Department of Health and Human Services
Centers for Medicare & Medicaid Services

Statement of Objectives for

Information Systems Foundational Components Support (ISFCS) II

Contents

1.0 Introduction

1.1 Purpose

The Centers for Medicare & Medicaid Services (CMS) seeks an effective contractor to develop foundational components, common infrastructure templates, tools, DevSecOps best practices and services for quality systems built and supported by the Information Systems Group (ISG) of the Center for Clinical Standards and Quality (CCSQ). The goal of this team is to make ISG's software development and DevSecOps more effective and efficient by building reusable code, providing tools and automation, monitoring site health, alerting, trouble-shooting incidents, debugging performance through distributed tracing, and searching through application and system logs. Resulting in cost savings and efficiencies where possible in our systems.

1.2 Background

CMS is a federal agency that ensures health care coverage for more than 100 million Americans. CMS continues to leverage internal resources and external partnerships to fulfill the CMS mission – as an effective steward of public funds, CMS is committed to strengthening and modernizing the nation's health care system to provide access to high quality care and equity of care.

In an effort to fulfill this charge, the CMS vision of future success is a high-quality health care system that promotes better care, access to coverage and improved health. The focus is on measurably improving care and population health by transforming the U.S. health care system into an integrated and accountable delivery system that continuously improves care, reduces unnecessary costs, prevents illness and disease progression, and promotes health. The Center for Clinical Standards and Quality (CCSQ) of CMS is dedicated to improving beneficiary health outcomes, enhance provider and clinical experience, and maximize value of healthcare program investments. The Information Systems Group (ISG) is located within CCSQ and its mission is to design, build, and continuously improve user-centered and innovative IT solutions to advance the CMS Quality Strategy.

Currently, the major quality programs, also referred to as lines of business (LOB), supported by ISG are: Hospital Quality Reporting (HQR), End Stage Renal Disease Quality Reporting System (EQRS), Internet Quality Improvement and Evaluation System (iQIES), Quality Payment Program (QPP), Enterprise System Services (ESS) and Quality Improvement Organizations (QIO) consisting of 4 main systems - Quality Management and Review Systems (QMARS), Financial Invoicing and Vouchering System (FIVS), Deliverable Administration Review Repository Tool (DARRT), and the CMS Quality Improvement Organization (QIO) Platform (CQP).

The Information Systems Group (ISG) manages multiple IT systems within each of its LOB. These IT systems facilitate the collection and management of provider information, patient demographic data, clinical data elements, survey information, and project data from Medicare and Medicaid providers. ISG has procured multiple IT vendors, also referred as Application Development Organizations (ADOs) to build and support these IT systems. These ADOs have deployed one or more development teams in charge of architecting, building and supporting these IT systems.

Each development team focuses on specific aspects of each system and may have a unique way of implementing certain processes, such as the deployment of code. The Information Systems Foundational Components Support (FC) contract was initially awarded to support the Quality Payment Program (QPP), and later expanded to support other ISG LOBs. The responsibility of the FC team is to focus on solving commonly occurring problems within the development teams, develop services to enable self-service of common tasks between teams, build foundation and common components and code library, and provide common DevSecOps and/or infrastructure framework when needed. In doing this, the FC team has helped maintain a unified voice within CMS and fostered continuing program improvements with respect to: Security, Stability, reliability, Scalability, Usability, Quality, and efficient delivery of work products. The current FC team is working with, and across most ISG LOBs that contain multiple development teams to ensure their overall success across several ISG's objectives (listed in Section 2.1 Objectives).

CMS believes one of the most effective ways to improve upon ISG's objectives is identifying and developing (following best practices such as automated testing and code review) common code, and automation that allows flexibility, re-usability, and efficient software deployment.

The Foundational Components team concept was modeled after the infrastructure teams that are common in private companies. This team is typically responsible for making other development teams within the company effective and efficient by building reusable tools and automation. In this way, the team provides "services" to the rest of the organization, and as such a member of this team tends to be highly technical (i.e., writing software), as well as very collaborative and a strong communicator.

1.3 Scope

With ISG LOB products workloads being spread across multiple ADOs and development teams, CMS has identified a need to address common pain points associated with the program. As part of the development process, different teams expend duplicate effort by solving similar problems, which has caused inconsistency in quality and delivery approach. For example, teams spend a lot of time and effort getting their code to meet deployment checklist requirements that are common to all teams. In general, the common pain points we have identified fall into categories such as incident response, identifying security threats, development process efficiency, and system observability. Existing development teams do not have enough bandwidth to speed up their deployment pipelines, effectively train and prepare for incidents, track and update security threats, set up and configure in-depth monitoring and logging, and a wide variety of other potential tasks that may yet arise and are foundational for an effective engineering process. Therefore, we have identified the continued need for an ISG Foundational Components support team to focus on developing, executing, and coordinating shared solutions to address these common pain points.

CMS is looking for the awarded contractor to establish small and effective teams to work with, and across all of these existing development teams to ensure the overall success of the ISG program across ISG's objectives, as listed in section 2.1 Objectives. Post award, these teams will work in collaboration with the CMS Technical Leadership, Solution Management Team (SMT) and CMS Product Managers (PMs) to prioritize among and within ISG's objectives, conduct user research with development teams understand existing pain points, build automated monitoring and visibility for the program success metrics, and establish a roadmap and backlog of technical user stories to improve overall Security, Stability, Reliability, Scalability, Usability, Quality and Efficiency of ISG Quality Systems. CMS is also looking for teams to drive innovation and pave the way for other LOBs struggling with capacity issues. This paving the way may come in the form of identifying new technologies or services that would enhance current LOB processes, presenting them to LOB SMT for approval, presenting these technologies to the ISG Technical Direction Board (TDB) for approval and to the Approved Technology Portfolio (ATP), and then presenting at meetings such as the ISG All-Hands or QualityNet (QNet) Chat to announce the intent and efficiencies of the new technology/service.

CMS requests Offerors to propose multiple FC teams to support multiple ISG LOBs as firm-fixed price (FFP) CLINs for performing the work as stated in this SOO. Historically, this CMS requirement has leveraged small high performing teams, most consisting of 6-8 highly technical individuals. CMS requests Offerors to justify their reasoning around their proposed staffing plan. We would expect these resources to primarily be very experienced and talented DevOps, Security, Cloud and Site Reliability/Platform engineers, with some Project Management support. The ideal team members can define and solve unconstrained problems, write code, and know how and when to make trade-offs when building systems.

It is important to note that CMS expect these FC teams to be fluid across ISG LOBs. Resources from one team should be able to immediately relocate to another team per the program need. Additionally, one LOB can be supported by exactly one FC team or by multiple FC teams depending on the size and need of the LOB. Similarly in some instances one team may be asked to support more than one LOBs or as an Enterprise FC team to support the ISG QNet holistically.

1.4 Assumptions and Constraints

1. The Contractor will actively participate in forums such as Communities of Practice and Town Halls at the request of CMS.
2. The Contractor will be onboarded within 5 business days after receipt of the intake form to QualityNet IT Services for QNet. The ISG Contract Engagement Lifecycle Standard Operating Procedures can be found here: https://QNetconfluence.cms.gov/display/ISGCO. Further information on the ISG Contract Engagement onboarding process can be found here: https://QNetconfluence.cms.gov/display/ISGCO/Access+to+Services.
3. All software/tools must be approved by CMS prior to use.
4. The Contractor will support the QNet Infrastructure Contractor, as needed in support of this requirement (e.g., for troubleshooting, upgrades, patching, maintenance weekends, etc.).
5. The Contractor shall adhere to all security requirements as noted in Section 3 of this document.
6. The Contractor shall utilize CMS supported tools such as Confluence, JIRA and Slack in its day-today operations. It is critical that any documents developed in the Contractor's own environment, be shared on the CMS supported tools noted, as CMS cannot rely on links to contractor supported Google drive documents, or the like, for long term access.
7. The Contractor shall comply with the 508 requirements.
8. The Contractor shall have a plan to transition from the incumbent Contractor at the beginning of the period of performance.
9. The Contractor shall have a plan to transition to a new Contractor at the end of the period of performance.

1.5 Task Order Expectations

The Contractor (also referred to in this document as Foundational Components (FC) team) is to act as a bridge between CMS leadership and ADO's development teams and enable those teams to better deliver value to CMS. That means this team's work is to be highly collaborative with various ISG development teams. The FC team has the difficult task of understanding, at a deep level, the successes and challenges of many different development teams. Doing this well requires building a level of trust between teams that can be difficult to develop.

One way to establish this trust and the corresponding boundary-spanning communication channels is by "embedding" high-skill technical servant leaders as productive members of each development team of LOB that the FC team would serve. Embedding a liaison into the team not only helps build trust, but it provides another level of expertise regarding architectural problem-solving. FC liaisons embedded within teams will work with teams to understand challenges and opportunities at the development level, program level and also at the CMS level. FC Liaisons will use the knowledge and insight gained from these relationships to respectfully advocate for positive continuous improvement in system development, amongst teams and by CMS.

Embedded Liaisons (ELs) roughly spend 50% of their time embedded with a development team, attending that team's sprint ceremonies and working on stories for that team. The remaining 50% of each liaison's time is spent as a part of the FC team, identifying cross-program opportunities for improvement and implementing solutions to those challenges (See Appendix A for example EL Concept). It is important to note that, depending on the development team's need, one EL may support multiple teams, or a single team may have more than one EL.
Additionally, each FC team engages with the program they serve within the context of that program, and that has led to a couple of different models of FC engagement. The EQRS FC team follow the embedded liaison model described above, while some programs may require little EL support with more focus on the FC team's backlog for developing and implementing common DevSecOps components, tooling and processes.

Another model is the Enterprise (QNet) FC team that serves entire QNet enterprise, developing and socializing shared solutions in partnership with each LOB but without embedding liaisons (See Appendix B for FC Team Concept for ISG Enterprise). At present time CMS is not requiring a separate and dedicated Enterprise (QNet) FC team. CMS requires that FC teams supporting individual LOBs (QPP, EQRS and QIO) shall not work in silos. These LOB FC teams shall collaborate with each other to make sure that common solutions are developed only once and shared and socialized to entire QNet enterprise, even outside of the LOB they serve. CMS would like Offerors to propose their ideas to ensure the support of QNet enterprise holistically and with strong collaboration between FC teams even in the absence of a dedicated Enterprise (QNet) team as conceptualized in the Appendix B.

CMS understands that ELs are one of many ways to build trust and improve cross team communication. CMS welcomes other innovative approaches and alternatives to the EL concept, and we ask Offerors to elaborate on their alternative and provide details on how their approach would work in the ISG environment and achieve the ISG objectives as stated in Section 2.1 Objectives.

The FC team also develops against a product backlog itself much like any other development team. This backlog is comprised of features and work to provide common components, solutions and support for the development teams. The product backlog is created by the team's ELs who surface the need or demand for a solution needed by their respective development team that will provides cross-program value. For instance, ELs may identify a need for development teams to have better quality test data. A solution to address this need is to create an automated tooling to de-identify and anonymize existing production level data for testing purpose. This story is then added to the FC team's product backlog and the tool is developed by the FC team to possibly serve more than one development team. The priority of the backlog is set by the program, with delivery integrated into each program's agile release train and other SAFe practices.

Other examples of the FC team's tasks may be to conduct user research with other development teams to identify common needs, develop common tooling (ideally by elevating work already done by one of the teams to a common tool), gather consensus for naming and other conventions (e.g. imagine if we rolled out DNS-based service discovery and needed to gain consensus on how to use Route53 and hostnames), and work with teams to incorporate common libraries and tools back into the various code bases. On this last point, the team might publish a new version of a shared logger, discover all codebases that require an upgrade, and create a pull request against those codebases to incorporate the new version. As described below, the success of many objectives is tied to adoption of common tools and standards across all teams on ISG. Based on our experience working across various projects, we believe that common tooling (i.e. software artifacts) is a better approach than shared services. This approach fits well with the ISG DevOps strategy in which each team does their own deployments. Rather than providing a centrally managed/controlled Jenkins instance, each team could build their own Jenkins (and install whichever plugins are needed) in order to do a deployment. This approach also allows a small team to have a greater improvement on the effectiveness of the program as a whole, without devoting a large amount of effort and resources to the operational support of internal services.

Often, the FC team will identify and work on initiatives that require changes to parts of the system build and maintained by other teams. In general, this team should be willing to drive those changes in any and all ways that they find effective (e.g. submitting pull requests to other teams Git repositories, pairing with developers from those teams to work through architectural issues). However, responsibility for the quality and performance of these changes still falls to the development team responsible for that part of the system. Similarly, for common tools and services maintained by this team, it is expected and encouraged for other development teams to contribute code or suggestions to those shared tools, but ultimately this FC team will be responsible for the quality and performance of those tools. For example, few of these common tools, services and processes developed by the incumbent are listed below. The new Contractor is to take total ownership of these tools and processes and make necessary improvements as needed.

- AWS Idle Instance Alerts – Utility to alert teams when instances are running idle for certain duration.
- EQRS Incident Response Process – Process to manage incidents within EQRS
- Monthly AWS Cost Report – Script to automatically create confluence page with AWS costs for the month and recommendations for savings

- QNet Bulk Data Faker – Utility to de-identify large volume of production files for testing purpose.
- Path to Production Checklist – A checklist before production deployment
- QOE (QPP Operational Efficiency) Dashboard – A UI dashboard to track AWS service expenditure by teams, services and time.
- QPP Automated On-boarding and Off-boarding – APIs to on-board and off-board team members by creating/removing accounts in various QPP tools
- QPP Bug Bash Process – Recurring events to identify bugs wherever they can be found by volunteers from development team modeled after "Bug Bounty" process
- QPP Data Faker – API to de-identify production level data for testing purpose
- QPP Incident Response Process – Process to manage incidents within QPP
- QPP Site Reliability Engineering (SRE), Security and Testing Guilds – Cross team forums to foster better DevOps, Security, and Testing practices
- QPP Synth Maker – Utility to create synthetic test data
- Technical Decision Log (TDL) Process – Process to make technical decisions on new technology, product or architecture.

In areas where the FC team can only achieve its objectives with the cooperation and coordinated action of other development teams (e.g. a shared logger that needs to be adopted by all teams), the FC team is expected to create a detailed recommendation, providing proof of concept and/or comparison of tools, describing the nature and magnitude of the work that needs to be done, outlining a timeline for the completion of that work, and enumerating specific measurable improvements achieved by this recommendation. This recommendation will be given to Solutions Management Team (SMT) and, assuming the recommendation is accepted by the product owners, incorporated into the work of the other teams as necessary. Once such a recommendation is accepted, both the FC team and the development team will share responsibility for ensuring that the recommendation is implemented correctly, efficiently, and effectively.

As such, this may mean that the FC team is only responsible for software libraries (and any testing environments) but not responsible for any production or management shared services. In cases in which a commercial tool or service is the best solution to the problem, the Vendor would provide licenses and support for onboarding (as automated as possible) of new teams to the tool.

Additionally, the members of the FC team will serve as Subject Matter Experts (SMEs) for the program and CMS. These SMEs will provide their expertise in the areas of Security, DevOps, Cloud, Architecture and AWS Cost Optimization. They are expected to work hand in hand with their Product Owners and with their respective leads from the other development teams to improve Security, Stability, Reliability, Scalability, Usability, Quality, and Efficiency of the system. In the event of any incident or any urgent needs, these SMEs are expected to jump in immediately and work with the development team to triage and solve the immediate issue in the most efficient manner. These SMEs will also be responsible for facilitating many Guilds namely, SRE Guild, Security Guild, and Testing Guild to enable discipline-specific sharing in the context of cross-functional teams.

Similar to the infrastructure teams discussed above, CMS does not intend for the FC team to accomplish each task simultaneously. Rather, CMS expects the FC team to be flexible and to prioritize the area of focus based upon primary need at the time. For example, during software development there may be more emphasis on deployment automation and threat modeling. Before a major launch, there may be more emphasis on incident detection and response areas.

Finally, the FC team will generally not be given specific direction to build a particular product or service. Rather, the team should bring recommendations on the best course of actions to their Product Owner and decide together what the best course of action is for the program they serve. We expect that the FC team will be comfortable determining and setting their own direction in collaboration with their CMS Product Manager in order to achieve ISG objectives outlined in "Section 2.1, Objectives". However, this requires the team to effectively identify, define, and prioritize worthwhile goals that will have substantial and specific positive impact on the program. To accomplish this, we expect that the FC team will approach their work using a data-driven approach, where objectives are tied to specific, measurable metrics, and recommendations for possible tools, services, or other improvements to the product development process.

2.0 Statement of Objectives

CMS/CCSQ/ISG seeks a contractor with the skills to enhance and maintain the existing Foundational Components to meet the ongoing and emerging needs of ISG.

For the successor contract, we expect the Contractor to continue the work done by the incumbent, including but not limited to:

1. Collaborate with CMS Technical leadership, CMS Solutions Management Team (SMT), Program Managers (PMs) and product teams to act as bridge between CMS leadership and ADOs while enabling those teams to better deliver value to CMS.
2. Identify existing pain points as it relates to code implementation and integration.
3. Help solve architectural problems and advocate for cross-product technical continuity.
4. Solve commonly occurring problems within the development teams by developing services to enable self-service, building foundational and common components, and providing common DevOps and/or infrastructure framework when needed.
5. Ensure ISG's overall success across several objectives as stated below.

2.1 Objectives – Task Areas

2.1.1 Increase efficiency of ISG's software development and DevSecOps by solving common problems with common code.

2.1.2 Increase efficiency and consistency of ISG's software development and DevOps by providing pre-vetted tools to expedite the path-to-prod and other readiness checklists. (See Appendix C for an example Path To Prod Checklist)

2.1.3 Improve the stability of ISG Quality systems for users by collaborating with and supporting other teams to ensure incidents are resolved quickly and effectively. Ensure practices and procedures are implemented to avoid further system degradation during an incident.

2.1.4 Improve confidence in ISG's Quality systems by quickly identifying incidents and clearly communicating system status to users as well as to internal and external stakeholders.

2.1.5 Improve product team and business owner confidence in the ISG Quality system security by ensuring a solid understanding of security implications of the software design and development process.

2.1.6 Improve product team and business owner confidence in ISG system security by ensuring threat modeling (See Appendix D for an example threat modeling process) is completed regularly on all parts of the system providing quick and consistent results without undue burden to existing development teams.

2.1.7 Improve the quality and velocity of ISG's development and deployment process by ensuring development teams can deploy and release features regularly and confidently, through automation.

2.1.8 Realize value of working software by deploying efficiently and as soon as possible after a feature is deemed ready by product owner.

2.1.9 Improve upon efficiency of software development and integration across teams by resolving issues quickly and efficiently after they are discovered.

2.1.10 Provide operational insight into the status of the website for all internal and external stakeholders in ISG by providing easy to use and automated reporting for relevant metrics.

2.1.11 Reduce overall cost of AWS Infrastructure by ensuring that ISG ADOs are making efficient use of AWS services (e.g., EC2 instance sizes, idle instances, etc.) and are accurately predicting future demand by implementing AWS Cost Dashboards, automated reporting, and alerts to provide cost feedback and detect waste.

2.1.12 Improve confidence in system ability to withstand major incidents by making best practices into automation (e.g., deploying across multiple availability zones and using auto scaling groups) and development processes (e.g., to update a vulnerable version of node.js or a library dependency).

2.1.13 Reduce burden on development teams by simplifying existing or implementing new internal processes such as Security Impact Analysis (SIA), Technical Decision Board (TDB), Technical Decision Log (TDL), etc. that enables development teams to get documented, researched, and approved direction from CMS with respect to significant or cross-cutting technical decisions and efficient approval for adoption of cutting-edge new technologies.

2.1.14 Enable discipline-specific sharing in the context of cross-functional teams by implementation of program mechanisms such as the SRE Guild, Security Guild, and Testing Guild within ISG LOBs.

2.1.15 Improve cross-product integration testing by implementing shared libraries to allow teams to consistently de-identify production data.

2.1.16 Improve testing capability and reduce individual team burden by implementing a self-service mechanism to allow teams and third-party service consumers to create synthetic test data that works consistently across disparate services and applications, such as creating appropriate QNet Access Roles and Profile (HARP) entities for authentication and authorization,

2.1.17 Improve program security awareness of ISG systems by implementation of periodic program-level bug bash that leverages the program's security expertise in creative ways that improve practical security.

2.1.18 Reduce burden associated with on-boarding and off-boarding of developers on a development team by creating self-service automated on-boarding and off-boarding tools that easily and automatically create accounts on various development tools.

2.1.19 Simplify and secure numerous AWS accounts for various development teams by implementing industry standard best practices with respect to AWS Accounts standardization and AIM policy managements.

2.1.20 Provide visibility of all work necessary to support efficient development and delivery of cross team business requirements by participating in SAFe Program Increment (PI) planning and working on Program Enablers to research, analyze, prototype prospective solutions and alternatives.

2.1.21 Provide Solution Architecture oversite from a holistic perspective of the application by understanding how things influence one another within a whole system, and helping teams understand the goal of the overall system architecture.

2.1.22 Develop dashboards that allow teams to see real time metrics on the quality of products they are delivering.

2.1.23 Work with other architects and systems teams throughout the QNet enterprise to promote reusability, as appropriate, and to understand the direction of the QNet enterprise.

2.1.24 Research and identify new technologies or methods that can be used by the whole program to deliver more value faster with cost savings. Help the QNet team continue to find innovative ways to deliver value faster.

2.1.25 Assist with driving down technical debt by helping with the refactoring of code.

2.1.26 Continually improve testing methodologies, and ensure end-to-end testing is complete.

2.1.27 Support the CMS Strategic Objectives and associated Strategic Pillars, support CCSQ Strategy, and support ISG Strategy and its associated Objectives & Key Results (OKRs) per CMS direction.

2.2 Coordination Between Teams

The coordination between the FC team and each development team will involve some coordination between ADOs and CMS Product Managers of the different teams.

For one, both teams (the FC team and the respective development team) are incentivized to ensure quality DevSecOps work on that application that provides security, performance, and reliability. If the development team is unable to fully meet those goals during a given deadline, CMS asks the FC team to indicate that there is a Severe Program Risk and that they are preparing to step in and take over the action to address the vulnerability and restore service to acceptable levels. This declaration would be made in coordination with the FC team's CMS Product Manager. This additional support would not be intended to be permanent and the application team, with the support and guidance of the FC team, would be expected to provide a plan for improvement to address the risk and take over maintenance of their operations going forward. The plan to address the program risk from the development team should include timelines, metrics, and clear deliverables to restore a high level of confidence in the DevOps program.

Similarly, the FC team is not intended as a replacement for high quality DevSecOps resources on any development team, including teams that are awarded new contracts for ISG. ISG will work to define minimum technical qualifications for each development team to ensure that they have sufficient qualifications to design, develop, and maintain their own operations meeting ISG's objective of security, performance, and reliability. If the FC team finds that the minimum technical qualifications are not sufficient in practice, or that teams are not meeting these minimum qualifications, the FC team should alert the CMS technical leadership. When this happens, the FC team is expected to write a "postmortem" style document describing, in as much details as possible, the issue, what problems it caused, and recommendations for how to resolve the issue.

2.3 Possible Metrics

CMS requests that each Offeror propose metrics for the performance of this contract. These metrics should be related to ISG's objectives as listed in section 2.1. The Offeror's metrics will become part of their PWS within the contract, so metrics should be chosen in such a way that they're easy to measure and track in an automated and low-overhead fashion.

As an example, metrics for the first 3 goals listed above are provided below. These metrics are not meant to be exhaustive or the exact right set of metrics, but presented as a sample:

1. Increase efficiency of ISG software development and DevOps by solving common problems with common code.
    - Adoption of shared libraries
    - Number of pull requests contributed to shared libraries by other teams.
    - Number of common issues (i.e. same cause) encountered across systems
    - Number of different tools that teams are using to accomplish the same tasks (e.g. CI build tools).
    - Number of new tools evaluated and incorporated into the common infrastructure.

2. Increase efficiency and consistency of ISG software development and DevOps by providing pre-vetted tools to expedite the path-to-prod and other readiness checklists.
    - Time from checklist review to final approval
    - Number of checklist items auto-approved due to usage of common tools

3. Improve the stability of ISG systems for users by collaborating with and supporting other teams to ensure incidents are resolved quickly and effectively. Ensure practices and procedures are implemented to avoid further system degradation during an incident.
    - Time to resolve incidents (real and simulated)
        - i. How long did it take to mitigate the issue?
        - ii. How long did it take to fully solve the issue?
    - Were any actions taken that made the problem worse?
    - Were any unnecessary actions taken that did not make the problem worse?

- Number of lessons learned in postmortem.
- Progress on implementing lessons learned from a postmortem.

CMS expects that the performance of this contractor will be dependent on the performance of other contractors' services. While this is unusual, this team is highly incentivized to make all work across all teams and for ISG, as a whole, successful.

2.4 Methodology and Quality Control

Unlike other development contracts, this team will generally not be given specific direction to build a particular product or service. We expect this team to be comfortable determining and setting their own direction in collaboration with their CMS product manager in order to achieve ISG's objectives as in section 2.1, and the quality of the FC team's work is in part determined by how effective the team is at identifying and/or anticipating problems on their own. As such, we expect that the methodology and quality control plans for this team will differ substantially from those of a typical development team focused on shipping a product.

Our expectation is that this team will, as part of its work, do substantial research and data analysis, including hands-on work with other teams, to devise recommendations which will deliver a measurable improvement on one of the ISG's objectives. These recommendations should contain a well-designed development plan, which may require work from this team as well as other development teams, key development milestones and a timeline for hitting them, (which should match the cadence on which the quality control assessments take place), as well as a clear and measurable estimate of the impact tied to existing metrics. The team can create concrete quality control measures based on the acceptance, implementation, and determine whether or not the observed improvement in our goal metrics is in line with the estimate.

Examples Quality Control Measures:

- Did we have a recommendation accepted by the Product Manager and start work this month?
  - This is a measure that shows that the team is generating high quality, high impact recommendations that are reasonable to implement.
- Did we deliver on a recommendation within the timeframe we proposed?
- Are we hitting the milestones we laid out when we put the recommendation in place?
  - These are example measures that show the team is accurately assessing the level of effort for each recommendation, including uncovering potentially unexpected aspects of the work ahead of time.
- Have we added a new metric that allows us a new way to measure our performance on one of the program level goals?

    - This is an example measure that shows that the team is taking a data-driven approach to identifying and measuring the impact of their recommendations.
- Have the recommendations improved on the performance metrics in the way we expected?
    - This is a measure that shows that this team is in fact making measurable improvements to the ISG product. This is likely to be the highest weight/most important part of any quality control plan.

2.5 Description of Technical Stack within ISG

While QPP was built natively on AWS Cloud Infrastructure, other ISG LOB's systems were on-prem and are currently at a different phase of being modernized and migrated to AWS Cloud Infrastructure. The below list includes all current ISG LOBs for informational purpose only. We are not creating an FC team to support each LOB at this time. We are only asking for three (3) teams; EQRS, QIO and QPP.

End Stage Renal Disease Quality Reporting System (EQRS):
EQRS is designed to unify the Consolidated Renal Operations in a Web-Enabled Network (CW) / Renal Management Information System (REMIS) and the Quality Incentive Program (QIP) systems into a combined system. This system is primarily built in AWS Cloud utilizing DevOps tools such as creating CI/CD pipelines with Jenkins, Talend studio, AWS PostgresSQL datatbase engines, Neo4j and Apache Zeppelin for data ingestion, exploration and visualization. EQRS primarily uses Amazon Linux, Microsoft Windows Server, and Distroless Base Images and associated software and libraries such as Python, Perl, etc. The EQRS System is based on the CMS three-tier architectural guidelines as QNet interprets them.
The EQRS System uses Java SE and Angular JS as the standard application development environment.
The following is a comprehensive (not all-inclusive) list of Tools/Technologies used by EQRS:

AWS Resources	Other
Athena AWS Backup AWS Config Certificate Manager CloudTrail CloudWatch Cost Explorer DynamoDB EC2	Angular CDK DefectDojo Docker Github Github Actions Java Jenkins Neo4j

EC2 Container Registry (ECR) EC2-ELB Elastic Container Service (ECS) Elastic File System (EFS) EMR GuardDuty Key Management Service (KMS) Kinesis Lambda Relational Database Service (RDS) Route 53 S3 SageMaker (Jupyter notebooks) Secrets Manager Security Hub Service Catalog Simple Email Service (SES) SNS SQS Step Functions Systems Manager VPC	Python R Scala Spark Snyk Sonarqube Spl

Quality Improvement Organizations (QIO):
Primary Support:

The CMS QIO Platform (CQP)
CQP is built using Salesforce as the platform (Service Cloud) with a few sites built using Experience Cloud. CQP also maintains a 3-tier AWS infrastructure to support data sharing between existing CCSQ systems and Salesforce. Below is a list of specialties a sprint team will need to focus on for staffing purposes.

- Salesforce – Platform (Service Cloud, Experience Cloud, CRM Analytics, Shield)
- AWS/API - API Gateway, S3, Glue, Lambda
- CI/CD - Copado, Copado Robotic Testing, Github, Github Actions
- Own Backup/Restore
- Security/Monitoring - ClamAV, Splunk, Snyk, New Relic, AppOmni

The primary CQP support area for this sprint team will be data sharing between Salesforce and internal/external systems. CQP will send and receive data from the Centralized Data Reposity (CDR) and will receive data from the Program Resource System (PRS) 2.0. CQP will also collect data from external sources of Provider data through APIs or uploads.

Quality Payment Program (QPP):

The QPP system is primarily built using Node.js and Angular, with one application (QPP Conversion Tool) running Java and three applications (QPP Cost+, QPP Analytics and Reporting, QPP Claims-to- quality) running Python. Node packages are used to share some functionality such as the scoring engines, the common style guide, and common libraries such as application loggers, a health check endpoint, and a versioning package. Databases are typically MySQL RDS, but there is also DynamoDB (used by the authentication session management service) and Redshift (used by analytics and reporting).

For almost all deployments, QPP uses Terraform to provision AWS resources, Packer to build AMIs, Docker to build and run applications, and includes other management tools written in Python. The QPP Front End team uses Ansible for both AMI builds and provisioning, is beginning to use Terraform, and is currently using a collection of custom auto scaling group deployment tools developed for healthcare.gov called Deployer.

Deploys are run by independent Jenkins servers. Each application development team runs their own VPCs, typically one per environment (DEV, IMPL, and PROD). Peering between the VPCs has been a source of some manual pain, as it requires the CCS AWS team to implement the request.

Logging is maintained in a centralized Splunk server, also run by CCS. NewRelic and Google Analytics are also run through shared accounts.

Internet Quality Improvement and Evaluation System (iQIES):

The iQIES is a cloud-native, API-first, micro services based application that integrates with (HARP) for authentication and authorization. While iQIES is a single application it can be decomposed into three major capabilities that supports Patient Assessments (PA), Survey and Certifications (S&C) and Reporting. The iQIES system is comprised of AWS infrastructure and services including the following, AWS EC2 Instances running RedHat Linux 7.4 operating system, AWS Simple Storage Service (S3), AWS Elastic Load Balancers (ELB), AWS ECS, AWS RDS PostGreSQL Database, and AWS Redshift Data Warehouse. The system is also comprised of the following software: Docker, Consul, Kong, NGINX, Node.js.

Enterprise Systems Services (ESS):

ESS consists of many COTS product, Open Source tools and some custom shared services that are provided for ISG Quality systems.

Headless Content Management System (H-CMS) uses MEAN Architecture Stack: MongoDB, Express, Angular and Node.js Open Source stacks and associated packages. Integrated Development Environment (IDE) Coding standards applied via IDE plugins/extensions for Prettier, ESLint and Editorconfig.
Managed File Transfer (MFT) uses COTS tool GoAnyWhere. Other COTS used are FileCloud and ServiceNow.

Data and Analytics uses several tools including SAS, TIBCO, ARCADIA and TRIFACTA.

Hospital Quality Reporting (HQR):
HQR system is currently being modernized so running in both an on-prem data center using enterprise licensed software as well as in a modernized Amazon Web Services Cloud environment using open source and modernized software. Some of the HQR legacy technologies are Informatica (ETL), WebLogic, Oracle RDBMS (RAC and standalone) Solaris servers, Axway (secure transport), F5 (load balancers). Some of the HQR modernized technologies are: AWS EC2, Cloud Formation, Jenkins, GitHub, Redshift, postgres11, Amazon RDS, AWS Schema Conversion Tool, Angular (presentation), AWS API Gateway, Amazon Dynamo DB, Amazon S3.

2.6 Example Backlog of Technical Stories

The following is an example of a backlog of technical stories. This is intended to provide an understanding of the type of work and skillsets needed by members of the FC team. As such, the user stories are not the best example of a well-written user story. They are also written from the perspective of this hypothetical team, so they may include some links and references that don't exist.

Note that the stories here are not written like traditional user stories (i.e. they don't follow "As a ___, I want ___ so that ___"), but are based on the notion of technical stories as described in the following link:

http://rgalen.com/agile-training-news/2013/11/10/technical-user-stories-what-when-and-how

The following section is a sample "un-prioritized backlog". These sample stories should go through refinement, estimation, and prioritization before they can become part of a sprint, a two-week timeframe.

Again, this should no way be taken as actual work that will be performed by the FC team. As stated in the previous section, the FC team will generally not be given specific direction to build a particular product or service. The FC team should be self-motivated to come up with the list of technical stories for the LOB they serve and include them on their backlog and prioritize in consultation with the development team and the CMS Product Manager.

ISG COMMON-X - Embed with Team X for one sprint

The purpose of this is to do primary research on the challenges this team faces with infrastructure, to use firsthand data to inform future decisions about what we work on. This will also give a better understanding of that team's processes and enable personal connections that can be used to increase cross team communication.

The deliverable from this issue is documentation that describes the overall vision of the team, from architecture to process, in a standard way that other teams can easily understand. This can, and should, reuse documentation from the team itself, assuming it is in a format that is easy to understand by people not on the team.

For example, this report might include:

- Any frustrations experienced by the team with the current process or tools.
- Any major concerns expressed by the team that have not made it up the chain.
- Any observed cross organization miscommunications or process dysfunction.
- List of technologies used, and how they are used.
- Documentation of current architecture, in as standard of a format as possible. For example:
  - Deployment pipelines
  - Monitoring stack.
  - Logging stack.
  - Application stack.
- List of custom-built tools with documentation.
- Possible opportunities for cross team sharing.
- Other items that are learned in the process that might be important to ISG.

Note that critical production issues should be fixed by working with the team directly rather than escalating or reporting on whenever possible, both to foster trust and to better understand the current incident resolution process.

ISG COMMON-X - Create or Find Standard ELB Monitoring Toolkit

This task is to find out if any teams already have the ELB Cloudwatch Alarms in configuration as code and repurpose that if possible. If not, the task is to build this toolkit, and have it reviewed by all teams to make sure it meets their needs and is a superset of the coverage of the current alarms they have configured already.

ISG COMMON-X - Run LOB-Wide Incident Drill

The main idea here is to simulate a real failure in the system, and then go through the process of fixing it while documenting the steps taken for each ISG LOBs. The goal is to learn about deficiencies both in the system and the incident response process before encountering a real-world incident.

The deliverables from this issue are creating a test plan that includes notifying stakeholders that a test is happening without disclosing any specific details, scheduling, and running the test, holding a postmortem meeting to generate a write-up of what went well and what needs to be improved, and doing the work necessary to get the follow up work in everyone's backlog.

ISG COMMON-X - Add Low Disk Space Cloudwatch Alarm to RDS Module

QPP has some common "configuration as code" for setting up and RDS module in AWS.

It was recently pointed out that this is missing a low disk space alert. Since there is no other alert that would tell us if disk space is low to mitigate this, it poses a high likelihood of an outage that teams don't receive advance warning to deal with. Since a full database is difficult to recover from quickly, the impact in terms of hours of outage would also be relatively high. On top of that, 5 teams are using this module, so the risk and impact are multiplied by 5.

So QPP has a high risk and high impact, resulting in **risk (high) * impact (high) = priority (high)**, this high risk is common across 5 (teams) and should be fixed as soon as there are no other more critical issues.

ISG COMMON-X - Understand Current Change Management Issues with Component Z

Team Z builds some foundational components that other teams heavily rely on, specifically Component Z. There have been several incidents that have been traced back to changes in Component Z, that other teams have not been prepared to address.

This task is to work with this team to fully understand the current process, the past issues, and the current roadmap to understand ways to achieve the outcome of reducing the number of incidents when an upgrade happens.

Things to look for:

- Cultural or procedural differences between teams that cause miscommunication.
- Components that are not in version control or inaccessible to those who need to see them.

- Opportunities to standardize with current common tools to make the boundaries more fault tolerant.

The result should be a proposal for how this system could be improved, including potential policy changes that could be made, and a fallback plan if those can't be made for some reason. This should include clearly documented downsides for the fallback plan if there are any, to gather data on the negative impact of the policy to hopefully inform future policy fixes (since they are on a much longer cycle than software).

ISG COMMON-X - Establish common tools for Secrets Management
It's clear that all teams need a common mechanism for configuring secrets for an application as well as a mechanism for configuring secrets differently for each environment. Currently, there are multiple tools are in use for projects within ISG. We should evaluate, analyze and propose the common tool for LOB or for ISG. It is preferred to reuse components from other teams wherever possible, and only write our own tools if no one else has started.

ISG COMMON-X - Threat Model for Secrets Management
Perform a threat modeling exercise for secrets management to identify threats related to the secrets stored in this system and how they are accessed.

ISG COMMON-X - Assess high value assets
Perform a top to bottom analysis of the ISG systems to identify and rank (based on work with stakeholders) the high value assets (note: an asset is not just a piece of data, e.g. an API token can be high value) for each. This list is to be used to order subsequent threat modeling exercise.

ISG COMMON-X - Develop dashboard for incident response times
Integrate with the PagerDuty API to pull data related to incidence and the time it takes for teams to response. Develop a real-time dashboard to report on various metrics (e.g. median and maximum response time per team).

ISG COMMON-X - Dashboard describing live versions of code across environments
In order to improve communication and debug ability, establish a simple web site that reflects the currently deployed version of all codebases in each environment. The dashboard should include a link to relevant GitHub and JIRA content about each codebase.

ISG COMMON-X - Evaluate Intrusion Detection System (IDS) for ISG Systems
In order to improve security and prevent intrusion, evaluate various IDS products (e.g.

Guard Duty) and recommend and implement the best fit for the program being served.

ISG COMMON-X – Standardize AWS Accounts across the program

When new ADOs were on boarded to AWS clouds they were assigned single linked account per vendor. As program grew, we have numerous AWS accounts based on vendors rather systems, components or environments. As vendors changed the account names did not make sense. Additionally, single accounts were used across all 3 tiers, DEV, IMPL and PROD that created security risk. The team should evaluate and implement best practices with respect to AWS accounts.

ISG COMMON-X – Create TIN service to encrypt/decrypt TIN system wide

There is frequent issue of spilling TIN and other sensitive information within Splunk, GitHub and other tools. Although databases are encrypted at rest, but TIN and other sensitive information may not always be encrypted in transit. TINs to be stored in a single location and individual components to store non-PII identifiers that are linked through a service to real TIN. Therefore, create a TIN service so that TIN is always safe and will only be available when needed to be seen by the end user.

ISG COMMON-X – Draft SIA (Security Impact Analysis) for XXX

SIA is needed whenever there is major change to an existing system or trying to implement new technology or tools within the system. Often time these SIA process present undue burden for the development team. The team should help the development team create SIA when needed or create entirely on their behalf working with the development team and CMS ISSOs.

ISG COMMON-X – Centralized Security Reporting

There is multiple security tooling across ISG systems such as Nessus scan, Snyk findings, GitHub vulnerability, AWS trusted advisors and so on. The team should centralize security findings from decentralized tooling used across accounts into a single place to improve security compliance and monitoring.

ISG COMMON-X – Create architecture for securing beneficiary data

Beneficiaries PHI and PII information are considered the most sensitive data within CMS. When there is requirement for displaying beneficiary data on internet to providers and beneficiaries, it presents challenges with respect to privacy and security. The team should review the exiting architecture, security and privacy rules implementation of the system and present recommendation or changes to handle beneficiary data.

3.0 Security

3.1 General CMS Security & Privacy Policies

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.

CMS/HHS Security and Privacy requirements based on the *“CMS Security and Privacy Language for Information and Information Technology Procurements” CMS Security & Privacy Library. Additional Information and IT considerations may be determined at the task orders.*

✓ 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

3.1.1 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 [X] Moderate [ ] High
      - **Integrity:** [ ] Low [X] Moderate [ ] High
      - **Availability:** [ ] Low [X] Moderate [ ] High
      - **Overall Impact Level:** [ ] Low [X] 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:

[X] No PII [ ] 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.
111

- 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:

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

3.1.2 Cloud Services

1. HHS FedRAMP Privacy and Security Requirements

   The Contractor (and/or any subcontractor) must be responsible for the following privacy and security requirements:

   a. **FedRAMP Compliant ATO**. Comply with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO by a timeline determined by CMS.

      i. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The *HHS Information Security and Privacy Policy (IS2P), HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance*, and the CMS Information System Security and Privacy Policy (IS2P2) further define the baseline policies as well as roles and responsibilities. The Contractor must also implement a set of additional controls identified by the agency when applicable.

      ii. A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and ***annually*** thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

   b. **Data Jurisdiction.** The contractor must store all information within the security authorization boundary, data at rest or data backup, within the Continental United States (CONUS) if so required. Refer to G.x Contractor Work Performed Outside of the United States and its Territories (April 2016) in the Solicitation/Contract.

   c. **Service Level Agreements.** *Add when applicable* The Contractor must understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with CMS to develop and maintain an SLA.

   d. **Interconnection Agreements/Memorandum of Agreements.** *Add when applicable* The Contractor must establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/CMS policies.

2. Protection of Information in a Cloud Environment

   a. If contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they must protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/CMS policies https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html.

b. HHS/CMS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS/CMS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS/CMS and hosted on contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data must be available to HHS/CMS within ***one (1) business day*** from request date or within the timeframe specified otherwise. In addition, the data must be provided at no additional cost to HHS/CMS.

c. The Contractor (and/or any subcontractor) must ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS/CMS policies.

d. The contractor must support a system of records in accordance with NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:

   i. Maintenance of links between records and metadata, and

   ii. Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

e. The disposition of all HHS/CMS data must be at the written direction of HHS/CMS. This may include documents returned to HHS/CMS control; destroyed; or held as specified until otherwise directed. Items returned to the Government must be hand carried or sent by certified mail to the COR.

   i. If the system involves the design, development, or operation of a system of records on individuals, the Contractor must comply with the Privacy Act requirements.

3. Assessment and Authorization (A&A) Process

a. The Contractor (and/or any subcontractor) must comply with HHS/CMS and FedRAMP requirements as mandated by federal laws, regulations, and HHS/CMS policies, including making available any documentation, physical access, and logical access needed to support the A&A requirement. The level of effort for the A&A is based on the system's FIPS 199 security categorization and HHS/CMS security policies. The contractor must obtain authorization prior to deployment or service implementation.

   i. In addition to the FedRAMP compliant ATO, the contractor must complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation within CFACTS in a timeline to be determined by CMS. The agency ATO must be approved by the CMS authorizing official (AO) prior to implementation of system and/or service being acquired.

   ii. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO but should not use self-assessment. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.

   iii. For all acquired cloud services, the A&A package must contain the following documentation:

      - Security Assessment Plan (SAP)/Security Assessment Report (SAR)

- System Security Plan (SSP)
- Plan of Action and Milestones
- Contingency Plan and Contingency Plan Test
- E-Authentication Questionnaire].

Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS*/CMS* policies using CMS templates and defined timelines.

b. HHS/CMS reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If HHS/CMS exercises this right, the Contractor (and/or any subcontractor) must allow HHS/CMS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS/CMS requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
c. The Contractor must identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the contractor must document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS/CMS may require remediation at the contractor's expense, before HHS/CMS issues an ATO.
d. The Contractor (and/or any subcontractor) must mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings must be remediated, in accordance with timelines specified in the HHS POA&M Standard, from discovery: (1) critical vulnerabilities no later than ***fifteen (15) days*** and (2) high within **thirty (30) days** (3) medium within **ninety (90) days** and (4) low vulnerabilities no later ***than three hundred and sixty (360).*** In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the timelines assigned to the POA&M within CFACTS. HHS/CMS will determine the risk rating of vulnerabilities using FedRAMP baselines.
e. **Revocation of a Cloud Service**. HHS/CMS have the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS/CMS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or CMS may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

4. Reporting and Continuous Monitoring
   a. Following the initial ATOs, the Contractor (and/or any subcontractor) must perform the minimum ongoing continuous monitoring activities specified below, submit required

deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities. Meetings shall be held at least monthly, or as needed.

b. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis via the CCIC requirements which can be provided by contacting EVM-CMP@cms.hhs.gov. Deliverables are identified as:
   i. Operating system, database, Web application, and network vulnerability scan results;
   ii. Updated POA&Ms;
   iii. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the CMS System Owner or AO; and
   iv. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/CMS security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the agency.

5. Configuration Baseline
   a. The contractor must certify that applications are fully functional and operate correctly as intended on systems using *HHS Minimum Security Configurations Standards Guidance*. The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved HHS*/CMS* configuration baseline.
   b. The contractor must use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS/CMS and NIST defined configurations and do not alter these settings.
6. Incident Reporting

   a. The Contractor (and/or any subcontractor) must provide an Incident and Breach Response Plan (IRP) in accordance with HHS*/CMS]*, OMB, and US-CERT requirements and obtain approval from CMS. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.
   b. The Contractor (and/or any subcontractor) must implement a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of federal data, afford HHS/CMS access to its facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of notification. The program of inspection must include, but is not limited to:
      i. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS/CMS personnel, or agents acting on behalf of HHS/CMS*,* using agency-operated equipment and/or specified tools. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol (SCAP) standards and have been approved by the

agency. The agency may request the Contractor's scanning results and, at the agency discretion, accept those in lieu of agency performed vulnerability scans.

ii. In the event an incident involving sensitive information occurs, cooperate on all required activities determined by the agency to ensure an effective incident or breach response and provide all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. In addition, the Contractor must follow the agency reporting procedures and document the steps it takes to contain and eradicate the incident, recover from the incident, and provide a post-incident report that includes at a minimum the following:
    - Company and point of contact name;
    - Contract information;
    - Impact classifications/threat vector;
    - Type of information compromised;
    - A summary of lessons learned; and
    - Explanation of the mitigation steps of exploited vulnerabilities to prevent similar incidents in the future.

7. Media Transport
    a. The Contractor and its employees must be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).
    b. All information, devices and media must be encrypted with HHS/CMS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.
8. Boundary Protection: Trusted Internet Connections (TIC)
    a. The contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes that are in compliance with the requirements of the Office of Management and Budget (OMB) Memorandum (M) 19-26: Update to the TIC Initiative, TIC 3.0.
    b. The contractor must route all external connections through a TIC.
    c. **Non-Repudiation**. The contractor must provide a system that implements encryption with current FIPS 140 validation certificate from the NIST CMVP that provides for origin authentication, data integrity, and signer non-repudiation.

3.1.3 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 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. 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.

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 Official (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.

4.0 Schedule and Deliverables

4.1 Period and Place of Performance

The period of performance is from task award through **[xx/xx/xxxx].** The primary place of performance will be the Contractor’s facilities with frequent visits to CMS facilities in Baltimore, Maryland.

4.2 Delivery Schedule

In performing the services and providing the support described in this Performance Work Statement, the Contractor must provide the following deliverables:

Section Reference	Deliverable Name	Due Date
2.1.5	**Complete Sprint Closeout Activities to Enable Jira Sprint Reporting**	**End of each Sprint/Iteration**

5.0 Software License Management

The current FC Contractor provides license/subscriptions for QPP, EQRS and QIO in support of the task areas and these should be included in the Offeror’s proposal as ODC.

Software and Applications, Subscriptions	License Expiration Date	Seat Count
• Sonar Cloud	N/A	N/A

• Zoom	N/A	13
• Docker Team	N/A	20
•		
•		-
•		-

CMS may add or remove licenses from this list as technologies needed to support the environment and user community may change.

6.0 Travel

The Contractor may be required to travel in support of this requirement. The Contractor should anticipate to travel to the following events:

CMS/ISG is reserving the right to potentially host no more than two, Program Increment Planning events in person per contract period for each LOB. If these events occur, they will either be held in the Baltimore, Howard, or Anne Arundle County areas. Offerors should include any applicable travel expenses for these potential events in their proposed cost. Based on previous events of this type, the Government predicts the following:

- Duration of Trip: 3-4 days (depending on flight availability)
- Travel Days: 2
- Lodging: 2-3 nights (depending on flight availability)

In addition to the above requirements, the Contractor should anticipate traveling to CMS Headquarters twice a year to review the contract with the program office and contracting team.

7.0 Contract Transition

7.1 Contract Transition-In

The contractor shall be available to receive the transition of information and system knowledge from the previous contractor to ensure the continuity of operations on day one of the contract. A Transition-In plan shall be prepared by the contractor and include the efforts that need to be conducted for a successful transition from the incumbent contractor. The Transition-In plan will need to be reviewed and approved by the CMS COR and CMS Program Managers after award so the plan can be in place on day one of the contract. The transition-in period will be 6 weeks (3 sprints).

7.2 Contract Transition-Out

The contractor shall be available to transition information and system knowledge to the incoming contractor at the end of the contract life to ensure the continuity of operations. A Transition-Out plan shall be prepared for by the outgoing contractor and include the efforts that need to be conducted for a successful transition from the incumbent contractor. The Transition-Out plan will need to be reviewed and approved by the CMS COR and CMS Program Managers 180 days prior to the end of the contract to ensure there is enough time execute the plan in full to the new contractor. The transition-in period will be 6 weeks (3 sprints).

The Transition-Out Plan shall include:

- Transition Schedule
- Delivery of final deliverables, artifacts, and lesson learned
- Delivery of software, release/code versions, processes, artifacts, and documents supporting each task area of the SOO or PWS
- Training of relevant Government personnel and Contractors.
- All security concerns such as badges, tokens, and accounts shall be communicated to the CMS COR.
- All final documentation and material will be archived in a secure location as directed by the CMS COR.
- Provide closeout certifications that include a statement that the contract is complete, all deliverables have been provided, all services are complete, and there are no outstanding contractual issues.
- Plan for ensuring that, prior to termination or completion of this effort, the Contractor/Subcontractor does not destroy any information in any form received from CMS, or gathered/created by the Contractor in the course of performing this effort without prior written approval by CMS PM/COR. Any data destruction done on behalf of CMS by a Contractor/Subcontractor must be done IAW National Archives and Records Administration (NARA) requirements.
- An orientation phase to introduce the successor Cloud Services Provider personnel, programs, and users to the incumbent team, explaining tools, methodologies, and business processes.
- A Phase-Out Migration Checklist (Contractor format).

Providing signed turnover agreements in the CMS designated format.

8.0 Section 508 – Accessibility of Electronic and Information Technology

Section 508 Requirements
Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communication technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

Item that contains ICT: ISFCS III

ISFCS III

E205.1 General Electronic content shall comply with E205.

E205.2 Public Facing Electronic content that is public facing shall conform to the accessibility requirements specified in E205.4.

E205.3 Agency Official Communication Electronic content that is not public facing shall conform to the accessibility requirements specified in E205.4 when such content constitutes official business and is communicated by an agency through one or more of the following:

A. An emergency notification;

B. An initial or final decision adjudicating an administrative claim or proceeding;

C. An internal or external program or policy announcement;

D. A notice of benefits, program eligibility, employment opportunity, or personnel action;

E. A formal acknowledgement of receipt;

F. A survey questionnaire;

G. A template or form;

H. Educational or training materials; or

I. Intranet content designed as a Web page.

E205.4 Accessibility Standard (WCAG 2.0) - Electronic content shall conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (Incorporated by reference, see 702.10.1).

E206.1 General. Where components of ICT are hardware and transmit information or have a user interface, such components shall conform to the requirements in Chapter 4.

E207.1 General Where components of ICT are software and transmit information or have a user interface, such components shall conform to E207 and the requirements in Chapter 5

Exception from E207.1 General: Software that is assistive technology and that supports the accessibility services of the platform shall not be required to conform to the requirements in Chapter 5.

E207.2 WCAG Conformance User interface components, as well as the content of platforms and applications, shall conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1).

Exceptions from E207.2 WCAG Conformance:

Software that is assistive technology and that supports the accessibility services of the platform shall not be required to conform to E207.2.

Non-web software shall not be required to conform to the following four Success Criteria in WCAG 2.0: 2.4.1 Bypass Blocks; 2.4.5 Multiple Ways; 3.2.3 Consistent Navigation; and 3.2.4 Consistent Identification.

Non-Web software shall not be required to conform to Conformance Requirement 3 Complete Processes in WCAG 2.0.

E208.1 General Where an agency provides support documentation or services for ICT, such documentation and services shall conform to the requirements in Chapter 6.

E301 General

E301.1 Scope. The requirements of Chapter 3 shall apply to ICT where required by 508 Chapter 2 (Scoping Requirements), 255 Chapter 2 (Scoping Requirements), and where otherwise referenced in any other chapter of the Revised 508 Standards or Revised 255 Guidelines.

E302 Functional Performance Criteria

302.1 Without Vision. Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that does not require user vision.

302.2 With Limited Vision. Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited vision.

302.3 Without Perception of Color. Where a visual mode of operation is provided, ICT shall provide at least one visual mode of operation that does not require user perception of color.

302.4 Without Hearing. Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that does not require user hearing.

302.5 With Limited Hearing. Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited hearing.

302.6 Without Speech. Where speech is used for input, control, or operation, ICT shall provide at least one mode of operation that does not require user speech.

302.7 With Limited Manipulation. Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that does not require fine motor control or simultaneous manual operations.

302.8 With Limited Reach and Strength. Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that is operable with limited reach and limited strength.

302.9 With Limited Language, Cognitive, and Learning Abilities. ICT shall provide features making its use by individuals with limited cognitive, language, and learning abilities simpler and easier.

503.1 General Applications shall conform to 503.

504.2 Content Creation or Editing Authoring tools shall provide a mode of operation to create or edit content that conforms to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1) for all supported features and, as applicable, to file formats supported by the authoring tool. Authoring tools shall permit authors the option of overriding information required for accessibility.

504.2.1 Preservation of Information Provided for Accessibility in Format Conversion. Authoring tools shall, when converting content from one format to another or saving content in multiple formats, preserve the information required for accessibility to the extent that the information is supported by the destination format.

504.2.2 PDF Export. Authoring tools capable of exporting PDF files that conform to ISO 32000-1:2008 (PDF 1.7) shall also be capable of exporting PDF files that conform to ANSI/AIIM/ISO 14289-1:2016 (PDF/UA-1) (incorporated by reference, see 702.3.1).

504.3 Prompts. Authoring tools shall provide a mode of operation that prompts authors to create content that conforms to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1) for supported features and, as applicable, to file formats supported by the authoring tool.

504.4 Templates. Where templates are provided, templates allowing content creation that conforms to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1) shall be provided for a range of template uses for supported features and, as applicable, to file formats supported by the authoring tool.

602.1 General. Documentation that supports the use of ICT shall conform to 602.

603.1 General. ICT support services including, but not limited to, help desks, call centers, training services, and automated self-service technical support, shall conform to 603.

Transition- Incumbent contractor shall transition to the incoming contractor the status of 508 testing activities, such as test dates and/or remediation plans.

9.0 Applicable Documents and Appendices

[Provide any documents or appendices that are specified in this PWS and are necessary to assist the Contractor with drafting the proposal.].

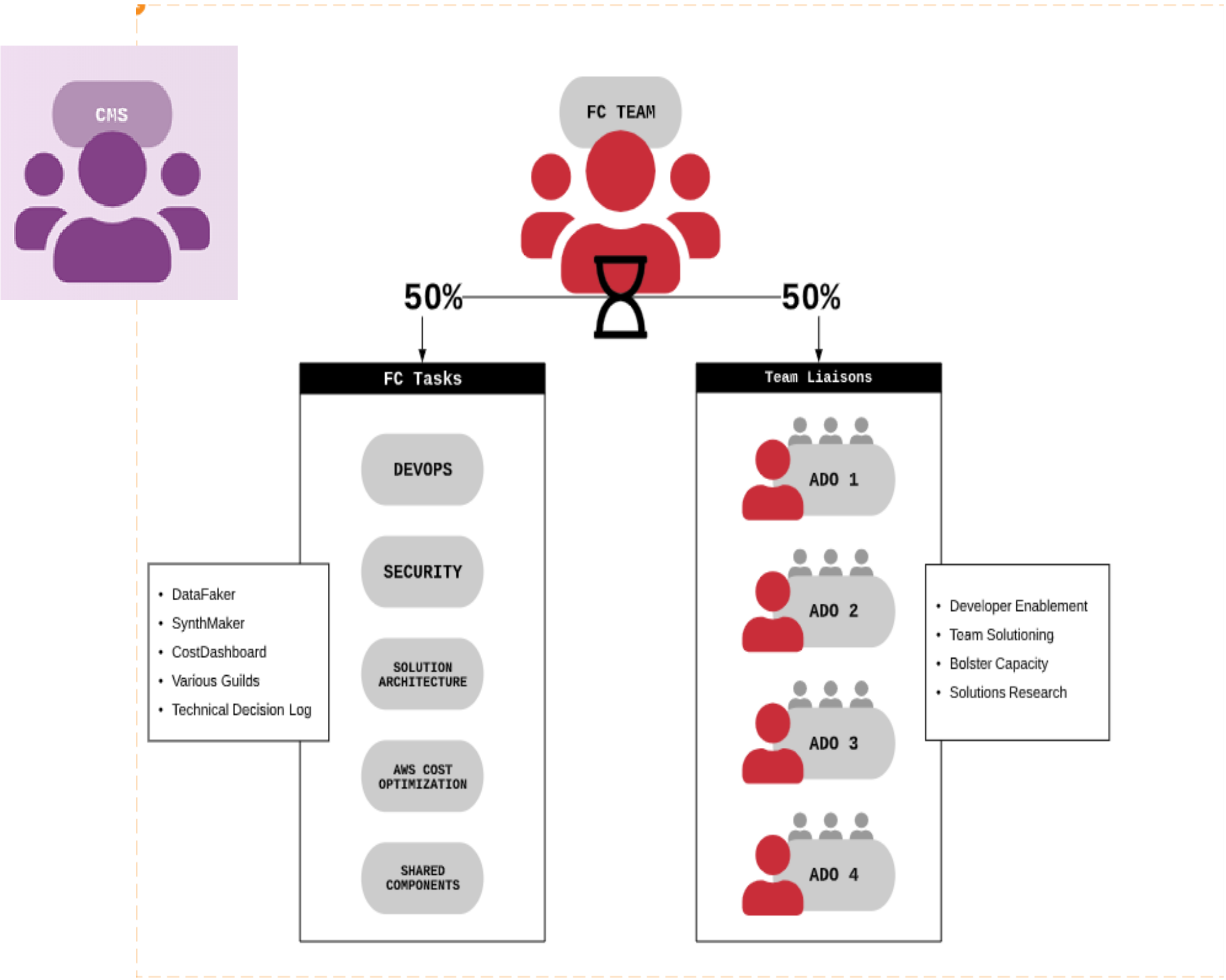
- 2020 QPP Final Rule: https://www.federalregister.gov/documents/2019/11/15/2019-24086/medicare-program-cy-2020-revisions-to-payment-policies-under-the-physician-fee-schedule-and-other
- 2020 QPP Final Rule Executive Summary: https://qpp-cm-prod-content.s3.amazonaws.com/uploads/738/2020%20QPP%20Final%20Rule%20Executive%20Summary.pdf
- QPP MIPS Scoring: https://qpp-cm-prod-content.s3.amazonaws.com/uploads/179/2018%20MIPS%20Scoring%20Guide_Final.pdf
- Data Submission UI: https://www.youtube.com/watch?v=q0Cvke6fnrg
- CMS Bene Sampler Reporting (Web Interface Seminar): https://www.youtube.com/watch?v=S4M5k3lgbHU&list=PLaV7m2-zFKpjIg8s_JgXZBsMWRQch9lP2
- QPP Account Creation video/HCQIS Access Roles and Profile (HARP):

https://youtu.be/4xGkWvPa33E

- EQRS website: https://eqrs.cms.gov/
- ESRD Quality Incentive Program: https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/ESRDQIP
- Social Security Act of 1881: https://www.ssa.gov/OP_Home/ssact/title18/1881.htm
- EQRS GitHub access will be provided to contractors upon request
- CQP MVP Architecture Diagram
- CQP 3-Tier AWS Architecture Diagram

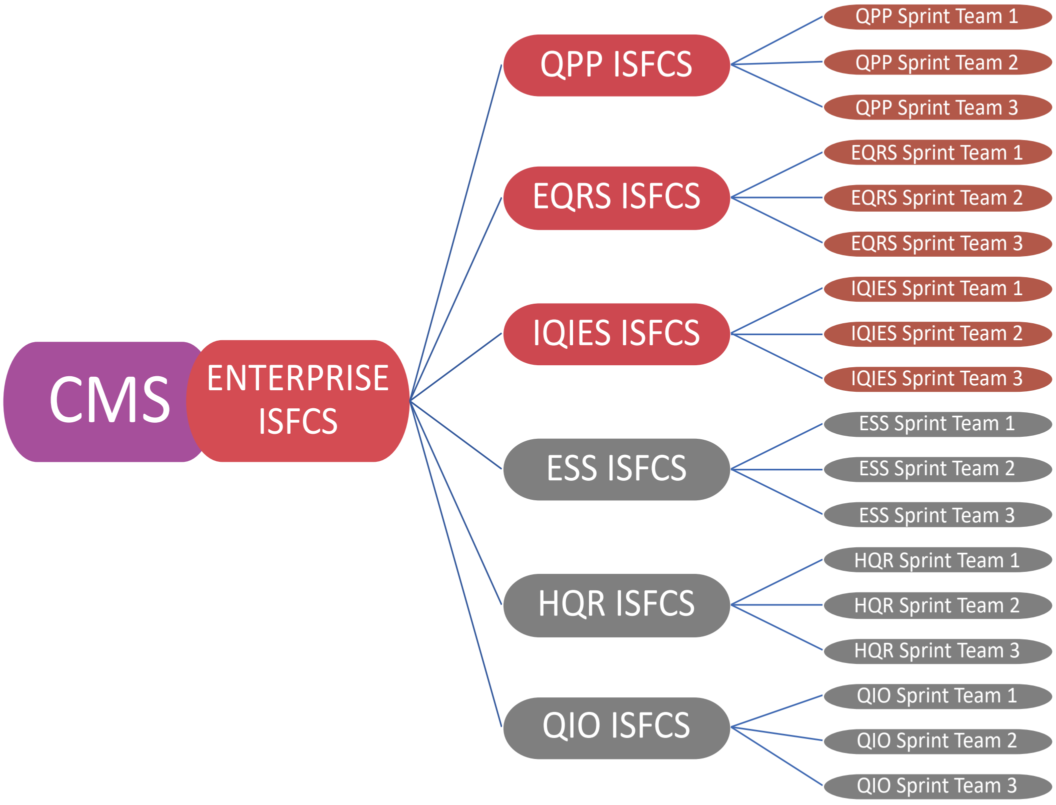
Appendix A: Example ISFCS Embedded Liaison Concept

This diagram provides the current work structure of the FC team:



Appendix B: ISFCS Team Concept for ISG Enterprise

This diagram is a concept of overall ISFCS team support for ISG LOBs. At this time, CMS is not requesting FC support for <u>ALL</u> LOBs shown in the diagram, only support for QPP, EQRS, and QIO.



Appendix C: Example Path to Prod Checklist

Checklist for including production data with PII in your environments, and for peering Impl and Prod with environments containing production data. For evidence, please link to the relevant confluence documentation, GitHub, Splunk, New Relic pages, etc.

	Area	Description
1	AWS	A list of all in-use, and proposed to use AWS services has been created. Only FedRAMPed or CMS Risk Accepted systems are used and with approved data (i.e. only systems approved for PII/PHI have that data).
2	Code Quality	All software must be maintained on GitHub, either at github.cms.gov or github.com/cmsgov
3	Code Quality	All deployed code has undergone and continuous to undergo static code analysis, unit testing, peer review before merging. Static Code Tool Examples: SonarQube - Node.js and Java (and others) Pylint, Pep8 - Python
4	Code Quality	All deployed code has undergone continuous integration.
5	Configuration as code	All deployment infrastructure code has meets the Code Quality item as well.
6	Configuration as code	All server configuration and deployment **must** be automated.
7	API Standards	All APIs follow the QPP RESTful API style guide
8	API Standards	All APIs has their endpoint request and responses documented in OpenAPI/Swagger
9	DevOps Response Plan	DevOps response plan has been documented on Confluence
10	Logging	Application and Server data for Impl and Prod environments is in Splunk
11	Logging	All additional background services or PaaS (e.g. RDS, ELB, DYnamoDB) have log data for impl and prod environments are in Splunk.
12	Logging	PII (including email addresses and user names) and PHI is not part of any application or request logging.
13	Monitoring	APM and Server (infrastructure) New Relic configuration are setup for any running services.

	Area	Description
14	Monitoring	All additional background services or PaaS (e.g. RDS, ELB, DynamoDB) are in New Relic. As an alternative, CloudWatch can be used if all relevant teams have access to the AWS account with those metrics.
15	Monitoring	All relevant monitoring links for the service have been added to the QPP Monitoring.
16	Alerting	PagerDuty or similar is configured
17	Alerting	A single alerting event has been triggered and the DevOps Response Plan exercised
18	Alerting	Splunk alert configured to fire when log data is missing. For example, if a host typically gets a health check every 1 minute that should appear in logs, then fire an alert if there hasn't been a log from that host for more than 15 minutes.
19	Security	Application codebase has been audited for database passwords, API secrets, etc.
20	Security	Handling of sensitive data, including any encryption scheme, has been documented and reviewed.
21	Security	Secrets and credential management has been documented and reviewed.
22	Security	AWS Trusted Advisor has no open issues (unless known and documented)
23	Security	Nessus Scans have been performed. No Critical, High, or Medium issues
24	Security	A list of all users with root access (or where to find the list in config-as- code)
25	Compliance	Architecture is covered by the QPP ATO (documented in CFACTS, SIA performed for any new services)
26	Compliance	Perform the Production Readiness Review (review of this document)

Appendix D: Example Threat Modeling Process

1. System selection - Identify parts of the system we need to threat model via brainstorming sessions with Program stakeholders and scenarios that come up in the development process. This list should include:
   - Key assets that need to be protected
   - Where the above assets live and who has access to them
   - Potential attackers and their motivations
2. Threat model pre-planning - For each part of the system, meet with relevant product owner, systems architect and scrum master to do the following:
   - Draw out system diagram
   - Answer these questions:
     - What assets are we protecting?
     - What is the system scope?
     - Who are our attackers?
3. Threat model session - Meet with larger group, including pre-planning group and people most knowledgeable about system's hosting/network infrastructure, to do a threat model. Example agenda:
   - Group to discuss system diagram and iterate/fill in gaps if necessary
   - Walk group through each part of the system and identify specific threats within that part of the system
   - Capture and summarize threats with notes on severity and attacker capabilities (see example below)
4. Mitigation
   - Prioritize mitigations for system
   - Work with product owner, system architect and scrum master on timeline for mitigations and how they would fit into milestones/existing work
   - Measure progress towards mitigation