) years
		• Password must be a minimum length of twelve (12) characters; eight characters if MFA is enabled
		• Password cannot contain all or a substantial part of the user ID or display name
		• Password must contain a combination of characters from all the following categories:
		  ○ Upper case characters (A-Z)
		  ○ Lower case characters (a-z)
		  ○ Base 10 digits (0-9)
		  ○ Non-alphanumeric characters (e.g., !&$%)
			1	N

07.11	Authenticator Management	Passwords have a minimum life and a maximum life (for example, one (1) day minimum and sixty (60) days max). Both options (min/max) shall be configurable.	1	N
07.12	Authenticator Management	Infrastructure, to the extent supported by manufacturers, must also comply with the complexity requirement.	1	N
07.13	Authenticator Management	Passwords must be encrypted both in storage and during transmission. Non-public transmissions across public networks are always encrypted using FIPS 140-2 compliant encryption methods in encrypted files or via VPN. Network devices, Windows Server and Red Hat operating systems are configured to automatically encrypt passwords within reserved storage areas unavailable for general use.	1	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
07.14	Authenticator Management	Temporary, single-use passwords are assigned when establishing new accounts or resetting the password on existing accounts. The temporary password is provided to the user via private means and should be sufficiently randomized.	1	N
07.15	Authenticator Feedback	The Proposed Solution shall ensure user account information is protected within the operating system through encryption and obfuscation on display.	2	N
07.16	Authenticator Feedback	When typing in user-defined or one-time passwords, the screen display should provide sufficient masking (in the form of asterisks or bullets) to avoid the password being read by an individual watching the user's screen.	2	N
07.17	Identification and Authentication (Non-Organization User)	The Proposed Solution shall ensure all users are issued individual approved identification and authentication credentials based on TCRS Policy.	1	N

C-08 Incident Response

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
08.01	Incident Response Policy and Procedures	The Proposed Vendor's formal documented incident response plan shall address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance applied to all organizational entities with access to the Proposed Solution.	1	Y
08.02	Incident Training Response	The Proposed Vendor shall ensure all vendor and third-party support personnel receive security incident response training specific to their incident response role as part of their employee orientation and on an annual basis thereafter.	2	Y
08.03	Incident Training Response	The specific training content will be refreshed every year to reflect the current threat environment.	2	Y
08.04	Incident Training Response	Post-occurrence, technical personnel are trained in appropriate sanitization methods.	2	Y
08.05	Incident Response Testing	The Proposed Vendor shall test its incident response capability annually and provide TCRS an after-action summary.	2	Y
08.06	Incident Response Testing	Incident response testing incorporates the following steps: • Develop test plan for incident response • Perform test • Analyze test results and obtain lessons learned • Incorporate lessons learned into incident response procedures and training • Distribute updated incident response documentation	2	Y
08.07	Incident Handling	Upon notification of an incident, an investigation is initiated to verify and confirm the incident.	1	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
08.08	Incident Handling	Once confirmed, notice is provided for further corrective action and the measures defined in the Incident Response policy and procedures are followed.	1	N
08.09	Incident Handling	TCRS Senior management should have sufficient visibility and span of control to ensure coordination between incident response personnel and contingency personnel, and can authorize contingency processes, such as transferring operations to an alternate facility.	1	N
08.10	Incident Monitoring	The Proposed Vendor shall ensure system administrators, network administrators, managers, and TCRS users are required to report incidents according to the TCRS Incident Management Policy.	1	Y
08.11	Incident Reporting	All incident reports are treated as sensitive with limited distribution from the time of initial reporting until final resolution, at which time the results are managed appropriately to the sensitivity of the incident.	1	N
08.12	Incident Response Plan	The Proposed Vendor shall develop a formal documented Incident Response Plan to ensure that all incidents are properly: • Recognized, • Identified, • Addressed, and • Resolved according to prepared methods and procedures.	1	Y

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
08.13	Incident Response Plan	The incident management plan shall: • Describe the structure and organization of the incident response capability including primary and secondary responders, • Provide a high-level approach and graphics for how incident response capability fits into the overall organization, • Address TCRS' unique requirements for supporting owned systems, • Define reportable incidents, • Provide metrics for measuring incident response capability, • Define the resources in terms of roles and staffing necessary to effectively maintain and mature an incident response capability, • Be reviewed and approved by TCRS management, • Define level of criticality based on Incident, and • Define Recovery Time Objectives and Recovery Resources	1	Y

C-09 Maintenance

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
09.01	System Maintenance Policy and Procedures	The Proposed Vendor shall document a maintenance policy including procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance applied to all organizational entities with access to the Proposed Solution.	1	N
09.02	Maintenance Tools	The Proposed Solution shall ensure all automated maintenance tools are properly controlled and monitored.	3	N
09.03	Maintenance Tools	The Proposed Solution shall ensure all media or software used to perform diagnostic and test programs are first examined by automated tools for malicious code before introducing the media or software to the Proposed Solution environment.	3	N
09.04	Remote Maintenance	The Proposed Solution shall ensure TCRS Administrator or designee shall authorize or pre-authorize Proposed Vendor maintenance on hardware and systems. Proposed Vendor monitors, logs and maintains maximum possible monitoring and control during maintenance and diagnostic activities.	2	N
09.05	Remote Maintenance	Access records for diagnostic and maintenance access should be retained, audited, and reviewed following established procedures applied to all remote maintenance access. These activities should be recorded within an automated system.	2	N
09.06	Maintenance Personnel	The Proposed Vendor shall limit access to system software and hardware maintenance only to authorized maintenance personnel.	2	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
09.07	Maintenance Personnel	Proposed Vendor maintenance personnel should be required to have appropriate access authorizations to the systems being supported.	2	N
09.08	Maintenance Personnel	Maintenance personnel external to Proposed Vendor must be pre-approved, continuously supervised by competent Proposed Vendor technical personnel, and have their access limited to only that time during which maintenance will be actively performed.	2	Y
09.09	Timely Maintenance	The Proposed Vendor shall ensure production maintenance windows are aligned to TCRS Policy. (defined in the Pro-Forma Contract).	2	Y
09.10	Timely Maintenance	The proposed solution shall ensure redundant hardware for egress failover during maintenance and/or system issues.	2	Y

C-10 Media Protection

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
10.01	Media Marking	The Proposed Vendor shall mark all removable media that contains fund data if removed from the designated controlled areas.	1	Y
10.02	Media Storage	The proposed vendor shall store media in accordance with FIPS 199 controls for a moderately rated system.	1	Y
10.03	Media Storage	Controls shall be maintained for the information system until the media is destroyed or sanitized using approved equipment, techniques, and procedures.	1	Y
10.04	Media Storage	Physical access to areas containing media must be controlled and restricted to specific parties who have been approved by TCRS.	1	Y
10.05	Media Sanitization	The Proposed Vendor shall ensure that all repurposed or retired media that contains fund information is sanitized in accordance with NIST Special Publication 800-88: Guidelines for Media Sanitization.	1	Y
10.06	Media Sanitization	The Proposed Vendor shall provide the ability to verify to TCRS that the sanitization process was successful.	1	Y
10.07	Media Use	The Proposed Vendor shall ensure that portable storage devices, such as flash drives, cannot be used to store fund information.	1	Y
10.08	Media Use	Proper data loss monitoring mechanisms shall be in effect to protect against this activity.	1	Y
10.09	Media Use	The Proposed Vendor shall ensure that portable storage devices are prohibited in accordance with the Media Use requirement contained herein.	1	Y

C-11 Physical and Environmental Protections

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
11.01	Physical and Environmental Protection Policy and Procedures	The Proposed Vendor shall inherit the Datacenter's physical and environmental protections, services, procedures, and Service Level Agreements (SLAs).	1	Y
11.02	Physical and Environmental Protection Policy and Procedures	The proposed primary and alternate datacenters shall be located within the United States. Additionally, both sites shall be required to meet all requirements contained herein. The primary and alternate datacenter locations shall be a minimum of 100 miles apart and on separate power grids.	1	Y
11.03	Physical Access Authorizations	The Proposed Vendor shall ensure the Datacenter provides secured computing facilities for production cloud infrastructure.	1	Y
11.04	Physical Access Controls	The Proposed Datacenter's Information Security Policy and associated Procedures shall ensure that formal physical security safeguards are in place for datacenter premises, which may include: • Premises monitored by CCTV • Entrances protected by physical barriers designed to prevent unauthorized entry by vehicles • Entrances manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management	1	Y
11.05	Access Controls for Transmission Medium	The Proposed Datacenter shall ensure network cables are protected by conduits and, where possible, avoid routes through public areas.	1	Y
11.06	Monitoring Physical Access	The Proposed Datacenter shall ensure electronic locking systems automatically log all access.	1	Y

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
11.07	Monitoring Physical Access	Visitors are required to present government or employer-issued ID and to sign a visitor log to provide a record of their appearance at the facility.	1	Y
11.08	Visitor Access Records	The Proposed Datacenter shall ensure all visitors log into the visitor's log and be authenticated by government- or employer-issued ID before they are recorded in the visitor log. Logs should be retained for at minimum one (1) year.	3	Y
11.09	Power Equipment and Cabling	The Proposed Datacenter shall ensure controlled access to areas of the facility that contain power equipment or cabling.	1	Y
11.10	Emergency Shutoff	The Proposed Datacenter shall ensure proper configuration and maintenance of emergency shutoff switches.	1	Y
11.11	Emergency Power	The Proposed Primary Datacenter shall ensure uninterruptible power that can sustain the Primary Datacenter for the duration of the recovery time required to establish operations at the Recovery Datacenter.	1	Y
11.12	Emergency Lighting	The Proposed Datacenter's Information Security Policy and associated Procedures shall address formal processes for maintaining emergency lighting.	1	Y
11.13	Fire Protection	The Proposed Datacenter's Information Security Policy and associated Procedures shall address formal processes for ensuring the availability of appropriate fire protection and detection systems.	1	Y
11.14	Temperature and Humidity Controls	The Proposed Datacenter's Information Security Policy and associated Procedures shall address the formal process for maintaining and monitoring temperature and humidity with alarms as applicable.	1	Y
11.15	Water Damage	The Proposed Datacenter's Information Security Policy and associated Procedures shall address formal processes and procedures to monitor, control and shut-off water to the facility and/or impacted areas.	1	Y

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
11.16	Delivery and Removal	The Proposed Datacenter shall ensure any physical movement of equipment is controlled by hand-delivered receipts and/or other authorized change control procedures.	1	Y
11.17	Alternate Work Site	The Proposed Recovery Datacenter Location has identical or equivalent protections consistent with controls established at the Primary work location / Datacenter.	2	Y
11.18	Alternate Work Site	All controls described in this document apply equally to both the Primary and Alternate Datacenters.	2	Y

C-12 Planning

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
12.01	Security Planning and Policy Procedures	The Proposed Vendor shall formally document the Proposed Solution System Security Plan and address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance applied to all organizational entities with access to the Proposed Solution.	1	N
12.02	Security Planning and Policy Procedures	The Proposed Vendor shall review and confirm implementation of security policies contained herein.	1	N
12.03	Security Planning and Policy Procedures	TCRS personnel will review and update annually and when significant changes are implemented.	1	N
12.04	Rules of Behavior	The Proposed Vendor shall ensure only those employees assigned responsibilities supporting the Proposed Solution or having a need to use the Proposed Solution are permitted access to the Proposed Solution.	1	N
12.05	Rules of Behavior	The Proposed Vendor shall ensure all employees with access to information system resources conform to what TCRS considers appropriate use of agency resources and includes language regarding the use of social media / networking sites.	1	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
12.06	Information Security Architecture	The Proposed Vendor shall align with this Proposed Solution System Security Plan document that reflects the overall philosophy, requirements, and approach to be taken about protecting the confidentiality, integrity, and availability of organizational information; describes how the information security architecture is integrated into and supports the enterprise architecture; and describes any information security assumptions about, and dependencies on, external services.	1	N
12.07	Security Planning	The Proposed Vendor shall provide a strategic plan identifying high-level plans for adjusting cybersecurity posture as new threats evolve.	2	N

C-13 Personnel Security

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
13.01	Personnel Security Policy and Procedures	The Proposed Vendor shall demonstrate a personnel security policy that Proposed Vendor third-party support personnel must abide by.	1	N
13.02	Personnel Screening	The Proposed Vendor shall demonstrate a personnel security policy that all Proposed Vendor employees and third-party personnel must abide by and requires background checks.	1	N
13.03	Personnel Screening	Proposed Vendor's HR should ensure that all new employees have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.	1	N
13.04	Personnel Termination	The Proposed Vendor shall ensure all access granted to employees who leave the Proposed Vendor are revoked the same day as their employment is terminated.	1	N
13.05	Personnel Termination	The Proposed Vendor must ensure that access to sensitive TCRS information and information systems is transferred to an authorized individual upon termination of an employee.	1	N
13.06	Personnel Termination	The Proposed Vendor is responsible for notifying TCRS when an employee supporting the Proposed Solution is terminated.	1	N
13.07	Personnel Transfer	The Proposed Vendor shall demonstrate a personnel security policy that address formal personnel security processes.	2	N
13.08	Personnel Transfer	Any employee transfer must trigger a review of access privileges to ensure that employee privileges are appropriately tailored to the new position with no excess privileges afforded.	2	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
13.09	Personnel Transfer	The Proposed Vendor is expected to follow the below procedure to effect and document all personnel transfers and reassignments at the time of transfer: • Any Proposed Solution account access not appropriate to the employee's new duties and job description are revoked • The Proposed Vendor initiates the review of access privileges to the Proposed Solution environment as soon as practical, but in all cases completes the review within five days	2	N
13.10	Third-Party Personnel Security	The Proposed Vendor shall demonstrate a personnel security policy that address formal personnel security processes.	1	N
13.11	Third-Party Personnel Security	Personnel security requirements are required to be documented in hiring documents for employees and in the contract documents for contract labor.	1	N
13.12	Third-Party Personnel Security	Proposed Vendor contractors that support the TCRS Proposed Solution environments are required, at a minimum, to successfully undergo a criminal background check with no adverse indications.	1	N
13.13	Third-Party Personnel Security	The Proposed Vendor is responsible for ensuring that all contracting and other supporting documents reinforce the requirements for all contractors to conform to the same security requirements as employees.	1	N

C-14 Risk Assessment

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
14.01	Vulnerability Scanning	All Proposed Solution network devices and servers should be scanned using an industry standard scanning tool to identify vulnerabilities.	1	Y
14.02	Vulnerability Scanning	Scans should use the latest available threat definitions as provided by the scanning tool vendor immediately prior to scanning.	1	Y
14.03	Vulnerability Scanning	The assessor should analyze the vulnerability scan reports and the results from security control assessments to ensure that the appropriate security posture is constantly maintained throughout the environment and check for false positive indications.	1	Y
14.04	Vulnerability Scanning	The assessor should prepare a standard report which provides a high-level vulnerability summary and then itemizes all identified vulnerabilities defining its reference and risk category, vulnerability title, server(s) affected, scheduled resolution date, status, and comments. This report will be provided to TCRS monthly.	1	Y
14.05	Vulnerability Scanning	The Vendor must resolve outstanding legitimate vulnerabilities within the following timeframes: • Zero day – 24 hours • Critical – 15 days • High – 30 days • Medium – 45 days • Low – 60 days	1	N

C-15 System Services and Acquisition

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
15.01	System Development Lifecycle	The Proposed Vendor shall ensure that any software and/or systems acquired in support of the Proposed Solution contain security considerations as part of the evaluation and selection criteria.	1	Y
15.02	Acquisition Process	The Proposed Vendor shall ensure that third-party contracts leveraged to provide solutions, software, and/or systems to support the Proposed solution contain security requirements and/or security specifications based on an assessment of risk.	1	N
15.03	Acquisition Process	The Proposed Vendor shall maintain documentation on internal and/or third-party design and implementation of security controls.	1	N
15.04	Acquisition Process	The Proposed Vendor shall ensure that solutions, software, and/or systems leveraged to support the Proposed Solution adhere to the prohibitions for functions, ports, protocols, and services contained herein.	1	N
15.05	External Information System Services	The Proposed Vendor will notify TCRS of any security vulnerabilities found within a third-party solution, software, and/or system.	1	N

C-16 System and Communications Protections

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
16.01	Application Partitioning	The Proposed Vendor shall allocate separate roles to support personnel and system users thereby enforcing a full separation between user interfaces and information system management functionality.	1	N
16.02	Information in Shared Resources	The Proposed Solution shall be logically separated from other datacenter hosted assets thereby preventing data leakage or spillage.	1	Y
16.03	Denial of Service Protection	Network perimeter devices shall be implemented in the Proposed Solution to provide protection from Denial-of-Service attacks.	1	Y
16.04	Boundary Protection	The Proposed Solution boundary devices shall control and monitor communications at the external boundary interface.	1	Y
16.05	Boundary Protection	These boundary control devices should be configured for and applicable to all processing sites, including alternate sites used for the system.	1	Y
16.06	Boundary Protection	The Proposed Vendor shall establish a gateway firewall that limits external traffic to the TCRS Proposed Solution environment.	1	Y
16.07	Boundary Protection	Each interface should have an established traffic flow control policy specific to that interface. No exceptions should be permitted to the traffic flow policy.	1	Y
16.08	Boundary Protection	The Proposed Solution perimeter firewalls shall be configured to deny all by default and allow network traffic only by explicit rule sets.	1	Y

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
16.09	Transmission Confidentiality and Integrity	The Proposed Solution shall ensure all sensitive related content transmitted outside of the TCRS Proposed Solution environment should be encrypted using FIPS 140-2 validated cryptography to ensure both the confidentiality and the integrity of transmitted content.	1	N
16.10	Transmission Confidentiality and Integrity	The Proposed Solution environment shall use FIPS 140-2 validated cryptography in sensitive information transmissions across public connections to ensure transmission integrity and identify changes in transmitted data; a failure in decryption would indicate a compromised transmission, either through an error occurring across the transmission links or some other form of interference with the transmission.	1	N
16.11	Cryptographic Key Establishment and Management	The Proposed Vendor shall obtain all PKI certificates from an approved service provider (certificate authority) using FIPS 140-2 validated encryption (e.g., Verisign, Entrust). Data specific to treasury may require keys to be generated by TCRS.	1	Y
16.12	Cryptographic Key Establishment and Management	The generation service should be reputable and be able to produce signed certificates that can be used for establishing and managing public and private keys as needed for secured communications of sensitive content.	1	Y
16.13	Use of Cryptography	The Proposed Vendor shall use encryption techniques using the most recent version of FIPS 140-2 and 140-3 (include in-transit, at-rest, and file level encryption), patch management, and log management.	1	N

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
16.14	Protection of Information at Rest	The Proposed Vendor shall implement the TCRS Proposed Solution environment with an encrypted database to protect data at rest. Including file level encryption and the ability to encrypt sensitive data.	1	N
16.15	Protection of Information at Rest	Proposed Vendor should use algorithms that are recommended in FIPS140-2 (e.g., SHA-256).	1	N

C-17 Systems and Information Integrity

ReqID	Sub-Category	Requirement Details	Flexibility Rating	Public Cloud Hosted Only (Y/N)
17.01	Flaw Remediation	The Proposed Vendor shall develop procedures to identify system flaws through system monitoring, security assessments and incident response.	1	Y
17.02	Flaw Remediation	As patches and updates become available, they are to be applied first to the test environment and subsequently, after all operational issues are resolved, to the production environment.	1	N
17.03	Malicious Code Protection	The Proposed Vendor shall develop an Information Security Policy and associated Procedures that address formal system and information integrity processes in the Proposed Solution.	1	N
17.04	Malicious Code Protection	The Proposed Vendor shall employ anti-virus / anti-malware software at endpoints on all servers.	1	Y
17.05	Information System Monitoring	The Proposed Vendor shall implement and configure monitoring tools to detect system behaviors indicative of possible system malfunction.	1	Y
17.06	Security Alerts and Advisories	The Proposed Vendor's security personnel shall receive and review service alerts, advisories, and directives from multiple sources. This includes U.S CERT and SANS Institute security bulletins.	1	N
17.07	Security Alerts and Advisories	The Proposed Vendor should provide notification, as appropriate, to technical personnel to determine appropriate response and initiate all activities necessary to protect the Proposed Solution environment and infrastructure.	1	N
17.08	Error Handling	Messages displayed to non-privileged users are constructed to prevent the release of content that adversaries could exploit.	2	N