Attachment 1

Information Security and Privacy Support Services

Statement of Work

Version 1.0

Contract# TBD

May 23, 2016

Table of Contents

1 Scope

1.1 Background

The Centers for Medicare & Medicaid Services (CMS) is part of the Department of Health and Human Services (HHS) and is the agency with the goal to cover millions of eligible people for enrollment in Medicare, Medicaid, the Children's Health Insurance Program (CHIP) or in a qualified health plan through the Health Insurance Marketplace. Another goal of the agency is to achieve a high quality health care system with the aim for better care at lower costs and improved health. In this capacity, CMS is responsible for payment of over $900 billion each year for medical services rendered to the nearly 100 million program beneficiaries and recipients. CMS has a central site in Baltimore and ten (10) regional offices in major cities throughout the country. CMS contracts with approximately 33 companies to process claims for reimbursement for medical services rendered under the Medicare program and the agency works with all states, the District of Columbia, and the U.S. territories as the focal point for all national program policies and operations related to Medicaid, CHIP, and the Basic Health Program (BHP).

In the administration of these programs, CMS utilizes many assets, including buildings, facilities, communications equipment, computer systems, employees, contractors, public trust, and information. A loss to any one of these assets could affect the goals or the quality of support necessary from CMS to its various customers and stakeholders.. Additionally, CMS collects, uses, and stores information that falls into the categories of privacy data, Protected Health Information (PHI), proprietary data, procurement data, inter-agency data, and privileged system information. Access to these types of information is controlled by the Privacy Act of 1974 (as amended), the Computer Security Act of 1987 (as amended), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Information Security Management Act (FISMA) of 2002, as well as many important rules, regulations, policies, and guidelines promulgated by HHS, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). As a result, CMS has a legal and practical responsibility to maintain the confidentiality, integrity, and availability (CIA) of this information.

CMS, like many organizations, faces significant challenges in managing agency risk across its dynamic mission and its large array of networks and information systems. Information assets have become increasingly difficult to protect due to advances in the threat landscape, such as easy-to-use cyber-attack frameworks, advanced threat actor persistence and technologic attack evolution, data obfuscation, and social engineering such as phishing attacks. These factors have resulted in a critical necessity for utilizing an innovative and forward thinking implementation of security at the agency. Through innovative advances in the implementation of security, inclusion of security requirements throughout the system and software development life-cycle, and the continuous monitoring and ongoing authorization program, the agency effectively manages risk through an optimal security posture, and thus protects the confidentiality, integrity, and ensures the availability (CIA)

of CMS information. Every day CMS has the responsibility to track and report on cyber activity at nearly 50 data centers / sites.
CMS is responsible for collecting, generating, storing, and therefore protecting personal, financial, healthcare, and other sensitive information. Much of this information relates to the healthcare provided to the nation's Medicare and Medicaid beneficiaries and has access restrictions required by legislative and regulatory directives. CMS is responsible for ensuring the CIA of this information, regardless of how it is created, distributed, or stored.

Furthermore, the CMS general support system (GSS) and applications supporting the Affordable Care Act (ACA), Health Insurance Marketplace will be accessed by more than thirty-five million individuals in a given year, and provides data exchange services to a variety of state governments, issuers, agents / brokers, assistors, and provides back end connections and data transformation services to many federal agencies. Distributed across 4 data centers and supported by a multitude of both contractor and federal personnel, the infrastructure supporting the Heath Insurance Marketplace program is a highly complex, dispersed and interdependent environment.

To safeguard the CIA of its information and information systems effectively, CMS has established an enterprise-wide Information Security and Privacy program under the Information Security and Privacy Group (ISPG). The Information Security and Privacy Group, charged with protecting CMS data, "*provides leadership to CMS in managing information security and privacy risks appropriate for evolving cyber threats*". ISPG executes this vision utilizing an innovative approach to provide optimal visibility, situational awareness, resilience and incident response readiness across all CMS FISMA Systems.

The ISPG Security and Privacy program is responsible for defining policy, providing security and privacy services, and leading compliance and oversight of the program. The ISPG is comprised of 3 divisions: Division of Security and Privacy Compliance (DSPC), Division of Cyber Threat and Security Operations (DCTSO) and the Division of Security, Privacy Policy and Governance (DSPPG); and supported by the Front Office. The following table states the responsibilities for each division.

Division	Responsibilities
Security, Privacy Policy and Governance	Establish security and privacy policy consistent with federal and HHS requirements and guidance. Ensure alignment of security and privacy policy with enterprise efforts in system develop lifecycle, enterprise architecture, and Federal IT Acquisition Reform Act (FITARA).

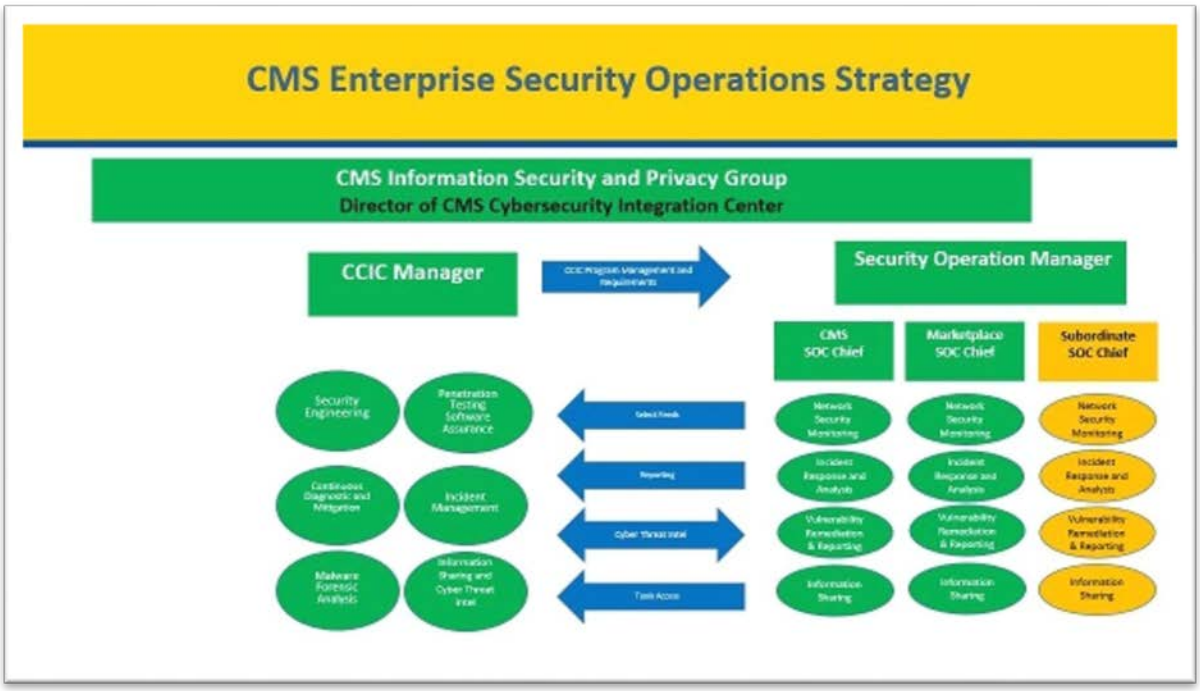
Division	Responsibilities
Security and Privacy Compliance	Manage the cybersecurity and privacy risk across CMS Centers and Offices for known security weaknesses and emerging cyber threats. Implement and manage the security authorization process (formerly called certification and accreditation) and develop a strategy and process to transition to a Continuous Diagnostic and Monitoring model to include Ongoing Authorization consistent with OMB and NIST guidance.
Cyber Threat and Security Operations	Mature the CMS Cybersecurity Integration Center (CCIC) to serve as a centralized focal point for incident response and oversight of all security operations centers servicing CMS. Mature cyber threat intelligence program into a comprehensive view of risk across CMS to include our federal, state, and commercial partners.

Table 1 - CMS ISPG Division Areas

ISPG works in close collaboration with contractor support and looks to this support not only to provide subject matter expertise and thought leadership, but also to take ownership of responsible work, manage quality, and provide the government with deliverables that are finished products ready to be delivered to senior management or ISPG customers across the agency. “Finished Products” are concise, relevant, well-formed and professional in appearance with content checked for accuracy and adherence to objectives through a contractor-managed quality control process.

The successful implementation of security and privacy controls to protect all information assets requires not only alignment with federal legislation, mandates, and executive orders, but also a collaborative approach between ISPG and all CMS FISMA system stakeholders. This interoperability is accomplished through close collaboration between roles such as the ISPG Cyber Risk Advisor (CRA), Data Guardian (DG), and system Information System Security Officers (ISSOs). The CRA is charged with bridging the security operations and compliance requirements with business objectives. The Data Guardian is a resource within the business units that coordinates program activities to protect consumer data, ensure open lines of communication between the offices of the CIO and CISO, and promotes the protection of agency assets. This enhanced and collaborative approach to the execution of the security and privacy functions has allowed ISPG to establish the goal and create a strategy to implement a methodology for Continuous Diagnostics and Mitigation (CDM) along with Ongoing Authorization (OA).

As a part of the new security paradigm at CMS, the Information Security and Privacy Group which was established in December 2014, consolidated information security and privacy-related operational capabilities, including incident response and security operations, relative to the historical organization of these activities within the Office of Technology Solutions (OTS) or the Office of Enterprise Management. This centralized model realizes efficiencies through easier coordination, standardization, and management. A critical component of this functionality aggregation is the CMS Cybersecurity Integration Center (CCIC). CCIC is the central point of Cybersecurity situational awareness and management across the agency and all FISMA systems. CCIC provides services, expertise and innovation in the areas of Penetration Testing, Software Assurance, Security Architecture and Engineering, Continuous Diagnostics and Mitigation, Incident Management, Malware & Forensic Analysis, Advance Threat Hunting, Information Sharing and Cyber Threat Intelligence. ISPG federal employee and contractor information security and privacy professionals implement and manage these services to maintain an optimal agency cybersecurity posture. The figure below provides a high-level depiction of the organizational structure of the CCIC described above:



The following provides the organizational structure with associated services:

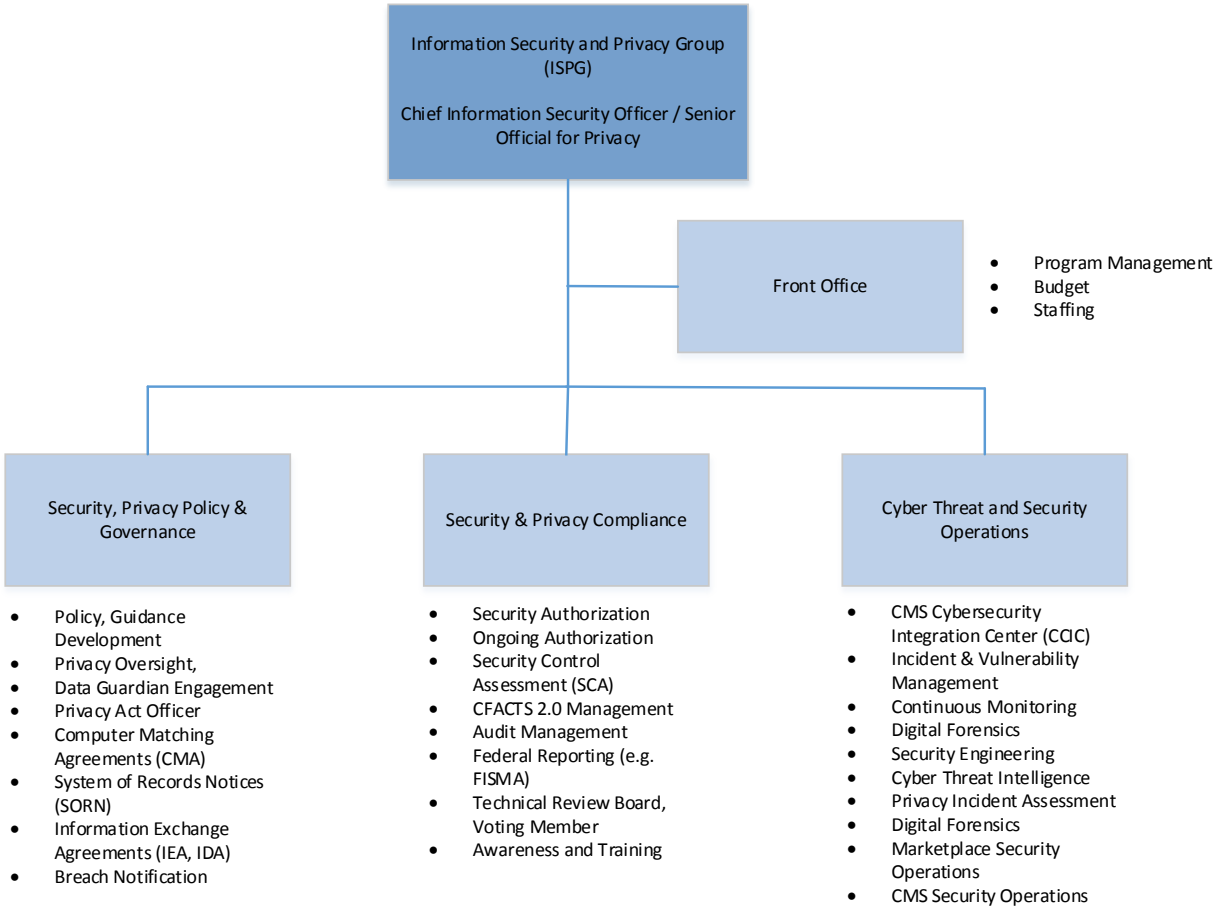


Figure 1 - ISPG Program Services

1.2 Purpose

This Statement of Work (SOW) describes a broad set of contractor responsibilities to support the Information Security and Privacy program activities under ISPG. The principal purpose of these responsibilities is to provide comprehensive expert cybersecurity support to the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) to:

- Provide Information Security and Privacy Program Management Support
- Ensure Information Security and Privacy Documentation is accurate, current, and relevant to CMS
- Develop and provide training and outreach regarding security and privacy to CMS employees
- Effectively manage agency risk by maintaining visibility across the agency, and verifying Incident Response readiness for all CMS FISMA systems
- Maintain comprehensive situational awareness of the cyber threat landscape as it relates to the CMS lines of business in support of the healthcare sector
- Maintain vigilance and routinely test incident response readiness
- Reduce cost and optimize agency Security Posture through complexity reduction and automation
- Deliver measurable Information Security and Privacy
- Define and/or improve CMS's Information Security and Privacy Shared Services Framework
- Effectively communicate with all parties, especially key stakeholders
- Improve Regulatory & Policy Alignment

2 Requirements

2.1 Task Areas

The Contractor shall perform tasks in the following areas:

1. Program, Project, and Task Management
2. Information Security and Privacy Program Support
3. Information Security and Privacy Subject Matter Expertise Technical Advisory Services
4. Information Security and Privacy Awareness and Training
5. Audit and Risk Management
6. CMS Cybersecurity Integration Center (CCIC)
7. CMS Security Operations Center
8. CMS Health Insurance Marketplace Security Operations Center

2.1.1 Task Area 1: Program, Project, and Task Management

The Contractor shall name a program manager (PM) to serve as the Government's single focal point. The PM shall have responsibility for the planning, execution, control, and direction of prime contractor employees' and any subcontractors' programmatic and technical work performed under this task order. The Contractor shall effectively and efficiently manage cost, schedule, and performance using integrated program management processes across all aspects of performance and in a manner that yields cost savings and/or performance efficiencies.

The PM shall assure that the necessary controls for work described herein are appropriately supplied using program plans, program oversight, and reporting. The PM shall have the necessary authority to utilize the company's resources to assure the work under this task order is accomplished consistent with technical, cost, and schedule requirements as well as prudent programmatic and technical risk mitigation. The PM is responsible for designing and implementation of plans of action to ensure control and direction of contractor personnel is performed by management personnel of the Contractor, rather than the Government, and thus avoiding the delivery of personal services.

The Contractor shall provide information security and privacy program management, project management task management, reporting, and issue/risk management to ensure the success of projects and to align project activities to CMS's overall Information Security & Privacy program goals.

Contractor program and project management and task management activities include, but are not limited to:

a. Follow project management best practices and perform project management activities for each task, including the following as needed: integration management, scope management, time management, cost management, quality management, resources management, communications management, risk management, and transition planning
b. Create and maintain project documentation for each task, including the following as needed: project charters, project management plans, project schedules, work breakdown structures, risk registers, lessons learned, requirements documents, meeting agendas, meeting minutes, action items, workflow diagrams, and others
c. A Transition-In and Readiness Test Plan for Marketplace Open Enrollment FY17
d. An integrated master project schedule of all task areas, dependencies and resource names
e. Proactively track and follow up on deliverables and sub-tasks for each task
f. Attend and organize regular status meetings with ISPG management and team members
g. Develop weekly Situational Reports (SITREP) and monthly status reports

Program Management:

The Contractor's program practices shall stress continuous and open communication with CMS, CMS's partnering contractors, and other stakeholders. Coordination and communication between the Contractor and CMS shall be conducted on both a formal and informal basis. Formal and informal liaison and coordination activities at the program level shall have performance issues as their main focus. Day-to-day interaction is typically required. Communications shall be conducted by telephone, email, reports, memoranda, and face-to-face interactions as necessary to conduct business in an efficient and effective manner.

The PM, and where needed other appropriate contractor personnel, shall participate in routine and periodic status meetings with key government personnel, at times on short notice. The purpose of such meetings is to ensure CMS stakeholders are informed of program status and progress on activities. The meetings provide an opportunity to set priorities, identify opportunities or concerns, and coordinate resolution of identified problems.

Utilizing an industry standard framework and methodology, the Contractor shall perform all program management functions. These functions, include but are not limited to, technical, business, risk and issue management functions that are necessary to execute the total effort required by this task order. The Contractor shall provide all personnel and other resources, except as otherwise specified in this task order, necessary to accomplish these functions. The Contractor shall affect these management functions through an integrated management approach, including cost, schedule, and technical performance. Consistent and meaningful communication between the Contractor and CMS is paramount at all levels from management down to government staff.

Assumptions, Service Level Agreements (SLAs), and Operating Constraints:

1. CMS expects that all program/project managers will have extensive project management experience of 7 or more years, managing projects of comparable scale and complexity to those described herein. PMP certification or equivalent is also required.

2.1.2 Task Area 2: Information Security and Privacy Program Support

2.1.2.1 Information Security and Privacy Program Management Support

The Contractor shall provide information security and privacy program support to CMS employees and contractors on the application of information security and privacy specific to business and technical situations and settings.

The Contractor shall be required to provide information security and privacy program support services, including, but not limited to the following:

a. Determine the impact of new technology or policy (e.g., CDM technologies, anomaly based tools, virtual environments, etc.) on the CMS information security and privacy program
b. Where requested, conduct meetings, including preparing, documenting, and recording minutes
c. Provide expert analysis and document preparation for various analytical efforts focused on processes and procedures
d. Review various draft documents and provide timely feedback to CMS employees and contractors
e. Develop and implement information security and privacy program strategic and tactical goals and objectives
f. Develop and implement information security and privacy program outreach and communication plans
g. Identify and develop a Performance Management program that includes performance measures, tracking metrics, and trend analysis
h. Generate regular and ad hoc dashboards, reports, and metrics
i. Recommend, develop, and maintain monthly, quarterly, and annual FISMA reporting documents in CMS's required format
j. Attend FISMA Working Group Meetings
k. Assist in researching FISMA Reporting Data Centers and Reporting Points of Contact
l. Support and prepare letters for submission such as:
    A. CISO Letter
    B. Administrator Letter (Annual)
    C. Cover Letter (Annual)
    D. Red Folder signature Page
    E. Reporting template
m. Using a CMS provided enterprise Governance, Risk, and Compliance (eGRC) tool, maintain a CMS FISMA inventory and Plan of Action & Milestone (POA&M) report in CMS's required format
n. Using a CMS provided eGRC tool, maintain a tracking system of all ISPG information security and privacy -related deliverables— regularly scheduled and ad hoc
o. Maintain the RSA Archer Platform (O&M-ApplicationAdministration)
p. Publish required information to the CDM dashboards
q. Assist the ISPG with transforming the organization and governance structure to support CMS information security and privacy initiatives
r. Assist the ISPG with transforming the processes for inquiries, Expedited Life Cycle (XLC) reviews and risk assessments
s. Assist ISPG to ensure roles and processes of Federal Information Technology Acquisition Reform Act (FITARA) are properly adhered to
t. Prepare responses to federal ad hoc reporting requirements
u. Update project charters, and project management plans yearly as required.
v. Update integrated master project schedule of all task areas, WBS, risk register, lessons learned.

w. Prepare meeting agenda's, minutes, diagrams as required.
x. Prepare FISMA Reporting documents quarterly and annually.
y. Report on FISMA Inventory and provide POA&M reports monthly.

2.1.2.2 Information Security and Privacy Policy and Documentation Support

The CMS Information Security website (http://www.cms.gov/InformationSecurity/) provides agency employees and contractors a virtual library of applicable security and privacy policies, procedures, guidelines, tools, directives, and templates. Security requirements are dynamic and must be updated routinely.

The Contractor, with ISPG direction, shall proactively review, update, and maintain information security policy, guidance documents, directives, templates, and materials to ensure all documentation reflects and incorporates the most recent version of all CMS information security and privacy program documentation.

The Contractor, with ISPG direction, shall provide Information Security and Privacy requirements and guidance, including, but not limited to the following:

a. Inventory existing Information Security and Privacy policies, handbooks, standards and procedures and recommend disposition (i.e. continued use as is , needs revision, or deactivate)
b. Recommend, review and update existing, and/or develop new Information Security and Privacy policies, handbooks, standards, and procedures
    i. Ensure documentation is current and relevant for CMS processes and programs
    ii. Ensure alignment with of security and privacy policy with agency programs like system development lifecycle, enterprise architecture, and FITARA
c. Routinely update, revise, and modify the CMS Acceptable Risk Safeguards (ARS)
    i. These updates shall be based upon research, investigation, and analysis of changes in federal, departmental, and CMS-specific policy, regulations, and mandates
    ii. Ensure documentation is current and relevant for CMS processes and programs
d. Incorporate new CMS policies, procedures, and controls into the agencies eGRC tool (RSA Archer)
e. Draft, review, and/or comment on Chief Information Officer (CIO) and CISO directives and other policies, procedures, and correspondence

f. Provide documentation and comprehensive system security planning and lifecycle management

g. Produce documentation, which includes security documentation, expedited lifecycle documentation, user manuals, training material, standard operating procedures (SOP), network diagrams, system-level security requirements, security specifications, and metrics for product/system testing evaluation and assessment.

h. Perform inventory review and update plan with schedule monthly

i. Routine updates to CFACTS, BPSSM, ARS and other noted ISPG documents as required

j. Delivery of ATO packages review packages to CISO and CIO as required.

Assumptions, SLAs, and Operating Constraints:

1. The Contractor shall receive approval from CMS before any documents are made public or sent through the approval process for posting on the CMS Information Security Library website.
2. The Contractor shall make sure any documents or updates to documents have gone through a quality control check for accuracy and appearance, including correction of spelling, grammar, and formatting errors, before submission to CMS.
3. The Contractor and ISPG shall agree on a timeframe for preparing, reviewing, and approving documents or updates to documents. This timeframe will be determined by the size, complexity, and breadth of the assignment.

2.1.2.3 ISPG E-Mail Support Services

The Contractor shall provide information support for CMS employees and contractors to obtain assistance with questions/problems concerning CMS information security and privacy standards, policies, procedures, Assessment and Authorization (A&A) artifacts, and any other security-related deliverables CMS requires of its contractors as documented and required on the CMS Information Security Library http://www.cms.gov/InformationSecurity.

Inquiries as received via the CISO mailbox at ciso@cms[.]hhs[.]gov, and Senior Official for Privacy mailbox at privacy@cms[.]hhs[.]gov, and PIA@cms[.]hhs[.]gov Support hours for the mailboxes are 9:00AM to 5:00PM Monday – Friday. For calendar year 2015 the CISO Mailbox received an average of 1,255 actionable emails per month; the privacy mailboxes received low volumes.

The Contractor shall provide an automatic response to the sender confirming receipt of the inquiry. Initial responses to inquiries shall be provided within a 24-hour period during business days. The Contractor shall prepare a monthly mailbox report that includes, at a minimum, metrics such as average monthly emails, and major categories of inquiries. The

Contractor shall not include emails in the monthly report that did not require a response. For example, the CISO mailbox is regularly copied on correspondence that is then archived without requiring any action from the support team.

The Contractor shall provide CISO communications support services, including, but not limited to the following:

a. Identify the processes for inquiries and make recommendations for process improvements
b. Respond to inquiries
c. Direct inquiries to the proper ISPG resource when necessary
d. Track and document responses to resolution
e. Manage and measure the effectiveness of the support function
f. Maintain a repository of frequently asked questions (FAQ) and ISPG subject matter experts (SMEs)
g. Provide explanation of the applicability of information security requirements to CMS employees and contractors
h. Provide technical assistance to CMS employees and contractors on usage and functionality questions related to the eGRC application
i. Provide technical assistance to CMS employees and contractors on application of the information security requirements to specific business and technical situations and settings
j. Provide subject matter advice to CMS employees and contractors on security and privacy artifact development and methodology questions as documented and required on the CMS Information Security and Privacy Library
k. Create and send e-mail broadcast messages as required
l. Update FAQ document monthly

Assumptions, SLAs, and Operating Constraints:

1. Provide final response to requestor in 5 business days, unless approved by ISPG employee.
2. Messages shall be professional in nature, and generally free of spelling and formatting errors.
3. Strong written and verbal communication skills are required for this task.

2.1.3 Task Area 3: Information Security and Privacy Subject Matter Expertise Technical Advisory Services

2.1.3.1 Assessment and Authorization (A&A) Subject Matter Expert Support

a. The Contractor shall provide overall subject matter expertise to the Information Security Assessment and Authorization (A&A) program program that currently comprises over 200 FISMA systems of varying size and complexity. Provide specific guidance and technical expertise in the form of standards, policies, procedures, and oversight for the CMS A&A program
b. Review and provide advice based on analysis for Privacy Impact Assessments (PIA)
c. Review and provide advice based on analysis for Third Party Website and Applications (TPWA)
d. Review and analyze all system artifacts for accuracy, completeness, in support of an authorization to operate (ATO) requests
e. Create or Review ATO packages prior to submission to CISO and CIO approval
f. Ensure all assessment and audit reports are uploaded properly to the CMS FISMA Controls Tracking System (CFACTS)
g. Conduct audits of closed Plan of Actions and Milestones (POA&M) for completeness and compliance
h. Develop and support the ongoing authorization (OA) process that includes continuous monitoring
i. Provide document development support for CISO sponsored events and responses to questions and concerns
j. Draft document review and feedback on application of security and privacy requirements (eg. TRB, review of SSPs, RA's, contingency plan, POA&M reports).

Assumptions, SLAs, and Operating Constraints:

A&A SME shall have 5 years or more experience actively working with the NIST 800 Series, and hold at least one professional security certification related to subject. Individual also must have experience working with the Privacy Act, and possess a working knowledge of HIPAA, and associated artifacts required by privacy officers.

2.1.3.2 Ad Hoc Security and Privacy Engineering Subject Matter Expert Services

CMS will require expertise in specific security or security-related engineering topics and privacy engineering, as necessary.

The Contractor Security Engineering SME expertise may include, but is not limited to, the following types of ad hoc activities, which could occur several times a month:

a. Prepare situational awareness briefings regarding information security policy and contractor and developer trends for CMS and HHS senior management
b. Develop alternatives of system designs and/or architectures which consider trade-offs between security requirements, functional/operational requirements and cost.
c. Determine the impact of new or changing applicable federal policy changes
d. Determine the impact of new or revised legislation and regulations (OMB, HIPAA, FISCAM, etc.)

e. Provide security engineering subject matter expertise in coordination with Enterprise Architecture and Technical Review Board to conduct technical review board program planning reviews related to future enterprise architecture updates and proposed information security mechanisms
    i. Support will be technology-related architecture guidance delivered in the form of PowerPoint briefings, email, or white papers addressing information security architecture vulnerabilities, risks, mitigation response, and emerging opportunities.
f. Conduct research and present analyses to evaluate and/or determine emerging industry technology trends, government agency best practices, and security issues:
    i. Contractor deliverables shall be in the form of white papers or development of PowerPoint briefing documentation as appropriate to the scope of the research, required analysis, and CMS method of dissemination and distribution.
    ii. The Contractor may be required to provide strategic thought leadership and verbal briefings related to security engineering risk identification and mitigation and emerging industry issues and best practices.
    iii. The Contractor shall be required to deliver written guidance or assessments in the form of short briefings, written documents, or presentations.

The Contractor Privacy Engineering SME expertise may include, but is not limited to, the following types of ad hoc activities, which could occur several times a month:

a. The Privacy Engineer is responsible for ensuring that privacy is an integral part of the very beginning phases of system design to support the mitigation of privacy risk from the processing of personally identifiable information (PII) within systems.

b. Privacy engineering objectives are designed to enable system designers and engineers to build or select technologies that are capable of implementing CMS's privacy goals and supporting the management of privacy risk. The Privacy Engineer should ensure all CMS systems exhibit privacy engineering objectives to be considered a system that could enable privacy protections while achieving its functional purpose.

c. The Privacy Engineer should understand technology and be able to integrate perspectives that span design, development, cyber security, business, and legal considerations. Functions can include:
    i. Participating in the development of privacy relevant policy and controls to ensure technical privacy is built into system engineering guidance
    ii. Integrating privacy into the CMS XLC by providing guidance on addressing privacy in systems documentation and other system development artifacts

iii. Assisting business owners and system engineers with selecting and implementing controls that protect privacy

iv. Participating in XLC gate reviews to ensure designers and developers are appropriately designing, developing, and deploying privacy protections into their systems.

Assumptions, SLAs, and Operating Constraints:

1. The Contractor shall receive approval from CMS before any documents are made public or sent through the approval process for posting on the CMS Information Security Library website.
2. The Contractor shall ensure that any documents or updates to documents undergo a quality control check for spelling, grammar, and formatting errors before submission to CMS.
3. ISPG shall determine a reasonable timeframe for preparing, reviewing, and approving documents or updates to documents. This timeframe will be determined by the size, complexity, and breadth of the assignment.

2.1.4 Task Area 4: Information Security and Privacy Awareness Training

CMS requires subject matter expert support for the development, delivery and maintenance of a comprehensive information security and privacy awareness and training program. This program will include, but is not limited to, providing support in the following areas:

a. Assess and provide recommendations of the existing training program and materials
b. Develop, deliver and maintain outreach and marketing strategy for security and privacy
c. Engage with the ISSO community to communicate changes to ISPG programs
d. Enhance, document, administer, and deliver a comprehensive program to measure and improve the information security and privacy awareness and vigilance of CMS system users, including those with significant security responsibilities
e. Develop and implement reporting and tracking processes for information security and privacy awareness and role-based information security training
f. Provide information security and privacy training (classroom, web-based, and other methods) across the gamut of information security and privacy areas, including CMS security and privacy specific topics and recent industry trends
g. Provide support to the development, implementation, and tracking of role-based information security and privacy training

Troubleshoot and provide solutions to issues with information security and privacy training software

h. Provide support to the coordination of training seminars, training meetings, conferences, etc.

Material developed for training may be in the form of, but are not limited to, audio, visual, computer-based, Web-based, or written media as directed by CMS. The Contractor may be required to provide instructors to present any of the material developed in the form of (but not limited to) classroom instruction, small group discussions, briefings, etc., as directed by CMS. The ability to allow courses to be captured electronically for use by personnel who cannot attend the training in person should be available. In addition, the Contractor shall develop and provide courses in other formats, including (but not limited to) webinars, avatar, PowerPoint presentations, etc. CMS will determine the distribution of the type of training to be provided with input from the Contractor.

The Contractor shall develop the following material for each class:

a. For classroom training:
    i. Student handout that contains a copy of the course briefing and/or other supporting material
    ii. A copy of the course briefing and/or other supporting material archived to CMS SharePoint training folder
b. For all courses:
    i. Course evaluation to be completed by each individual attending the class.
    ii. Certificate of Attendance to be awarded to each individual completing the class.
    iii. Proficiency examination that will be administered by the Contractor at the conclusion of each class, if warranted by the content.
    iv. Certificate of Accomplishment for individuals successfully completing the examination. If appropriate, this certificate may be in the form of a Committee for National Security Systems (CNSS) or other Government-recognized certification.
    v. Electronic copy (e.g., Acrobat file) of the scanned image of the completed course evaluations
    vi. Attendance file for upload to CMS Computer Based Training System (CBT) to record attendance.
    vii. Trainings are made Section 508 compliant.

In addition to training, the Contractor shall develop and execute an outreach and marketing campaign in order for integration of ISPG services by CMS programs. The Contractor shall develop a strategy. Once the government approves the strategy, the Contractor shall execute the strategy. Additionally, the Contractor shall develop all materials to include

brochures and slick sheets. The Contractor shall also conduct outreach activities such as brown bags and displays.

Assumptions, SLAs, and Operating Constraints:

1. All system software must be developed using CMS standard application development tools, including Visual Studio, SQL Server, and Adobe development tools.
2. Classroom training and outreach will be conducted at the CMS Single Site, in Baltimore, MD. Attendees could be remote and the Contractor may need to work across US timezones.
3. All meetings shall take place at the CMS Single Site, in Baltimore MD.
4. The Government shall provide the room/space for all meetings.
5. Training shall be all-encompassing (including the cost of all course material and assembly).
6. The Contractor shall make sure any documents or updates to documents have gone through a quality control check for spelling, grammar, and formatting errors before submission to CMS.
7. On average during calendar year 2015 the Contractor conducted 2 - 3 in person classes per month and 2 remote classes per month. Examples include: Cybersecurity Essentials, Risk Management, Contingency Planning and Assessment & Authorization.
8. The Contractor shall conduct brown bag seminars on various ISPG topics on a monthly basis
9. Training team must maintain an average feedback rating at or above 8.5 out of 10 on Course Evaluation forms.
10. Trainer must have at least 5-years' experience developing and providing training.

2.1.5 **Task Area 5: Audit Management**

CMS requires subject matter expertise and audit management support for involvement in the development and maintenance of an Audit and Risk Management program.

The ISPG facilitates audits for various reason to include requests from The Government Accountability Office, Statement on Standards for Attestation Engagements (SSAE), CMS Section 912 audit, FISMA compliance, Office of Management and Budget Circular A-123 Management's Responsibility for Internal Controls, and Audits, Chief Financial Officer (CFO) audits, Internal Revenue Service (IRS) audits, and Office of Inspector General (OIG) audits.

Th e Contractor will provide support to include, but is not limited to, providing support in the following areas:

a. Maintain an audit request and response database that is accessible by multiple stakeholders
b. Support the Audit Liaison in research, gathering information, and submitting audit artifacts
c. Support the Audit Liaison in research and writing audit responses
d. Maintain a findings list and follow the findings through remediation and closure
e. Manage each audit engagement in collaboration with all stakeholders
f. Assist with creating finding spreadsheets based upon audit reports, for upload to CFACTS
g. Assist with managing and maintaining visibility of plans of action and milestones (POA&M) to achieve acceptable levels of risk
h. Maintenance of metrics to show progress of audit.
i. Report on audit and risk as required,
j. Meet due dates and deadlines for audit work and responsibilities.

Assumptions, SLAs, and Operating Constraints:

1. The Contractor and ISPG shall agree on a timeframe for preparing, reviewing, and approving documents or updates to documents. This timeframe will be determined by the size, complexity, and breadth of the assignment.
2. The Contractor should receive government approval prior to contacting any stakeholders external to ISPG for data collection or other information.
3. The Contractor must provide draft documents as agreed upon by the PM and COR; the final report is due 5 days after receiving government input on a draft report.

2.1.6 Task Area 6: CMS Cybersecurity Integration Center

The CMS Cybersecurity Integration Center (CCIC) is comprised of 6 functional areas and is responsible for maintaining comprehensive situational awareness, visibility, and response readiness across the CMS enterprise. The six functional areas are as follows: Security Engineering, Continuous Diagnostics and Mitigation, Forensics and Malware Analysis, Cyber Threat Intelligence, Penetration Testing, and Incident Management. The CCIC works closely with the CMS and Marketplace Security Operations Centers to perform the function of operational security for the Agency. The Contractor will be required to provide staffing towards the CCIC. The CCIC is currently in Woodlawn Maryland, just a few miles from CMS Central Office.

The CMS Cybersecurity Integration Center collaborates with approximately 33 different external contractors/partners at approximately 50 distributed data center sites that support over 200 FISMA-reportable systems. Each of our external contractors/partners manages a local SOC with an incident response team (IRT). The CMS Cybersecurity Integration Center synthesizes data from each of these 33 contractors/partners for oversight monitoring by the CMS SOC. CMS requires on-site support for the Cybersecurity Integration Center and the CMS SOC to integrate and monitor the systems and technologies, including the activities that relate to managing the security operations and incident response coordination with these external partners.
The Contractor shall provide, but is not limited to providing, the following services:

2.1.6.1 Penetration Testing

a) The CCIC Penetration Testing Team coordinates and conducts all Agency penetration testing on systems operated by and on behalf of CMS. Using a documented test plan and methodology identified in the CCIC Penetration Testing CONOPS, the team utilizes a variety of CMS approved tools to conduct vulnerability assessments and penetration tests for all CMS FISMA systems [approximately 300 unique tests per year are conducted including development of the test plan, testing, and providing test results]; volume of tests are expected to grow by 25% year over year.
b) PenTesting team will develop and follow a testing schedule that includes flexibility to conduct ad hoc tests upon request
c) The team shall be required to brief or explain to ISPG staff, CMS Leadership, and other stakeholders the results of penetration testing activities.
d) Simulate internal lateral movement activities observed in successful attacks from known adversaries
e) Identify security deficiencies and determine the efficacy of security controls design and implementation;
f) Provide advisement on countermeasures to mitigate threats;
g) Provide a basis for evaluating the effectiveness of proposed or implemented security measures;
h) Provide vulnerability to exploit mapping;
i) Perform FISMA System post-implementation security posture determination;
j) Provide penetration testing services in support of the CMS Continuous Diagnostic and Mitigation process;
k) Integrate penetration testing activities with other testing efforts, including but not limited to, vulnerability assessments, threat modeling, event detection evaluation, continuous monitoring tool verification, incident response, and incident reporting compliance;
l) Threat modeling utilizing intelligence from CCIC Cyberthreat Intelligence team.Develop Enterprise Penetration Testing Plan and Schedule.
m) Develop, maintain and update Penetration Testing Concept of Operations and Standard Operating procedures.

n) Draft CMS Rules of Engagement and Test Specific, Penetration Documents for engagements.
o) Prepare Test Plan, Draft Report and Final Report
p) Maintain overall tracker of Penetration Testing activities.
q)

2.1.6.2 Forensics, Malware Analysis and Advanced Hunting

a) The CMS CCIC Forensics and Malware Analysis Team provides network and media digital forensics, advanced threat hunting, malware analysis capabilities.
b) Utilizing industry standard techniques, tools and procedures, perform network and media digital forensics, incident response, malware analysis, advanced threat hunting across CMS infrastructure;
c) Execute proactive defense of all CMS FISMA systems through Indicators of Compromise (IOC) sweeps / host interrogation and persistent threat hunting;
d) Provide status updates for Incident Response, Digital Forensics, and Malware Analysis according to the battle rhythm established by CCIC IMT for a particular incident.
e) Prepare Enterprise Forensics, Malware Analysis and Advanced Hunting Plan
f) Provide Monthly Technical Status Report
g) Prepare Malware Analysis SOP, Forensic Analysis SOP, Advanced Hunting SOP
h) Maintain Daily Activities Tracker and CCIC FMTA
i) Develop, maintain and update FMAT Concept of Operations and SOP

2.1.6.3 Security Engineering

a) The CCIC Security Engineering team engineers, implements, optimizes, and administers innovative security solutions that reduce Agency risk by providing increased visibility and response readiness across the enterprise;
b) Ensure security System Architecture and Engineering is built into the solution/design as part of the SDLC and solutions implementation;
c) Support CMS and Marketplace SOC Operations and the tools that are used by the various subordinate SOCs;
d) Provide oversight and leadership into the use of current and future security tools used to additionally secure CMS and its datacenters as a whole;
e) Bridge security gaps and enhance Tool interoperability through development and implementation of open source toolkit;
f) Research, Develop, Administer and actively tune Security Implementation for the CMS enterprise that provides Visibility, Situational Awareness, Active Defense, and Response Readiness.
g) Develop Enterprise Security Engineering Plan

h) Develop and Maintain an Enterprise Security Architecture
i) Develop Architectural Drawings for OSSM Network
j)

2.1.6.3.1 Continuous Diagnostics and Mitigation

k) The CCIC Continuous Diagnostic and Mitigation program's primary function is to reduce the risk associated with CMS FISMA systems while lowering the cost of cybersecurity by proactively scanning the CMS enterprise for potential weaknesses, such as: vulnerabilities in unpatched systems, misconfigurations, unaccounted for network aware systems, and the presence of unauthorized software.
l) Provides visibility and improved response readiness across all CMS FISMA systems.
m) Alerting data center technical POC's to potential risks presented by vulnerabilities or unaccounted for systems.
n) Provide mitigation steps for identified vulnerabilities where possible.
o) Continually expand and improve the CDM program to ensure that the Agency maintains an optimal security posture.
p) Prepare CDM Test Plan, Program Reports, Concept of Operations, Standard Operating Procedures
q) Maintain overall tracker of CDM Activities
r) Provide Weekly Project and Activity Status Reports

2.1.6.4 Incident Management

a) The CCIC Incident Management Team provides a variety of critical functions related to situational awareness, incident and vulnerability management, coordination, collaboration, and security oversight for CMS information systems. The IMT is also responsible for setting the Incident Battle rhythm for incident and compromise response activities. The team ensures that each of the individual IR teams and associated stakeholders are provided with timely relevant information to allow for the most effective response activities possible. The IMT ensures that the IR lifecycle as identified in RMH 7.1 and 7.2 is adhered to.
b) The IMT serves as the central coordinating and communications component for security efforts coordination, incident and vulnerability management, for the teams supporting CMS FISMA systems;
c) Provides CMS leadership and appropriate stakeholders with comprehensive situational awareness regarding the status of all security related incidents and activities relating to CMS FISMA systems;

d) Conducts data calls out to federal and contractor staff who own or operate CMS FISMA systems;
e) Provide centralized oversight for all CMS security teams.
f) Provide Privacy expertise to assist ISPG with research and responding to privacy incidents, regardless of how the incident is reported (to include events reported by external partner(s)). An individual with analytical skills, privacy knowledge, and knowledge of healthcare is needed.
g) Incident Response and Management reporting per incident
h) Incident Response Reporting using CMS Template
i) Timeline Report using CMS Template
j) Lessons Learned document
k) Incident Response Exercise documentation
l) Meeting minutes as appropriate
m) Threat information briefs
n) Update CCIC IMT SOP and Concept of Operations
o) CCIC IMT Tracker
p) Weekly Project
q) Incident Response Management Reporting Contribution

2.1.6.5 Cyberthreat Intelligence and Information Sharing

a) The Threat Management Program ensures an optimal Agency security posture by identifying ongoing, immediate, and emerging threats to the organization, including threat actors, attack vectors, and breach scenarios. Proactive threat management informs stakeholders, improves situational awareness, highlights high-risk configuration vulnerabilities, facilitates rapid response, supplies relevant security material, and helps quantify organizational security risk.

b) Provides an architecture and methodology for the collection and sharing of threat intelligence to CMS Leadership, ISPG staff, CCIC functional areas, CMS SOC, Marketplace SOC, and other stakeholders as appropriate to ensure maximum situational awareness.

c) Develop, maintain and optimize an automated integration system to receive, leverage and disseminate cyber threat intelligence identified from multiple classified and open sources for the purpose of detecting, tracking, preventing, and responding to threats and threat actors.

d. Cyberthreat Intel Sharing Enterprise Plan Quarterly Review
e. Weekly Cyberthreat Intel Brief
f. Weekly Technical Status Report
g. Incident Response Threat Package – per incident
h. Develop and Maintain Cyberthreat SOP and Concept of Operations

i. Provide Ad hoc Status Report for ongoing investigations
j. Cyberthreat Intel Tracker
k. Weekly Project and Activity Status Reports

Assumptions, SLAs, and Operating Constraints - for Task Area 6 subcategories:

Penetration Testing Assumptions, SLAs, and Operating Constraints. for 2.1.6.1)**:**

a) The contractor will work with target system personnel to obtain a test specific ROE, Test Plan, and provide Draft and Final Reports;
b) Requires Secret level clearance. The company will not require classified systems or storage, but cleared employees will receive classified Cyberthreat briefings, review reports and information at CMS Controlled Access Area. The government technical representative will provide direction and guidance related to the use of classified systems and information.
c) Have a Rules of Engagement document in place with CMS prior to any testing;
d) Shall also engage in testing not specifically defined as penetration testing, including, but not limited to, vulnerability analysis, lateral movement testing, Red Team / Blue Team activity;
e) Shall complete all penetration testing and Indicators of Compromise (IOC) data received from the Cyberthreat Intel team;
f) Shall format findings into Plan of Action and Milestones for entry into CFACTS II utilizing CMS format;
g) Shall maintain, and make available to appropriate ISPG staff, an up to date library of supporting documentation for each test (ROE, Draft and Final Reports);
h) Shall provide a draft report to ISPG 5 business days after completion of testing, and final report 5 days after receiving government input on a draft report;
i) All deliverables will be provided on time per the Schedule of Deliverables, or as directed by the COR.
j) The contractor shall collaborate with, and provide support to, internal and external entities (CMS groups, contractors, US-CERT, HHS, Local Law Enforcement) for incident response and investigative activities as needed;
k) Conduct ad hoc, daily, weekly, and monthly security briefs and reporting to ISPG staff, executive management, and CMS stakeholders related to the CCIC Penetration Testing program and activities;
l) Continually develop, maintain, and optimize all program documentation related to Penetration Testing based upon innovation, industry techniques, policies, laws, and regulations. Documentation includes, but is not limited to Concept of Operations, Guidelines, and Standard Operating Procedures;
m) Develop, Maintain, Optimize and make available to appropriate ISPG staff, a centralized mechanism for activity tracking CCIC penetration testing projects and activities;
n) Documents, or updates to documents, will be of professional quality, free of spelling, grammar, and formatting errors prior to submission to CMS;

o) Maintains constant communication with CCIC teams for collaboration, process optimization, tools tuning, information sharing and compromise response;
p) Perform operations, maintenance, administration, and optimization activities to maintain and enhance the CCIC Penetration Testing team's toolset;
q) Provide expertise and guidance to ISPG, CMS business owners, and CMS FISMA system stakeholders with regard to secure development, implementation and operation of systems, or enhancement of systems supporting the CMS mission;
r) Provide risk analysis for vulnerabilities, incidents and change requests appropriate;
s) Provide subject matter expertise on policies, industry trends, techniques related to penetration testing;
t) Provides constant situational awareness, and maintains high level of responsiveness to ISPG staff;
u) Receive government approval prior to contacting any stakeholders external to ISPG for any reason;
v) Review scheduled tasks, ad hoc requests, and operations and maintenance (O&M) activities daily and reprioritize as necessary based upon current need;
w) Work with CCIC functional areas to Develop and Optimize CCIC Security Toolset and services distribution to provide comprehensive visibility, situational awareness, and response readiness for all CMS FISMA systems.

Forensics and Malware (Pricing Assumptions, SLAs, and Operating Constraints.):

a) The contractor conducts network and media forensics in support of Agency incident and compromise response activities. Including, but not limited to: Malware Detection, Lateral Movement Detection, Data Collection Detection, and Data Exfil Detection;
b) Requires Secret level clearance. The company will not require classified systems or storage, but cleared employees will receive classified Cyberthreat briefings, review reports and information at CMS Controlled Access Area. The government technical representative will provide direction and guidance related to the use of classified systems and information.
c) Performs Advanced Adversary Hunting;
d) Provides guidance and expertise to Incident Response Teams supporting FISMA systems operated by or on behalf of the CMS mission in the areas of digital forensics and malware analysis;
e) Monitors industry threat intelligence sources to proactively tune tools;
f) Develops, maintains and optimizes malware analysis laboratory environment;
g) Maintains digital evidence Chain of Custody in support of forensic activity, congruent with policy, industry standard processes, and the law;
h) Prepares and provides network and media forensics, malware analysis, and advanced hunting reports using proper CMS reporting format;
i) Utilizes industry standard evidence acquisition, transport, storage and destruction to prevent unauthorized disclosure of data;
j) Develops and shares Indicators of Compromise (IOCs) with CCIC IMT for dissemination to relevant stakeholders;
k) Utilizes CMS Malware Analysis form for forensics and malware analysis reporting;

l) All deliverables will be provided on time per the Schedule of Deliverables, or as directed by the COR.
m) The contractor shall collaborate with, and provide support to, internal and external entities (CMS groups, contractors, US-CERT, HHS, Local Law Enforcement) for incident response and investigative activities as needed;
n) Conduct ad hoc, daily, weekly, and monthly security briefs and reporting to ISPG staff, executive management, and CMS stakeholders related to the CCIC Forensics and Malware Analysis program and activities;
o) Continually develop, maintain, and optimize all program documentation related to Forensics, Malware Analysis and Advanced Hunting based upon innovation, industry techniques, policies, laws, and regulations. Documentation includes, but is not limited to Concept of Operations, Guidelines, and Standard Operating Procedures;
p) Develop, Maintain, Optimize and make available to appropriate ISPG staff, a centralized mechanism for activity tracking CCIC FMAT projects and activities;
q) Documents, or updates to documents, will be of professional quality, free of spelling, grammar, and formatting errors prior to submission to CMS;
r) Maintains constant communication with CCIC teams for collaboration, process optimization, tools tuning, information sharing and compromise response;
s) Perform operations, maintenance, administration, and optimization activities to maintain and enhance the CCIC FMAT toolset;
t) Provide expertise and guidance to ISPG, CMS business owners, and CMS FISMA system stakeholders with regard to secure development, implementation and operation of systems, or enhancement of systems supporting the CMS mission;
u) Provide risk analysis for vulnerabilities, incidents and change requests appropriate;
v) Provide subject matter expertise on policies, industry trends, techniques related to Forensics, Malware Analysis, and Advanced Hunting;
w) Provides constant situational awareness and maintains high level of responsiveness to ISPG staff;
x) Receive government approval prior to contacting any stakeholders external to ISPG for any reason;
y) Review scheduled tasks, ad hoc requests, and operations and maintenance (O&M) activities daily and reprioritize as necessary based upon current need;
z) Work with CCIC functional areas to Develop and Optimize CCIC Security Toolset and services distribution to provide comprehensive visibility, situational awareness, and response readiness for all CMS FISMA systems.

Security Engineering – (Assumptions, SLAs, and Operating Constraints, cont.)

a) The contractor coordinates and provisions access for ISPG federal staff, contractors, and approved non-ISPG staff/contractors;
b) Requires Secret level clearance. The company will not require classified systems or storage, but cleared employees will receive classified Cyberthreat briefings, review reports and information at CMS Controlled Access Area. The government technical representative will provide direction and guidance related to the use of classified systems and information.

c) Creates and maintains inventories of resources used by CCIC;
d) Creates, maintains, and documents security baselines based upon applicable policy;
e) Identifies gaps in security tool coverage or capability, and recommends solutions to address them;
f) Provides subject matter expertise for creation and implementation of security-related hardware and software pilots to enhance the CMS security posture;
g) Serves as Security System architecture and engineering (SA&E) innovation subject matter experts (SMEs) on matters of enterprise security across all CMS FISMA systems;
h) Designs, develops, maintains, and makes available to ISPG personnel detailed security drawings expressing current system security architecture;
i) Operates, maintains and provides 24/7 technical O&M support and administration for the OSSM system. Ensures authority to operate without any lapse in system authorization;
j) All deliverables will be provided on time per the Schedule of Deliverables, or as directed by the COR.
k) Conduct ad hoc, daily, weekly, and monthly security briefs and reporting to ISPG staff, executive management, and CMS stakeholders related to the CCIC Security Engineering program and activities;
l) Continually develop, maintain, and optimize all program documentation related to Security Engineering based upon innovation, industry techniques, policies, laws, and regulations. Documentation includes, but is not limited to Concept of Operations, Guidelines, and Standard Operating Procedures;
m) Develops, Maintains, Optimizes and make available to appropriate ISPG staff, a centralized mechanism for activity tracking CCIC Security Engineering projects and activities;
n) Documents, or updates to documents, will be of professional quality, free of spelling, grammar, and formatting errors prior to submission to CMS;
o) Maintains constant communication with CCIC teams for collaboration, process optimization, tools tuning, information sharing and compromise response;
p) Performs operations, maintenance, administration, and optimization activities to maintain and enhance and deploy the CCIC toolset;
q) Provides expertise and guidance to ISPG, CMS business owners, and CMS FISMA system stakeholders with regard to secure development, implementation and operation of systems, or enhancement of systems supporting the CMS mission;
r) Provide risk analysis for vulnerabilities, incidents and change requests;
s) Provides subject matter expertise on policies, industry trends, techniques related to Security Engineering;
t) Provides constant situational awareness, and maintains high level of responsiveness to ISPG staff;
u) Receives government approval prior to contacting any stakeholders external to ISPG for any reason;
v) Review scheduled tasks, ad hoc requests, and operations and maintenance (O&M) activities daily and reprioritize as necessary based upon current need;

w) The contractor shall collaborate with, and provide support to, internal and external entities (CMS groups, contractors, US-CERT, HHS, Local Law Enforcement) for incident response and investigative activities as needed;

x) Work with CCIC functional areas to Develop and Optimize CCIC Security Toolset and services distribution to provide comprehensive visibility, situational awareness, and response readiness for all CMS FISMA systems.

Continuous Diagnostics and Mitigation (Subtask of Security Engineering)

Assumptions, SLAs, and Operating Constraints.):

a) The contractor monitors and maintains infrastructure supporting credentialed scans for each CMS FISMA system;
b) Requires Secret level clearance. The company will not require classified systems or storage, but cleared employees will receive classified Cyberthreat briefings, review reports and information at CMS Controlled Access Area. The government technical representative will provide direction and guidance related to the use of classified systems and information.
c) Performs O&M activities to maintain and enhance the CDM toolset operations;
d) Performs user administration on Toolset to ensure individuals have access to appropriate data;
e) Works with DHS to continue the maturation process of the CDM effort at CMS;
f) Coordinates with appropriate data center technical POC's for CDM Toolset rollout and maintenance to ensure all networks and assets that process, store, and / or transmit CMS data are scanned;
g) Reviews CMS Component report cards for accuracy prior to submission to government or CMS FISMA system POC's;
h) Works with FISMA system technical POC's to review and evaluate false positives;
i) Generates Weekly Report Cards for CMS Business Owners/ISSOs;
j) Provides direction to end users during mitigation activities if requested;
k) Provides CDM support for the ISPG Ongoing Authorization effort;
l) All deliverables will be provided on time per the Schedule of Deliverables, or as directed by the COR.
m) The contractor shall collaborate with, and provide support to, internal and external entities (CMS groups, contractors, US-CERT, HHS, Local Law Enforcement) for incident response and investigative activities as needed;

Incident Management Team – (Assumptions, SLAs, and Operating Constraints, cont.)

a) The contractor shall communicate threat information and other relevant security data and alerts to CMS FISMA system stakeholders;
b) Requires Secret level clearance. The company will not require classified systems or storage, but cleared employees will receive classified Cyberthreat briefings, review reports and information at CMS Controlled Access Area. The government technical

representative will provide direction and guidance related to the use of classified systems and information.

c) Conducts briefings and provide reporting to ISPG staff, executive management, and Business Owners on the results of Incident Management Team efforts;
d) The contractor coordinates and reports on Vulnerability Assessment activities e.g. DHS Cyber-hygiene activity, Penetration Testing Activity;
e) The contractor sets-up, conducts, and executes after action activities for cross-functional area incident response activities.
f) The contractor shall conduct data calls for, but not limited to, IOC, patching, threat response and vulnerability remediation activity.
g) The contractor shall provide incident management functions for multi-functional area / extra-agency incident response activities related to CMS FISMA systems.
h) The contractor shall provide situational awareness briefs for CMS Leadership and appropriate stakeholders. e.g. Marketplace Daily Security Stand-up
i) The contractor shall set-up and conduct meetings, then provide minutes for meetings related to, but not limited to, data calls, and incident / vulnerability management efforts.
j) All deliverables will be provided on time per the Schedule of Deliverables, or as directed by the COR.
k) Conduct ad hoc, daily, weekly, and monthly security briefs and reporting to ISPG staff, executive management, and CMS stakeholders related to the CCIC IMT projects and activities;
l) Continually develop, maintain, and optimize all program documentation related to Incident and Vulnerability Management based upon innovation, industry techniques, policies, laws, and regulations. Documentation includes, but is not limited to Concept of Operations, Guidelines, and Standard Operating Procedures;
m) Develop, Maintain, Optimize and make available to appropriate ISPG staff, a centralized mechanism for activity tracking CCIC IMT activities;
n) Documents, or updates to documents, will be of professional quality, free of spelling, grammar, and formatting errors prior to submission to CMS;
o) Maintains constant communication with CCIC teams for collaboration, process optimization, tools tuning, information sharing and compromise response;
p) Perform operations, maintenance, administration, optimization activities to maintain and enhance the CCIC toolset;
q) Provide expertise and guidance to ISPG, CMS business owners, and CMS FISMA system stakeholders with regard to secure development, implementation and operation of systems, or enhancement of systems supporting the CMS mission;
r) Provide risk analysis for vulnerabilities, incidents and change requests appropriate to penetration testing;
s) Provide subject matter expertise on policies, industry trends, techniques related to penetration testing;
t) Provides constant situational awareness, and maintains high level of responsiveness to ISPG staff;
u) Receive government approval prior to contacting any stakeholders external to ISPG for any reason;

v) Review scheduled tasks, ad hoc requests, and operations and maintenance (O&M) activities daily and reprioritize as necessary based upon current need;
w) The contractor shall collaborate with, and provide support to, internal and external entities (CMS groups, contractors, US-CERT, HHS, Local Law Enforcement) for incident response and investigative activities as needed;
x) Work with CCIC functional areas to Develop and Optimize CCIC Security Toolset and services distribution to provide comprehensive visibility, situational awareness, and response readiness for all CMS FISMA systems.
y) Incident Response Reporting using CMS Template

Cyberthreat Intelligence and Information Sharing – (Assumptions, SLAs, and Operating Constraints, cont.)

a) Provides threat briefs to CMS Leadership, ISPG staff, and other stakeholders as appropriate.
b) Requires Secret level clearance. The company will not require classified systems or storage, but cleared employees require access to classified systems at CMS Controlled Access Area to research, analyze, and disseminate classified Cyberthreat briefings, reports and information. The government technical representative will provide direction and guidance related to the use of classified systems and information.
c) Monitor threat intelligence sources (security alerts, warnings, and other indicators) from the HHS Computer Security Incident Response Center (CSIRC), the U.S. Computer Emergency Readiness Team (US-CERT), and other OSINT sources to compile CMS-related threat intelligence.
d) Provide cyber-threat intelligence on CMS related topics including, but not limited to: Affordable Care Act, Medicare/Medicaid, or healthcare IT threats, contractors, healthcare providers or government officials.
e) Provide cyber-threat intelligence on cyber campaigns against U.S. information technology that could potentially affect CMS systems.
f) Provide cyber-threat intelligence on a cyber-related attack against the federal/private healthcare sector.
g) Cyber-threat intelligence reports include, but are not limited to the following data elements:
    a. The source or origination of the attack.
    b. The type of attack.
    c. Targeted entity (such as, agency or company)
    d. The known extent of damage or compromise of data.
    e. The specific vulnerabilities in program, code, configurations, social engineering, etc., that are being exploited.
h) Provide contextual intelligence on Einstein alerts.
i) Provide any intelligence on information technology vulnerabilities being reported across the federal and private sectors.

j) Provide intelligence on cyber threat tactics, techniques, and procedures being reported across the federal and private sector.
k) Provide the following information on Advanced Persistent Adversaries a.k.a. Advanced Persistent Threats (APT) tactics, techniques and procedures being using to exploit vulnerabilities in systems.
    a. Objectives – The end goal of the threat / adversary.
    b. Timeliness – The time spent probing and accessing the target system/ environment.
    c. Resources – The level of knowledge, expertise, and tools used.
    d. Risk Tolerance – The extent to which the threat goes to remain undetected.
    e. Skills and methods – The tools and techniques used throughout the event.
    f. Actions – The precise actions taken.
    g. Attack origination points – Points where the event originated.
    h. Numbers involved – Value indicating the number of systems (internal & external) involved. To include system sensitivity.
    i. Knowledge source – The ability to discern any information regarding any of the specific threats through online information gathering.
l) Develop, maintain, optimize a system for collecting, managing, storing, and sharing of cyber threat intelligence
m) Contributes to Incident Response activities by providing contextual Threat Intelligence Package related to IOC(s) identified
n) All deliverables will be provided on time per the Schedule of Deliverables, or as directed by the COR.
o) The contractor shall collaborate with, and provide support to, internal and external entities (CMS groups, contractors, US-CERT, HHS, Local Law Enforcement) for incident response and investigative activities as needed;
p) Conduct ad hoc, daily, weekly, and monthly security briefs and reporting to ISPG staff, executive management, and CMS stakeholders related to the CCIC Cyberthreat Intelligence program and activities;
q) Continually develop, maintain, and optimize all program documentation related to Penetration Testing based upon innovation, industry techniques, policies, laws, and regulations. Documentation includes, but is not limited to Concept of Operations, Guidelines, and Standard Operating Procedures;
r) Develop, Maintain, Optimize and make available to appropriate ISPG staff, a centralized mechanism for activity tracking CCIC Cyberthreat Intelligence projects and activities;
s) Documents, or updates to documents, will be of professional quality, free of spelling, grammar, and formatting errors prior to submission to CMS;
t) Maintains constant communication with CCIC teams for collaboration, process optimization, tools tuning, information sharing and compromise response;
u) Perform operations, maintenance, administration, optimization activities to maintain and enhance the CCIC Cyberthreat Intelligence team's toolset;
v) Provide expertise and guidance to ISPG, CMS business owners, and CMS FISMA system stakeholders with regard to secure development, implementation and operation of systems, or enhancement of systems supporting the CMS mission;

w) Provide risk analysis for vulnerabilities, incidents and change requests appropriate to penetration testing;
x) Provide subject matter expertise on policies, industry trends, techniques related to Cyberthreat Intelligence;
y) Provides constant situational awareness, and maintains high level of responsiveness to ISPG staff;
z) Receive government approval prior to contacting any stakeholders external to ISPG for any reason;
aa) Review scheduled tasks, ad hoc requests, and operations and maintenance (O&M) activities daily and reprioritize as necessary based upon current need;
bb) Work with CCIC functional areas to Develop and Optimize CCIC Security Toolset and services distribution to provide comprehensive visibility, situational awareness, and response readiness for all CMS FISMA systems.
cc) Extreme care shall be continually employed to ensure classified information remains within the control of the authorized CMS secure locations. Those allowed using a 'tear line' method. IOC consumption will use approved CMS processes and procedures.

2.1.7 Task Area 7: CMS Security Operations Center

a) The CMS Security Operations Center provides comprehensive operational cybersecurity situational awareness and response readiness by either peering with existing data center SOCs, or directly performing 24x7 cybersecurity monitoring and advanced analytics for in support of CMS FISMA systems that lack expertise in these areas.
b) SOC Manager Requires Secret level clearance. SOC contractors require Secret level clearance. The company will not require classified systems or storage, but cleared employees will receive classified Cyberthreat briefings, review reports and information at CMS Controlled Access Area. The government technical representative will provide direction and guidance related to the use of classified systems and information.
c) Monitor, defend and protect perimeter interface for malicious network traffic
d) Monitor, defend and protect hosts within each FISMA boundary for malicious activity or activity that could indicate lateral movement within the environment
e) Performing advanced network analysis of egress and ingress traffic;
f) Monitoring security events, correlated information from data center feeds and CCIC functional areas to identify incidents, issues, threats, and vulnerabilities;
g) Conduct initial triage, containment, categorization, and escalation for suspicious events and incidents;
h) Providing compromise response activities as necessary;
i) Support other SOC's throughout the CMS enterprise as needed to maximize visibility, response readiness and situational awareness
j) Incident Response Threat Package – Ad hoc per incident
k) Develop and maintain SOC SOP and Concept of Operations
l) Prepare Incident Handling documentation per incident

m) Prepare SOC Enterprise Plan
n) Maintain SOC Activities Tracker
o) Monthly Project Status and Monthly Activities Report
p) Incident Response and Management Reporting Contribution

Assumptions, SLAs, and Operating Constraints:

a) All deliverables will be provided on time per the Schedule of Deliverables, or as directed by the COR.
b) Conduct ad hoc, daily, weekly, and monthly security briefs and reporting to ISPG staff, executive management, and CMS stakeholders related to the CMS Security Operations Center program and activities;
c) Continually develop, maintain, and optimize all program documentation related to the CMS Security Operations Center based upon innovation, industry techniques, policies, laws, and regulations. Documentation includes, but is not limited to Concept of Operations, Guidelines, and Standard Operating Procedures;
d) Develop, Maintain, Optimize and make available to appropriate ISPG staff, a centralized mechanism for activity tracking CMS SOC projects and activities;
e) Documents, or updates to documents, will be of professional quality, free of spelling, grammar, and formatting errors prior to submission to CMS;
f) Maintains constant communication with CCIC teams for collaboration, process optimization, tools tuning, information sharing and compromise response;
g) Perform operations, maintenance, administration, optimization activities to maintain and enhance the CMS Security Operations Center team's toolset;
h) Provide expertise and guidance to ISPG, CMS business owners, and CMS FISMA system stakeholders with regard to secure development, implementation and operation of systems, or enhancement of systems supporting the CMS mission;
i) Provide risk analysis for vulnerabilities, incidents and change requests;
j) Provide subject matter expertise on policies, industry trends, techniques related to penetration testing;
k) Provides constant situational awareness, and maintains high level of responsiveness to ISPG staff;
l) Receive government approval prior to contacting any stakeholders external to ISPG for any reason;
m) Review scheduled tasks, ad hoc requests, and operations and maintenance (O&M) activities daily and reprioritize as necessary based upon current need;
n) The contractor shall collaborate with, and provide support to, internal and external entities (CMS groups, contractors, US-CERT, HHS, Local Law Enforcement) for incident response and investigative activities as needed;
o) Work with CCIC functional areas to Develop and Optimize CCIC Security Toolset and services distribution to provide comprehensive visibility, situational awareness, and response readiness for all CMS FISMA systems.

2.1.8 Task Area 8: Marketplace Security Operations Center

a) The CMS Marketplace Security Operations Center provides comprehensive operational cybersecurity situational awareness and response readiness by performing 24x7 cybersecurity monitoring and advanced analytics for the 45+ FISMA systems spread across 3 data centers that comprise the ACA Health Insurance Marketplace infrastructure.
b) Marketplace SOC Manager requires Secret level clearance. SOC contractors require Secret level clearance. The company will not require classified systems or storage, but cleared employees will receive classified Cyberthreat briefings, review reports and information at the CMS Controlled Access Area. The government technical representative will provide direction and guidance related to the use of classified systems and information.
c) This is accomplished through monitoring collected data feeds from all 3 data centers supporting the Marketplace;
d) Monitor, defend and protect every perimeter interface for malicious network traffic
e) Monitor, defend and protect every host within each FISMA boundary for malicious activity or activity that could indicate lateral movement within the environment
f) Performing advanced network analysis of egress and ingress traffic;
g) Monitoring security events, information correlation from data center feeds and CCIC functional areas to identify incidents, issues, threats, and vulnerabilities;
h) Conducting initial triage, containment, categorization, and escalation for suspicious events and incidents;
i) Providing compromise response activities as necessary.
j) Incident Response Threat Package – Ad hoc per incident
k) Develop and maintain Marketplace SOC SOP and Concept of Operations
l) Prepare Incident Handling documentation per incident
m) Prepare Marketplace SOC Enterprise Plan
n) Maintain Marketplace SOC Activities Tracker
o) Monthly Project Status and Monthly Activities Report
p) Incident Response and Management Reporting Contribution

Pricing Assumptions, SLAs, and Operating Constraints:

a) All deliverables will be provided on time per the Schedule of Deliverables, or as directed by the COR.
b) Conduct ad hoc, daily, weekly, and monthly security briefs and reporting to ISPG staff, executive management, and CMS stakeholders related to the Marketplace SOC program and activities;
c) Continually develop, maintain, and optimize all program documentation related to Penetration Testing based upon innovation, industry techniques, policies, laws, and

regulations. Documentation includes, but is not limited to Concept of Operations, Guidelines, and Standard Operating Procedures;
d) Develop, Maintain, Optimize and make available to appropriate ISPG staff, a centralized mechanism for activity tracking Marketplace SOC projects and activities;
e) Documents, or updates to documents, will be of professional quality, free of spelling, grammar, and formatting errors prior to submission to CMS;
f) Maintains constant communication with CCIC teams for collaboration, process optimization, tools tuning, information sharing and compromise response;
g) Perform operations, maintenance, administration, optimization activities to maintain and enhance the Marketplace SOC toolset;
h) Provide expertise and guidance to ISPG, CMS business owners, and CMS FISMA system stakeholders with regard to secure development, implementation and operation of systems, or enhancement of systems supporting the CMS mission;
i) Provide risk analysis for vulnerabilities, incidents and change requests appropriate to penetration testing;
j) Provide subject matter expertise on policies, industry trends, techniques related to penetration testing;
k) Provides constant situational awareness, and maintains high level of responsiveness to ISPG staff;
l) Receive government approval prior to contacting any stakeholders external to ISPG for any reason;
m) Review scheduled tasks, ad hoc requests, and operations and maintenance (O&M) activities daily and reprioritize as necessary based upon current need;
n) The contractor shall collaborate with, and provide support to, internal and external entities (CMS groups, contractors, US-CERT, HHS, Local Law Enforcement) for incident response and investigative activities as needed;
o) Work with CCIC functional areas to Develop and Optimize CCIC Security Toolset and services distribution to provide comprehensive visibility, situational awareness, and response readiness for all CMS FISMA systems.

3 Contract Management Requirements

3.1 Kickoff Meeting

Upon award, a Kickoff meeting and Contractor Orientation Meeting shall be held with CMS and the Contractor to introduce team members to the CMS Program and to review the SOW task areas and to discuss expectations

The Contractor shall schedule the Kickoff meeting to occur within 5 days of contract award at which time, the following will be provided by the Contractor:

- Project work schedule
- Staffing Plan including resumes, as requested.

- Non-Disclosure Agreements for Contractor shall be provided and require signature

The Contractor shall provide minutes of this meeting.

3.2 Project Status Meetings

The Contractor shall perform all project management duties, including technical and business management functions, in order to plan, implement, track, report, and deliver the services requested under this contract. Monthly Project Status Meetings shall be conducted among the Contractor, and the Contracting Officer's Representative (COR). Other CMS stakeholders may be invited to attend at the COR's discretion. Meetings will be held monthly, at a minimum, and may be more frequent at the COR's discretion. The meetings will be held at a location designated by CMS. At these meetings, the Contractor shall provide a progress review of the tasks listed above.

The progress review shall include:

1. An overview of the items completed since the last reporting period
2. An overview of the project status with a focus on outstanding issues and risks
3. An overview of the work to be performed through the next reporting period
4. An overview of the financial status
5. A discussion of issues and risk
6. A discussion of items delayed/not on schedule

The Contractor shall prepare and submit an agenda 2 business days prior to each meeting and prepare and provide minutes of each meeting within 24 hours after the meeting. The meeting minutes, at a minimum, shall include the following:

1. List of participants
2. Purpose of the meeting
3. Decisions reached during the meeting
4. Action items identified (including the person responsible for addressing the action and the date the action is to be completed)
5. Date, time, and location of next meeting

3.3 Location

All work will be performed in a Government provided facility.

3.4 Key Personnel

All proposed substitutions of key personnel shall be submitted, in writing, to CMS at least thirty (30) days prior to the proposed substitution, or as soon as reasonably known. Each request shall provide a detailed explanation of the circumstances necessitating the proposed substitution, a complete resume, and any other information required by CMS. All proposed substitutions shall have qualifications equal to or greater than the person(s) being replaced.

Key Personnel include, but are not limited to:

1. One (1) Program Manager
    a. Must be PMP Certified
2. One(1) Project Manager
3. SOC Manager
4. Task 6 Lead

3.5 Contractor Facility Clearance

This contract requires the contractor to have and maintain a Facility Clearance (FCL) approved by the Defense Security Service (DSS) granted at the Secret Level. The purpose of this requirement lies in the nature of the work performed as part of this contract. The government does not expect the contractor to store any classified information at their facility from work performed on this contract. All classified information resulting from work performed on this contract will be stored within government controlled facilities.

3.6 Deliverables

The Contractor shall ensure the timeliness and quality of the deliverables for the individual task orders. The deliverables shall be given to the COR NO LATER THAN the due dates listed in the Deliverable Schedule for each individual task order. Unless otherwise noted, CMS will review each of the deliverables and return comments to the Contractor within ten (10) business days. Where feasible, the Contractor shall correct the deliverable and return a final product to the COR within four (4) business days after receiving comments.

If CMS changes to a newer version of the MS-Office products or products providing similar functionality of MS-Office, the contractor shall provide deliverables in the new version. All deliverables provided must be Section 508 compliant. All reports created shall be submitted to CMS via email or a CMS provided portal.

The Contractor shall develop a document naming convention that uniquely identifies the document title, version, date, draft or final. (e.g. xxx.yyy.mm/yr. draft) as follows. DRAFT/FINAL (containing version number, author, and QA reviewer): Many of the requirements for the deliverables require both a Draft and a Final version. The Final copy is to be a submission of the full document with all CMS comments resolved. The deliverable cover page shall be clearly marked Draft or Final. All final updated deliverables shall be delivered in two versions: one copy utilizing the "tracking" function in MS-WORD or similar "tracking" word processor if CMS moves from MS-Office; and one copy as final with all tracking functionality removed.

The Contractor shall provide a "quick-look" draft of the deliverable prior to the initial draft delivery. The "quick-look" shall be in the form of an annotated outline to ensure the document contains the necessary information earlier in the development process.

UPDATES: In addition, many of the deliverables require the Contractor to provide updates, unless otherwise specified. The Contractor is expected to notify CMS when it foresees a change to the content and then provide an updated document based upon CMS-approved content revisions and a mutually agreed upon delivery date. Those deliverables, which are updates to existing material, shall utilize the MS-WORD "tracking" function or similar "tracking" word processor if CMS moves from MS-Office; to highlight all changes, additions, and deletions to the original documents.

All documents, once approved, shall be maintained and kept current by the Contractor. MONTHLY REPORTS: The data collection period for each monthly report shall be based on the whole month, based on the Contractor's accounting month (e.g. April 1 through 30). The Contractor shall ensure that the data in the recurring monthly reports are accurate and consistent with one another assuring that each monthly report also incorporates any subcontractor's data for the same period of time.

3.6.1 Schedule of Deliverables

Deliverable #	SOW/Ref #	Description of Deliverable	Date Required
0001	B.1	Kick Off and Contractor Orientation Meeting	5 business days after contract award
0002	B.1	Project Management Plan, Staffing Plan and Project Schedule	Initial: 2 weeks after contract award
0003	E.	Quality Assurance Plan, and Transition-In Plan	Initial: 3 weeks after contract award
0004	H.	Monthly Technical Status Report	Monthly
0005	2.1.1	Situational Report	Weekly

Deliverable #	SOW/Ref #	Description of Deliverable	Date Required
0006	2.1.1	Status Report	Monthly
0007	2.1.3.1	Provide accomplishment report of A&A support provided	Monthly
0008	2.1.2.3	Mailbox Report Card	Monthly
0009	2.3	Information Security Help Desk Status Report	Monthly
0010	2.1.3.2	Provide accomplishment report of Ad hoc S/P Engineering services provided	Monthly
0011	2.1.4	Provide accomplishment report of S/P Awareness and Training services provided	Monthly
0012	2.1.5	Provide accomplishment report of S/P Audit support provided	Monthly
0013	2.1.6.1*	Weekly Project Status Report	Weekly
0014	2.1.6.1*	Weekly Activity Status Reports for Penetration Testing Team	Weekly
0015	2.1.6.1*	Monthly Project Status Report	Monthly
0016	2.1.6.1*	Monthly Penetration Testing Roll-up of activities	Monthly
0017	2.1.6.3.12*	FISMA System Report Card	Monthly
0018	2.1.6.3.1	Monthly Project Status Report	Monthly
0019	2.1.6.3.12*	CCIC CDM Monthly Roll-up of activities	Monthly
0020	2.1.6.3*	CCIC FMAT Monthly Roll-up of activities	Monthly
0021	2.1.6.3.*	Monthly Activity Status Reports for CCIC FMAT	Monthly
0022	2.1.6.3*	Monthly Project Status Report	Monthly
0023	2.1.6.3*	CCIC Security Engineering Monthly Roll-up of activities	Monthly
0024	2.1.6.4*	Monthly Project Status Report	Monthly
0025	2.1.6.4*	Monthly CCIC IMT Roll-up of activities	Monthly
0026	2.1.6.5*	Monthly Project Status Report	Monthly
0027	2.1.6.5*	Monthly Cyberthreat Intelligence and Information Sharing Roll-up of activities	Monthly
0028	2.1.8.1*	Monthly Project Status Report	Monthly
0029	2.1.8.1*	Monthly CMS Marketplace Security Operations Center Roll-up of activities	Monthly

* information / documents associated with these SOW/Ref# has the potential to be classified. The government technical representative will provide direction and guidance related to the use of classified information. (In accordance with existing classification security guides, source documents, or compilation of unclassified information.)

The deliverables shall be submitted to the COR as listed below:

Contracting Officer's Representative (COR):

TBD

3.8 Quality Assurance

The Contractor shall include Quality Assurance (QA) as part of large and small tasks performed. QA procedures should be on a scale appropriate for the size, criticality, and complexity of the task order requirements. QA applies to all deliverables, including project plans, periodic reports, findings and reports, gap analysis, training materials, written and verbal Help Desk response, and technical advisory services for security related documentation. All written deliverables shall be clearly written without any grammar or spelling errors. At a minimum, the contractor shall provide CMS with QA that will:

1. Provide a planned process which makes certain that products are produced in conformance with established standards and requirements;
2. Promote secure systems with quality built in early in the development lifecycle based on consistent application of information security guidance; and
3. Establish a uniform/structured approach to make certain that quality considerations are addressed in regard to information security with emphasis on early security risk detection and continuing improvement of the development and QA process.

CMS has the right to inspect, observe, and evaluate all work performed and all work efforts or products as they progress and is not limited to the final deliverables. CMS shall review all work products developed by the contractor(s) prior to finalization. Final acceptance of all work products is subject to CMS's approval. CMS retains ownership of all work products.

Qualified Personnel
Throughout the period of this contract, the Contractor shall provide only those personnel who are fully qualified and competent to perform their assigned work and who possess the minimum background/experience to complete the work as called out in SOW. The Contractor shall designate as key the Project Manager for this contract who oversees day-to-day activities of this contract and act as primary point of contact for the Contracting Officer and COR.

3.9 Reporting

The Contractor shall provide the project status information cited in the Contract, on a monthly basis or more often as directed by the Contracting Officer. The Contractor shall provide a (1) Monthly Electronic Technical Progress Report, (2) Monthly Contract Summary Report, and (3) Monthly Financial Planning Report to the CMS COR as directed. The reports shall be in hard copy and electronic format compatible with CMS Government

hardware and software. Other deliverables and reporting requirements may be specified in addition to those described in the following subsections.

The Government will review and return each submission of a draft report indicating approval or disapproval, and comments, as specified in each task order. In the event the Government delays review and return of any submission of draft reports beyond the period specified, the Contractor shall immediately notify the Contracting Officer in writing and the Contractor will be entitled to an extension in submission of the approved report(s).

The Contractor shall notify the Contracting Officer when 80 percent of the task funds have been spent.

3.9.1 Monthly Technical Progress Report

The Contractor shall submit a summary monthly electronic progress report, one (1) copy each to the Contracting Officer, and the COR. The monthly status report shall briefly state the progress made, and the actual work completed. Specific areas of interest shall include difficulties encountered during the reporting period and remedial action taken, and a statement of activity anticipated during the subsequent reporting period. The report shall include any proposed changes of key personnel concerned with the contract effort.

3.9.2 Monthly Contract Summary Report

The summary report is due to the COR by the fifteenth (15th) calendar day of the month.

3.10 Execution, Monitor and Control of Project Deliverables

Using standard methodology and good practice provide work progress, performance and scope information to enable accurate monitoring of project performance and to capture variances against baseline.

Partner with CMS project team to control all aspects of the project such that the delivery of the managed service and associated deliverables remains on track and in accordance with identified terms of the agreed upon Service Level Agreement.

In addition to the proposed Contractor's Service Level Agreements, the following are the minimum quality measures that will be executed, monitored and controlled.

Category	Performance Standard	AQL	Surveillance Methodology
Deliverables are Timely, Complete, and Accurate	Timely: deliverables are received within the prescribed time of delivery as defined by the project schedule	All deliverables during the period are received on time in accordance with the Project Schedule.	100% inspection
	Complete: deliverables contain all the prescribed information in accordance with HHS and CMS standards and program guidance	100% of the document is compliant with governing standards and guidance	100% inspection
	Accurate: deliverables reflect the necessary scope and information. They also are free of grammatical and typographical errors	100% of the document is compliant with the performance standard	100% inspection
Customer Satisfaction	The Contractor has provided value-added advice/thought leadership and deliverables that reflect the ISPG's needs to achieve program success	99% satisfaction	Help desk surveys, Annual Past Performance Evaluation
Responsiveness	The Contractor responds to ISPG staff and acknowledges inquiry within one business day	99% of all inquiries are responded to	Direct Observation

3.11 Project and Development Methodology Compliance

Weekly reviews and monthly update sessions will occur to ensure project documents are accurate and up to date.

3.12 Non-Disclosure

Information collected before, during, and after the CMS period of performance shall be treated as proprietary and shall only be disclosed to designated CMS officials and CMS-authorized personnel.

The Contractor shall identify any actual, apparent, or potential organizational or personnel conflicts of interest in relation to each task order request issued hereunder, and in relation to specific work requirements awarded to the Contractor, and shall immediately notify the Contracting Officer regarding any identified concerns in accordance with the requirements at FAR Subpart 9.5.

3.13 Government-Furnished Information, Equipment, & Facilities

The Contractor is responsible for providing all facilities necessary for performance of the work specified herein, with the exception of contractor personnel performing tasks under the task "CMS SOC." Contractor personnel supporting that task will be located in a Government-Furnished facility which is currently located in the Woodlawn, MD area.

CMS will provide the following types of government-furnished information (GFI) listed below, when applicable, to individual task order requirements:

1. Government-furnished equipment and authorizations to enable connection of contractor equipment to CMS Networks
2. Information Security Program Documentation to include:
    a. Source documents identified as public access documentation available on the CMS information security website virtual library
    b. Proposed enterprise-wide program documentation preliminary revisions or draft updates under consideration by CMS information security program
    c. Design Documents
    d. Architecture Documents
    e. Concept of Operations Documents
    f. Help Desk Scripts and related Documents
    g. User Guides
    h. Risk Assessments
    i. Application Developer Guides
    j. CMS Internet Architecture Document
    k. CCIC Hardware and software will be purchased on a separate CMS contract and be provided to the Contractor for use.

3.14 Service Level Agreements

Part of the strategic vision of CMS is to evolve to a more services-based enterprise. Service Level Agreements (SLAs) are a contractual tool that establishes the level of performance expected of the Contractor on a given task as agreed to between the Contractor and CMS. Although the Contractor is required to be fully compliant with all requirements of this task order, the SLAs help define acceptable levels of compliance. They are intended to measure

how well the key aspects of the SOW are carried out. SLAs are the mechanism to facilitate and enforce a services based enterprise.

The Contractor shall, at minimum report monthly on SLAs and in coordination with CMS, evaluate the effectiveness of the SLAs to modify, develop, and implement more effective SLAs.

4 POST-AWARD CONFERENCE

The contractor shall plan and participate in an initial meeting/kickoff meeting between the COR and other participants as identified by CMS. The kick-off meeting will be held at the CMS Office at 7500 Security Boulevard, Woodlawn, MD location within five (5) business days after contract award. All travel costs associated with the initial meeting/kickoff meeting shall be included in the contractor's firm fixed price proposal.

4.1 Transition from an Existing Contractor

The following relates to transition from an existing contractor subsequent to the award of this contract should a transition be necessary. Activities related to transition shall be conducted over a period of approximately one month, not expected to exceed 6 months. During this transition period, the incumbent contractor shall work with CMS and the new contractor to set up a transition schedule including a schedule of events to smoothly changeover to the new contractor.

Not more than two weeks after notification by CMS that the transition to a new contractor shall take place, the incumbent contractor shall submit to the COR and PO a draft written Joint Operating Agreement (JOA). Both the incumbent contractor and the new maintenance contractor shall sign the JOA.

The JOA shall define the responsibilities for the incumbent contractor and the new contractor and shall be submitted to CMS for review and approval before final signatures are obtained. In addition, as part of the JOA, the incumbent contractor and the new contractor shall form a joint coordinated management team that shall ensure that communication, coordination, cooperation, and consultation between the two entities is maintained in support of the transition and ongoing work. Such a team shall have regular meetings and shall monitor the work of any subgroups during transition and ongoing work, and shall submit status reports as determined by CMS.

During the first half of the transition, the incumbent contractor shall remain responsible for program maintenance. The incoming contractor shall "shadow" the activities of the incumbent contractor. For the remaining half of the transition period, the new contractor shall take responsibility for program maintenance while the incumbent contractor shadows their activity. The exact date of responsibility transfer is not fixed and is subject to the approval of CMS.

4.2 Transition to a New Contractor

Transition to a new contractor may be subsequent to the award of this contract, should a follow-on contractor be awarded this contract. The transition to a new contractor may be required as a result of a future competitive RFP for this effort.

Activities related to transition (should the transition be required) shall be conducted over a period not expected to exceed 6 months. During this transition period, the incumbent contractor shall work with CMS and the new contractor to set up a transition schedule including a schedule of events to smoothly changeover to the new contractor.
Not more than two weeks after notification by CMS that the transition to a new contractor shall take place, the incumbent contractor shall submit to the PO a draft written JOA. Both the incumbent contractor and the new contractor shall sign the JOA.

The JOA shall define the responsibilities for the incumbent contractor and the new contractor and shall be submitted to CMS for review and approval before final signatures are obtained. In addition, as part of the JOA, the incumbent contractor and the new contractor shall form a joint coordinated management team that shall ensure that communication, coordination, cooperation, and consultation between the two entities is maintained in support of the transition and ongoing work. Such a team shall have regular meetings and shall monitor the work of any subgroups during transition and ongoing work and shall submit status reports as determined by CMS.

No later than four weeks after notification by CMS that the transition to a new contractor shall take place, the incumbent contractor shall submit a Transition Plan. The Plan shall include but not be limited to the following:

4.2.1 Transition Plans and Procedures:

1. Transition milestones and timeframes, including a detailed timeline for work-in-progress;
    l. A comprehensive listing of the responsibilities of all personnel participating in the transition to include the policies, practices, and procedures to be employed by the incumbent contractor to ensure there is no conflict between routine program maintenance and the activities of the transition;
    m. An in-depth schedule and thorough description of the methodology employed by the incumbent contractor to ensure no degradation of service during the transition period;
    n. A risk management plan that includes a list of the potential risks during the transition period and the plan to mitigate each;
    o. A complete and detailed resource-planning/resource-turnover analysis; and
    p. Any travel necessary to support the transition.

4.2.2 Training:

The incumbent contractor shall provide comprehensive training and training materials. The training shall be conducted in the Baltimore, Maryland, area. Training and materials shall include, but not be limited to, the following:

1. Customer support;
    q. History and derivation of any systems;
    r. CMS Information Security Policy;
    s. Security Operations Center Procedures;
    t. Authority to Operate Review Process;
    u. Standard Operating Procedures;
    v. Quality assurance procedures;
    w. System documentation;
    x. User documentation; and,
    y. Continuity of operations.

Training Requirements for Cleared Employees.

1. The Facility Security Officer (FSO) must ensure cleared employees complete the training below prior to performing work on this CMS contract. This training is in addition to the required company training for employees with a security clearance.

    a. Employees that will produce classified documents and/or access classified systems:

DSS/CDSE Courses	**Hours**	**Course #**	**Exam #**	**Remarks**
Derivative Classification Course and Exam	2.5 hours	IF103.16	IF103.06	Every 2 years
Introduction to Information Security Course and Exam	3 hours	IF011.16	IF011.06	One time
Marking Classified Information Course and Exam	2 hours	IF105.16	IF105.06	One time
Unauthorized Disclosure of Classified Information Course and Exam	2 hours	IF130.16	IF130.06	One time

2. The Contract Officer Representative (COR) and/or Government Technical Representative (GTR) will ensure the following training is completed by all individuals during the first week of work at CMS:

CMS Security Training	Hours	Remarks
CI, Insider Threat, Cyber Security/Threat	1.5 hours	LMS - Annually
Review the NSI Policy and Handbook	1 hour	Intranet – One time
Review the Secure Space SOP	1 hour	Employees working in the Secure Space – One time

3. The information identified above is not all inclusive. Additional training may be required, depending on the level of security clearance and access to classified systems.

4.2.3 List of Attachments:

a. DD254

4.2.4 Travel

The Contractor is responsible for all travel required in connection with the performance of the tasks described in this document. Travel associated with supporting this work is expected to be about 30 business days for each contract year to attend information security best practices conferences and/or training. These conferences could be throughout the continental United States including, but not limited to Florida, Nevada, and California. However, in the event of Conference Moratoriums or travel restrictions imposed by the Agency this could change and travel may not be allowed.

All contractor key personnel participating in the work described herein are assumed to work within the local commuting area of their duty station, wherever that may be. All contractor personnel shall be available for monthly and weekly periodic meetings at CMS in Baltimore, Maryland. Accordingly, the travel estimate provide herein does not include any travel to CMS Headquarters or from the personal residence of contractor personnel to their duty station.

4.2.5 DD Form 254

The Contractor is required to have and maintain an active DD Form 254 as part of this contract. The DD 254 will convey the security requirements, classification guidance and provide handling procedures for the classified material received and/or generated on a classified contract. Classified information at the Secret level will be accessed and reviewed within the Centers for Medicare and Medicaid Services (CMS).

The Contractor will participate in classified Cyberthreat briefings, review classified reports and information within CMS Controlled Access Areas only. The government technical representative will provide direction and guidance related to the use of classified systems and information. As requested, the Contractor will monitor threat intelligence sources (security alerts, warnings, and other indicators) from the HHS Computer Security Incident Response Center (CSIRC), the U.S. Computer Emergency Readiness Team (US-CERT), and other OSINT sources to compile CMS-related cyber threats. The contractor will have occasional access to JWICS to review cybersecurity threat information including, but not limited to, Indicators of Compromise (IOCs).

The Contractor will not be required or authorized to maintain classified systems or classified storage at their location in support of this program/contract.

4.2.6 Federal Information Security Management Act (FISMA) of 2002

CMS collects, uses, and stores information that falls into the categories of privacy data, Protected Health Information (PHI), proprietary data, procurement data, inter-agency data, and privileged system information. Access to these types of information is controlled by the Privacy Act of 1974 (as amended), the Computer Security Act of 1987 (as amended), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Information Security Management Act (FISMA) of 2002. As a result, CMS and the Contractors that perform work on our behalf have a legal and practical responsibility to maintain the confidentiality, integrity, and availability (CIA) of this information.

FISMA is applicable to the proposed acquisition in as much as the Contractor's responsibility will include protecting federal information and federal information systems by conducting cybersecurity operations and assisting in the development of IT security policies. Rather than developing an IT security test plan and performing IT assessments, the contractor will review in such assessments and conduct of security assessments. The Contractor must comply to relevant HHS policies to include HHS OCIO Policy for Enterprise Architecture. A copy of this policy is available at: http://www.hhs.gov/ocio/policy/index.html.

4.2.7 FIPS HSPD12

In accordance with Homeland Security Presidential Directive (HSPD)-12, contractor access to HHS-controlled facilities, information technology systems, or sensitive data all Contractor staff of this acquisition must be cleared at a minimum of PT6 and for some tasks as high as Secret.

4.2.8 Records Management Requirements

All data and deliverables are the property of CMS and are required to be maintained in accordance with HHS/OCIO's policy on records management. This policy is available at:

http://www.hhs.gov/ocio/policy/2007-0004.001.html. All reports created shall be submitted to CMS via email or a CMS provided portal.

4.2.9 Section 508 Requirements

The Contractor shall comply with the Section 508 accessibility standards listed below:

- Subpart A — General
- Subpart B — Technical Standards
    - Software Applications and Operating Systems (1194.21)
    - Web-based Intranet and Internet Information and Applications (1194.22)
    - Telecommunications Products (1194.23)
    - Video and Multimedia Products (1194.24)
    - Self Contained, Closed Products (1194.25)
    - Desktop and Portable Computers (1194.26)
- Subpart C — Functional Performance Criteria
- Subpart D — Information, Documentation, and Support

4.2.10 HHS Enterprise Performance Life Cycle (EPLC)

All IT systems development or enhancement tasks supported by the contractor shall follow the HHS Enterprise Performance Life Cycle (EPLC) framework and methodology. Information about EPLC policy and framework is available at http://www.hhs.gov/ocio/policy/2008-0004.001.html and http://www.hhs.gov/ocio/eplc-lifecycle-framework.pdf.