CMS Security & Privacy Requirements

This section provides an overview of general CMS Security policies and outlines requirements applicable to all CMS contractors and subcontractors. The CMS Information Security and Privacy Program website provides additional details of CMS security policies and procedures across CMS, and is referenced throughout this document.

The Contractor must adhere to all CMS and Federal IT Security and Privacy standards, policies, statutes, and reporting requirements, as well as all National Institute of Standards and Technology (NIST) standards and guidelines, and other Government-wide laws and regulations for the protection and security of Government Information.

The Contractor must also adhere to the guidance and requirements provided within the CMS Information Systems Security and Privacy Policy (IS2P2). The IS2P2 consolidates existing information security and privacy policy documents into a single volume and directly integrates the enforcement of information security and privacy through the CMS CIO, Chief Information Security Officer, and Senior Official for Privacy.

The CMS/HHS Security and Privacy requirements are based on the policies within the *"CMS Security and Privacy Language for Information and Information Technology Procurements"*. The areas listed below were selected by CMS based on the specific security and privacy requirements identified for this project. *Additional information security and privacy considerations may be identified for individual task orders, depending on the contract structure.*

✓ ***2. Information Security and/or Physical Access Security***

✓ ***3. Privacy Act Records***

☐ ***4. Government Information Processed on GOCO or COCO Systems***

☐ ***5. Cloud Services***

☐ ***6. Other IT Procurements***

a. ☐ Hardware
b. ☐ Software
c. ☐ IT Application Design, Development and Support
d. ☐ Physical Access to Government Controlled Facilities

Information Security and/or Physical Access Security

1. Baseline Security Requirements

    a. **Applicability.** The requirements herein apply whether the entire contract or modification (hereafter "contract"), or portion thereof, includes either or both of the following:

i. **Access (Physical or Logical) to Government Information:** A Contractor (and/or any subcontractor) will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.

ii. **Operate a Federal System Containing Information:** A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the HHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

b. **Safeguarding Information and Information Systems.** All government information and information systems must be protected in accordance with HHS/ CMS policies and level of risk. At a minimum, the Contractor (and/or any subcontractor) must:

i. Protect the:

- **Confidentiality**, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
- **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
- **Availability**, which means ensuring timely and reliable access to and use of information.

ii. Categorize all information owned and/or collected/managed on behalf of HHS/*CMS* and information systems that store, process, and/or transmit HHS information in accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. Based on information provided by the ISSO, CISO, CMS SOP, or other representative, the impact level for each Security Objective (Confidentiality, Integrity, and Availability) and the Overall Impact Level, which is the highest watermark of the three factors of the information or information system are the following:

- **Confidentiality:** ☐Low ✓Moderate ☐High
- **Integrity:** ☐Low ✓Moderate ☐High
- **Availability:** ☐Low ✓Moderate ☐High
- **Overall Impact Level:** ☐Low ✓Moderate ☐High

iii. Based on the agreed-upon level of impact, implement the necessary safeguards to protect all information systems and information collected and/or managed on behalf of HHS/CMS regardless of location or purpose.

iv. Report any discovered or unanticipated threats or hazards by either the agency or contractor, or if existing safeguards have ceased to function immediately after discovery, **within one (1) hour or less**, to the government representative(s).

v. Adopt and implement all applicable policies, procedures, controls, and standards required by the HHS/CMS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain all applicable security and privacy policies by contacting the CO/COR or HHS/CMS security and/or privacy officials.

c. **Privacy Act.** Comply with the Privacy Act requirements (when applicable), and tailor FAR and HHSAR clauses as needed.

d. **Privacy Compliance.** Comply with the E-Government Act of 2002, NIST SP 800-53, and applicable HHS/CMS privacy policies, and complete all the requirements below:

i. Per the Office of Management and Budget (OMB) Circular A-130, Personally Identifiable Information (PII), is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Examples of PII include, but are not limited to the following: Social Security number, date and place of birth, mother's maiden name, biometric records, etc.

ii. Based on information provided by the ISSO, system/data owner, or other security or privacy representative, it has been determined that this solicitation/contract involves:

[ ] No PII [X] PII

iii. The Contractor must support the agency with conducting a Privacy Threshold Analysis (PTA) for the information system and/or information handled under this contract to determine whether or not a full Privacy Impact Assessment (PIA) needs to be completed.

- If the results of the PTA show that a full PIA is needed, the Contractor must support the agency with completing a PIA for the system or information within *[CMS to insert contract-specific timeline]* after completion of the PTA and in accordance with HHS policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
- The Contractor must support the agency in reviewing the PIA at least every ***three years*** throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

e. **Controlled Unclassified Information (CUI). Executive Order 13556 defines** CUI as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR,* part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "*handling"* refers to "…any use of CUI,

including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323. The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be:

i. Marked appropriately;
ii. Disclosed to authorized personnel on a Need-To-Know basis;
iii. Protected in accordance with NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system; and
iv. Returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Information and/or data must be disposed of in accordance with NIST SP 800-88*, Guidelines for Media Sanitization*.

f. **Protection of Sensitive Information**. For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) must protect all government information that is or may be sensitive by securing it with a solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.

g. **Confidentiality and Nondisclosure of Information**. Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS must be used only for the purpose of carrying out the provisions of this contract and must not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its employees and subcontractors must be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any HHS records may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

The confidentiality, integrity, and availability of such information must be protected in accordance with HHS and CMS policies. Unauthorized disclosure of information will be subject to the HHS/CMS sanction policies and/or governed by the following laws and regulations:

i. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);
ii. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
iii. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

h. **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol must comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*.

i. **Information and Communications Technology (ICT).** ICT products and services from prohibited entities/sources must not be used/acquired in compliance with Public Law 115-232, Section 889 Parts A and B, FAR 4.21, FAR 52.204.23, FAR 52.204.24, and FAR 52.204.25. The contractor (and/or any subcontractor) must notify the government if

they identify prohibited ICT products and/or services are used during the contract performance.

j. **Government Websites.** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS must enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, HTTPS is not required, but it is highly recommended. Consult the *HHS Policy for Internet and Email Security* for additional information.

k. **Contract Documentation**. The Contractor must use provided templates, policies, forms and other agency documents found at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library to comply with contract deliverables as appropriate.

Standard for Encryption. The Contractor (and/or any subcontractor) must:

i. Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.
ii. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
iii. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and CMS-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).
iv. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with current FIPS 140 validation certificate from the NIST CMVP. The Contractor must provide a written copy of the validation documentation to the COR *[CMS-provided delivery date]*.
v. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys http://csrc.nist.gov/publications/. Encryption keys must be provided to the COR upon request and at the conclusion of the contract.

l. **Contractor Non-Disclosure Agreement (NDA)**. Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract must complete the CMS non-disclosure agreement. Contractors (and/or subcontractors) must submit a copy of each signed and witnessed NDA to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

2. Training Requirements

a. **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on this contract must complete the applicable HHS/CMS Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees must complete CMS Information Security Awareness, Privacy, and Records Management training at least ***annually***, during the life of this contract. All provided training must be compliant with HHS training policies.

b. **Role-based Training.** All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training ***annually*** commensurate with their role and responsibilities in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.

c. **Training Records.** The Contractor (and/or any subcontractor) must maintain training records for all its employees working under this contract in accordance with HHS policy. A copy of the training records must be provided to the CO and/or COR within ***30 days*** after contract award and ***annually*** thereafter or upon request.

3. Rules of Behavior

a. The Contractor (and/or any subcontractor) must ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior*, and *HHS Rules of Behavior for Privileged Users*.

b. All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least ***annually*** thereafter, which may be done as part of annual CMS Information Security Awareness Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.

4. Incident Response

a. The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/ CMS IRT teams **within 24 hours,** whether the response is positive or negative.

FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. In accordance with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*, an incident is "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies" and a privacy breach is "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized

user accesses or potentially accesses personally identifiable information for an other than authorized purpose." For additional information on the HHS breach response process, please see the *HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*."

b. In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) must:
   i. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract, with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
   ii. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor must send CMS approved notifications to affected individuals in accordance with the CMS Breach Analysis Team (BAT) instruction.
   iii. Report all suspected and confirmed information security and privacy incidents and breaches to the CMS Incident Response Team (IRT) *via the CMS Help Desk (410) 786-2580 or CMS IT Service Desk (cms_it_service_desk@cms.hhs.gov)*, COR, CO, CMS SOP (or his or her designee), and other stakeholders, including breaches involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than **one (1) hour**, and consistent with the applicable CMS and HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contact information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor must:
      - Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
      - Not include any sensitive information in the subject or body of any reporting e-mail; and
      - Encrypt sensitive information in attachments to email, media, etc.
   iv. Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* and HHS/CMS privacy breach response policies when handling PII breaches.
   v. Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.

5. Position Sensitivity Designations

All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract: **Tier 2S; Moderate Risk Public Trust (MRPT)**

6. Homeland Security Presidential Directive (HSPD)-12

   The Contractor (and/or any subcontractor) and its employees must comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; OMB M-05-24; OMB M-19-17; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS HSPD-12 policy; and *Executive Order 13467, Part 1 §1.2.*

7. Roster

   The Contractor (and/or any subcontractor) must submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster must be submitted to the COR and/or CO within a timeframe to be determined by CMS of the effective date of this contract. Any revisions to the roster as a result of staffing changes must be submitted within a timeframe to be determined by CMS of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.

   If the employee is filling a new position, the Contractor must provide a position description and the Government will determine the appropriate suitability level.

8. Contract Initiation and Expiration

   a. **General Security Requirements.** The Contractor (and/or any subcontractor) must comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor must follow the HHS EPLC framework and methodology or the CMS SDLC, as amended and in accordance with the HHS Contract Closeout Guide (2012).

   b. **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to HHS System Development Life Cycle requirements, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC and CMS SDLC that require artifact review and approval.

   c. **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) must provide all required documentation in accordance with the CMS SDLC, as Amended to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.

   d. **Notification.** The Contractor (and/or any subcontractor) must notify the CO and/or COR and system ISSO within as soon as possible or as determined by CMS before an employee stops working under this contract.

   e. **Contractor Responsibilities upon Physical Completion of the Contract**. The contractor (and/or any subcontractors) must return all government information and IT

resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor must provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or CMS policies.

f. The Contractor (and/or any subcontractor) must perform and document the actions identified the COR when an employee terminates work under this contract within 30 calendar days of the employee's exit from the contract. All documentation must be available to the CO and/or COR upon request.

9. Records Management and Retention

a. The Contractor (and/or any subcontractor) must maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and *HHS Policy for Records Management* and CMS policies and must not dispose of any records unless authorized by HHS/CMS.

b. In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, he/she must document and report the incident in accordance with HHS/CMS policies.

High Value Asset (HVA)
If a system is identified as HVA, the contractor must comply with the HHS Policy for the High Value Asset (HVA) Program and the DHS HVA Control Overlay in addition to the above requirements

Privacy Act

It has been determined that this contract is subject to the Privacy Act of 1974, because this contract provides for the design, development, or operation of a system of records about individuals from which records are retrieved by name or other identifying particular.

The System of Records Notice that is applicable to this contract is:

ESRD Program Management and Medical Information - **09-70-0520**
ASPEN Complaints/Incidents Tracking System (ACTS) - **09-70-0565**
Hospice Item Set (HIS) - **09-70-0548**
Inpatient Rehabilitation Facilities – Patient Assessment Instrument (IRF-PAI) - **09-70-0521**
Long Term Care Hospitals Quality Reporting Program (LTCH QRP) - **09-70-0539**
Long Term Care Minimum Data Set (LTCMDS) - **09-70-0528**
HHA Outcome and Assessment Information Set (OASIS) - **09-70-0522**

The system of records design, development, or operation work the Contractor is to perform is:

In performing this task, the contractor shall use all available CMS data bases, including the National Claims History, Standard Analytical Files, Physician/Supplier File, Enrollment Database, OPTN transplant file, OPTN transplant follow-up file, OPTN transplant waiting list file, ESRD Annual Facility Survey, OSCAR/CASPER, ESRD Facility Cost Reports, ESRD Network files, ESRD Network Standard

Information System files, OSCAR/CASPER files, Fistula First, and Group Health Plan files. Data from these systems will contain PII/PHI level data, which will be used to create program level non-PII reports.

The disposition to be made of the Privacy Act records upon completion of contract performance is:

Contractor will follow the HHS/CMS Records Management Policy and processes for data disposition.

CMS Security & Privacy Requirements Deliverables

Document	Deliverable Title/Description	Due Date
Roster	Roster	Initiation of contract and annually thereafter
Contractor Employee Non-Disclosure Agreement (NDA)	Contractor Employee Non-Disclosure Agreement (NDA)	Prior to performing any work on behalf of HHS/*CMS*
Training Records	Copy of training records for all mandatory training	In conjunction with contract award and annually thereafter or upon request
Rules of Behavior	Signed ROB for all employees	Initiation of contract and at least annually thereafter
Incident Response	Incident Report (as incidents or breaches occur)	As soon as possible and without reasonable delay and no later than 1 hour of discovery
Incident Response	Incident and Breach Response Plan	Upon request from *CMS*
Personnel Security Responsibilities	List of Personnel with defined roles and responsibilities	Initiation of contract and at least annually thereafter
Personnel Security Responsibilities	Off-boarding documentation, equipment and badge when leaving contract	Initiation of contract and at least annually thereafter
Background Investigation	Onboarding documentation when beginning contract.	Prior to performing any work on behalf of *CMS*
Certification of Sanitization of Government and Government Activity- Related Files, Information, and Devices.	Form or deliverables required by *CMS*.	At contract expiration
Contract Initiation and Expiration	If the procurement involves a system or cloud service, additional documentation will be required, such as Disposition/Decommission Plan	At contract expiration

CCSQ/QualityNet Security Requirements

In addition to all standard CMS requirements, contractors leveraging/utilizing CCSQ applications residing in the QualityNet Cloud are must also follow all applicable QualityNet policies, procedures and processes. This includes but not limited to the following; the

1. QualityNet Security and Privacy Framework policy
2. Security Awareness Training (SAT) procedures
3. QulaityNet CFE Use and Data Management Guide
4. QualityNet Incident Response procedures
5. QualityNet Vulnerability Remediation Guide
6. QualityNet Compliance Remediation Guide
7. QualityNet App Guidelines
8. QualityNet ATO procedures
9. CCSQ Agile Security Framework and processes
10. QualityNet DevSecOps processes
11. OualityNet onboarding/offboarding procedures
12. Other related security policies, procedures or memorandums

QualityNet Compliance & Vulnerability Management

Accurate and timely patching of known software vulnerabilities, whether published in vendors' periodic/ad hoc patch bulletins, or discovered through vulnerability testing, is essential to maintaining the security of Q- Net systems. Security Control SI-02 of the CMS ARS requires CMS to ensure that contractors install security-relevant software and firmware updates within specified timeframes. All contractors must follow CMS and QualityNet requirements, and industry best practices in keeping QualityNet systems at the latest patch level.

The process and timelines for management of vulnerabilities are located in the QualityNet Vulnerability Remediation Guide (*authentication required*). Processes and timelines for management of Compliance Baselines are located in the QualityNet Compliance Remediation Guide (*authentication required*).

Technical Reference Architecture (TRA)

The TRA communicates CMS's architecture approach and technical reference standards. By adhering to these standards, CMS, and project teams:

- Ensure an effective, standardized operating environment
- Assure sound and consistent security practices
- Promotes compliance with CMS decisions in future CMS task orders and acquisitions
- Enables interoperability and encourages reuse/shared infrastructure
- Provides a consistent set of architectural best practices for use throughout CMS

Please see the CMS Technical Reference Architecture (TRA) page in Confluence for additional information.

Technical Direction Board

The Technical Direction Board (TDB) has technical authority over all funded IT programs and IT projects assigned to ISG and included, or to be included, within CCSQ QualityNet. The TDB authority applies to the entire product lifecycle from the initial concept, planning, budgeting and acquisition activities through operations, product termination, archival, and contract close outs. Governance of CCSQ QualityNet Systems and the TDB is managed by ISG's Division of Quality Systems, Governance, Engineering and Development (DQSGED) and includes representation from other ISG groups and divisions including the ISG Front Office and the Information Security Staff (ISS) division. The TDB is comprised of subject matter experts in areas such as Cloud, Network, Shared Services, etc.

For a list of approved technology for use in the Q-Net environment (maintained in ISG Approved Technology Portfolio) or to submit a request for new technology, see the CCSQ QualityNet IT Governance page in Confluence (*authentication required*).

CCSQ/QualityNet Security and Compliance Roles

The Contractor must maintain security staff members on the contract at all times whose experience level is commensurate with their individual levels of responsibility. Contractors working within applications and systems within CMS and QualityNet must assign and designate individuals to the appropriate role in alignment with the work being performed. These roles are designed to help ensure security compliance within the respective Contractor organization and meet FISMA requirements of the Federal system being accessed. The Depending on the work being performed, an individual may obtain multiple security roles to support one contract. The Contractor must be responsible for properly protecting, safeguarding, and disposing of all information used, gathered, or developed as a result of work under this contract. The Contractor must also protect all government property or information, including, but not limited to, data and equipment, by treating the property or information as sensitive. The Contractor must consider all information about the systems gathered or created under this contract to be Controlled Unclassified Information (CUI).

For each of the applicable roles described below, the Contractor must identify the assigned personnel to the COR within one business day of contract award (as required by the onboarding process). Further, the assigned personnel must be able to perform the duties associated with the respective role within three days of the beginning of the contract's period of performance.

Additional information regarding CCSQ security and compliance roles may be found at the Qualitynet Contract Services site.

Security Point of Contact (SPOC):

The Primary goal of the Security Point of Contact is to ensure Contractor personnel adhere to CMS policies, including, but not limited to, applicable HHS Rules of Behavior (ROB) when using CMS and QualityNet information systems, the Contractor must assign a Security Point of Contact (and backup SPOC) to assist with helping CMS safeguard data as stated in such policies. The Contractor must use the QualityNet Security Point of Contact Appointment processes to identify both the SPOC and backup SPOC. The backup SPOC must be identified within 30 calendar days of the beginning of the period of performance.

The SPOC is required to support the *Baseline Security Requirements* outlined above to ensure the overall contractor and subcontractor personnel are compliant with security requirements set forth by CMS policy. The SPOC works directly with the QualityNet Cloud Contractor and the CMS QualityNet security team on multiple levels of security-related topics and is the central point of contact at the Contractor organization regarding security matters. The SPOC must fulfill the following responsibilities, including, but not limited to:

1. Maintain a general understanding of CMS and QualityNet security requirements and policies.
2. Assure all users complete necessary Security and Privacy training prior to accessing any CMS system and annually thereafter.
3. Manage and maintain all users' Annual Security Awareness Training (SAT) certificates.
4. Fulfill incident management responsibilities, to include immediate response to security incidents, and report any potential security incidents involving PII or PHI in a timely manner (1 hour from the time of identification).
5. Coordinate the destruction of sensitive information (if applicable).

Security Official (SO):

Access and Authorization management is essential component for security compliance. Each contractor holds the responsibility of ensuring individuals working on any task requiring access to CMS Federal systems are authorized based on their contractual needs. The Contractor must identify Security Officials (SOs) to work as "account administrators" responsible for managing user accounts and access related to the various QualityNet IT Services and Cloud environment. CCSQ provides a Federated Identity and Access management known as *HCQIS Access and Roles Provisioning system (HARP)*, the role for account administration is labeled as the "Security Official" (SO). The SO is responsible for managing accounts and access for various "QualityNet IT Services" that utilizes the HARP system for authentication and authorization. In addition, the Contractor must identify one or more backup SO within 30 days of the beginning of the contract's period of performance. The SO role is required to support the *General CMS Security & Privacy Policies* and its responsibilities may include, but are not limited to, providing or requesting new user accounts, password resets, locking and unlocking accounts, and performing account reviews.

System Security Officer (SSO):

Note: This role is applicable if the task order contains sections "*Government Information Processed on GOCO or COCO Systems*", "*Cloud Services*" and "*Other IT Procurements*" of the *CMS Security and Privacy Language for Information and Information Technology Procurements.*
Contractors tasked with developing and supporting a CMS system or application must identify a System Security Officer (SSO). In addition, the Contractor may identify an SSO back up. The SSO is only required to support IT Management or IT System Development and is responsible for implementing and maintaining system and application security controls and procedures to achieve and maintain technical compliance with CMS security requirements. The SSO must fulfill the following responsibilities, including, but not limited to:

1. Support the CMS ISSO in the achievement and maintenance of an ATO for each application or system supported by the Contractor.
2. Have a full understanding of the CMS' SA&A Processes.
3. Implement and maintain ARS controls for the appropriate system security level.

4. Develop and maintain FISMA system documentation.
5. Ensure systems adhere to Technical Reference Architecture (TRA) foundational and supplemental documents as additional security specifications, when applicable (available upon request).
6. Use approved security tools for continuous monitoring and management of security baselines.
7. Implement audit tools or processes for auditing and reporting services that support Continuous Diagnostics and Monitoring (CDM).
8. Provide engineering services and participation in Continuity of Operations Planning (COOP) and Disaster Recovery (DR) planning and exercises.
9. Develop and implement Configuration Management and Change Management plans when necessary.
10. Develop and maintain artifacts related to the CMS eXpedited Life Cycle (XLC) and CASF (the CASF is available upon request).
11. Perform or participate in threat and vulnerability management for applicable FISMA systems.
12. Perform POA&M management.
13. Assist the CMS ISSO with other additional security support efforts within the scope of contractual responsibilities.