**SAMPLE – For Reference Only** – This sample is a redacted copy of a work statement accomplished under a NITAAC GWAC. A Statement of Work (SOW) is typically used when the task is well-known and can be described in specific terms. Statement of Objective (SOO) and Performance Work Statement (PWS) emphasize performance-based concepts such as desired service outcomes and performance standards. Whereas PWS/SOO's establish high-level outcomes and objectives for performance and PWS's emphasize outcomes, desired results and objectives at a more detailed and measurable level, SOW's provide explicit statements of work direction for the contractor to follow. However, SOW's can also be found to contain references to desired performance outcomes, performance standards, and metrics, which is a preferred approach. **This sample is not all inclusive, therefore the reader is cautioned to use professional judgment and include agency specific references and regulations to their own PWS/SOO/SOW.**

IT Security and Privacy Services Statement of Work

# Background

## <AGENCY> Mission

The <AGENCY> mission is to fund research and education in science and engineering disciplines while supporting programs to strengthen the scientific and engineering research potential. Mission activities include receiving research proposals, conducting peer reviews through the use of panels or electronic messaging, and awarding funds to institutions and their principal investigators.

## Background

<AGENCY> is an independent agency of the US Government, established by the XXX. <AGENCY> funds research and education in science and engineering. It does this through grants, contracts, and cooperative agreements to more than 2,000 colleges, universities, and other research and/or education institutions in all parts of the US. <AGENCY> accounts for about 20 percent of federal support to academic institutions for basic research.

Each year, <AGENCY> makes approximately 9,000 new awards and receives approximately 40,000 new or renewal support proposals for research, graduate and postdoctoral fellowships, and math/science/engineering education projects. The awards typically go to universities, colleges, academic consortia, nonprofit institutions, and small businesses.

<AGENCY> strives to be on the leading edge of grants administration and management practices. <AGENCY> was the first Federal agency to explore accomplishing its proposal and award administration functions through electronic means. From the inception of the FastLane System in 1994, <AGENCY> has worked to facilitate business transactions and exchange information between <AGENCY> and its grantee community.

In February 2006, the Office of Management and Budget (OMB) selected <AGENCY> to lead a research-focused grants consortium called Research.gov as part of the Grants Management Line of Business (GMLoB) initiative. OMB selected <AGENCY> to lead this initiative for the research community because of <AGENCY>’s successful track record with FastLane, focus on the research community, high standards and level of performance to its customers, and leadership position within the grants community. Research.gov is a partnership, led by the <AGENCY>, of federal grant-making agencies with a shared vision of enhancing customer service for the research community while streamlining and standardizing processes among partner agencies. <AGENCY> is leveraging its FastLane capabilities, experience, and expertise to deliver a menu of services for grantees to conduct business with federal agencies.

<AGENCY> occupies XXX.

The XXX (the Board) is the governing board of <AGENCY>. The Board is composed of 24 part-time members, appointed by the President, and confirmed by the Senate. They are selected on the basis of their eminence in basic, medical, or social sciences; engineering; agriculture; education; research management; or public affairs. The <AGENCY> Director serves on the Board ex officio. Other senior officials include a Deputy Director, who is appointed by the President with the advice and consent of the US Senate, and eight Assistant Directors.

In addition to the Board, <AGENCY> is divided into more than 50 organizational divisions that support various staff and program offices and is structured as follows:

* <AGENCY> Director
* <AGENCY> Deputy Director
* Five Staff Offices serving the Office of the Director
* Seven Directorates
* Two functional Offices oriented to financial or administrative support areas

More information about the <AGENCY> can be obtained at: <Website Reference and Link has been removed to avoid identifying the Originating Agency>.

## Organizational Background

The Contractor will provide support to the <AGENCY> XXX. The mission of XXX is to provide information systems, human resource management, and general administrative and logistic support functions to the <AGENCY> community of scientists, engineers, and educators as well as to the general public. XXX is responsible for <AGENCY>-wide information technology (IT) systems as well as the infrastructure necessary to support these systems.

The XXX has primary technical responsibility for the technical direction of the work described herein. XXX is responsible for <AGENCY>-wide IT systems development and maintenance as well as the infrastructure necessary to support these systems. The division is composed of approximately 60 federal employees and approximately 300 contractors. In addition to serving the program offices at <AGENCY> through existing major applications such as Research.gov, eJacket, the Proposal and Reviewer System (PARS), FastLane, and other grant management applications, XXX-managed systems also serve specific proponent organizations such as XXX.

XXX is presently organized into seven Branches, as listed below:

* Administrative Systems Branch (ASB): Provides application systems development and related services supporting <AGENCY>’s administrative functions.
* Customer Support and Assessment Branch (CSAB): Serves as the single point of contact (POC) for customer service and provides new technology assessment and desktop management services.
* External Systems Branch (ESB): Provides application systems development and related services supporting the external community dealing with <AGENCY> in program areas.
* Infrastructure Management Branch (IMB): Provides database management support as well as large system and client/server operations.
* Research Directorate Systems Branch (RDSB): Provides application systems development and related services to support <AGENCY>’s program areas.
* Security, Architecture, Policy and Plans Branch (SAPPB): Provides support for agency- wide information technology initiatives in the areas of security, enterprise architecture (EA), policy and plans, investment planning, and management.
* Telecommunications Branch (TCB): Provides support in data communications (LAN, Internet, etc.) and voice communication (telephone, voice mail, cable plant, etc.), email and related areas, and disaster recovery support.

## Environment

<AGENCY> has a total workforce of approximately 1,900 at its XXX headquarters, including approximately 1,300 career employees, 200 scientists from research institutions on temporary duty, and 400 contract workers. <AGENCY>’s population is varied and is heavily staffed by senior scientists. Nearly one-third of the senior scientists are on temporary (term) duty of 1-2 years’ duration at <AGENCY>. Consequently, <AGENCY> has many employees who are sophisticated in computing, are pressured by their short tenure, and must learn the environment quickly to be productive. <AGENCY> also has a segment of staff, whether temporary (term) or permanent, who tend to explore and test new tools. Although the ultimate goal is to provide a standardized desktop computing environment, central computing services must remain flexible and accommodate the corporate culture.

<AGENCY> supports a heterogeneous desktop environment; however, the most common standard configuration desktop computer is a personal computer (PC) running Windows XP that is configured via an <AGENCY> standard “image,” Microsoft Active Directory Group Polices, and an <AGENCY> “standard boot” network login procedure to meet the Government-wide Federal Desktop Core Configuration as well as <AGENCY>-specific requirements.

<AGENCY> standard software applications are accessed by users via WinStation, an

<AGENCY>-developed menu system. <AGENCY> primarily uses a combination of Commercial-off-the-Shelf (COTS) products and WinStation to install and update standard software. <AGENCY> also supports Macintosh desktop computers and iPads for numerous staff.

<AGENCY>’s technological infrastructure and applications are in a state of transition. It will be critical for the Contractor to provide the security-related expertise and leadership to drive these transformation initiatives as well as adapt and evolve their services and resource and support model to reflect the changes in requirements that these transitions bring to the organization.

Contractor leadership will be crucial in the planned transformation initiatives listed below:

* <AGENCY>’s standard set of application development tools is evolving from the Sun Application servers to Oracle WebLogic Application servers; from client-server applications to thin client (Web) interfaces; and with respect to database management, <AGENCY> is moving from Sybase’s database management server to Oracle.
* <AGENCY> intends to migrate the current on-site data center to a consolidated external service provider and leverage an Infrastructure as a Service (IaaS) operating model.
* <AGENCY> is in the process of transitioning to a commercially-provided Trusted Internet Connection (TIC) in the first half of XXX. <AGENCY>’s migration will satisfy requirements of OMB Memorandum M-08-05 and the Federal Information Security Management Act (FISMA) with the goal of improving its security posture and optimizing security with external network connections.
* <AGENCY> is actively evaluating transition of its email application and operations to a third-party hosted solution.
* <AGENCY> is working to plan, design, and transition its internal network to IPv6 protocol.
* <AGENCY> is working to ensure that it can proactively and effectively support changing desktop requirements while maintaining network security by restating and refining its desktop management approach.
* <AGENCY> is evaluating transitions to cloud computing and the Software as a Service (SaaS) model for its major business and grant management applications.

### Security Environment

<AGENCY> maintains a defense-in-depth security environment that provides successive security controls as a person progresses through the security architecture. The <AGENCY> maintains firewalls, intrusion detection systems, managed security services, and anti-virus/anti- spyware on the desktop. Laptops are encrypted for protection of data, Web traffic is filtered, and a security event/log management has been deployed. <AGENCY> maintains a vulnerability management program that is used to perform multiple scans each month and operates a mature process for ensuring that identified vulnerabilities are analyzed, reported, and addressed.

### Cultural Environment

Support teams must to be able to communicate with <AGENCY> staff and customers on a wide range of technical questions. As <AGENCY> staff and customers represent a wide range of computer skills, levels of responsibility, and job pressures, it is important to be sensitive to customer perception, remain tactful in tense situations, and diffuse tensions and complaints. Support teams must listen attentively and patiently to a wide range of questions and requests; log them specifically and correctly; and respond with tact and consideration. Questions range from consultations that can be solved over the phone to very complex problems or questions that may require escalation to the appropriate specialist(s). Customer follow-up and proper closure is considered a necessary condition in the delivery of quality and timely customer service.

Customer satisfaction is paramount. <AGENCY> cannot stress enough the importance of our customer service support programs to ensure a positive customer experience.

### <AGENCY> Computing Environment and Technical Infrastructure Overview

#### Email

<AGENCY> primarily uses Microsoft Exchange Server with Outlook 2007 clients, and makes extensive use of email for communication between staff and with the outside academic and business communities. <AGENCY> also integrates voice mail with the email system, which allows customers to receive voice mail messages via their email inboxes on both desktops and mobile computers such as iPads, iPhones, and Blackberry devices. <AGENCY> is actively evaluating transitioning its internal email operations to a third-party hosted service.

#### Local/Wide Area Network

Most of <AGENCY>’s central and personal computer applications and files are accessed via the customer’s desktop over <AGENCY>’s internal network. Additionally, <AGENCY> maintains an external network to provide Internet connectivity for visitors and guests (e.g., scientists on various panels). The external guest network supports most of the 40,000-50,000 visitors <AGENCY> receives annually. Network file, print, application, database, and utility servers are located in <AGENCY> data centers. Network devices (e.g., routers, switches) are located in the <AGENCY> data centers and in communications equipment rooms located on the floors of <AGENCY>’s two Headquarters buildings, which are adjacent and essentially cabled as one building. <AGENCY> has two redundant DS3 connections to the Internet (each from a different Internet Service Provider) and a 300MB connection to Internet2. Additionally, migration to 1GB or higher redundant Wireless Area Network (WAN) connections to an off-site hosting site or sites are in progress and expected to continue. As discussed above, <AGENCY> is in the process of migrating to a TIC and the Contractor will be required to support that transition and ensure continuity of high-quality, secure Internet service.

#### Remote Access

Secure remote access to most applications is available to <AGENCY> staff while at off-site locations (e.g., on travel or at home). Remote access is provided through Access Workspace, a Virtual Private Network (VPN)-based service; Remote LAN Services (RLS), a Citrix-based service; and Outlook Web Access (OWA) for email access. Secure access is ensured with the use of SecurID tokens, which are provided to <AGENCY> employees, Contractors, and customers for authentication. <AGENCY> currently supports approximately 2,000 active and enabled SecurID tokens. Blackberry devices are supported for portable remote access and wireless services.

#### Phone/Voice Support

<AGENCY>’s voice system is composed of a Siemens Hicom 300 E Communications Server and associated hardware and software. Voice mail is provided through the Siemens Xpressions Messaging System, a unified messaging system that, in addition to providing traditional voice mail services via the telephone, integrates with Microsoft Exchange email to provide access to voice mail messages in Outlook and to email messages via the telephone.

#### Data Center

<AGENCY>’s on-site systems are located within the secured data center, which is staffed 24 hours per day, 7 days per week. The data center provides a controlled environment for the systems and acts as the focal point for system monitoring and customer services. <AGENCY>’s Operations Team provides operations support, production control, UNIX and Windows system administration, database administration, and hosting services for <AGENCY>’s corporate Web and database applications hosted on-site. The Operations Team ensures systems and services are working at all times except during scheduled outages; reports issues to the appropriate <AGENCY> and XXX personnel; and coordinates support with the agency’s off-site storage Contractor(s). <AGENCY> intends to migrate the current on-site data center to an external service provider(s). <AGENCY> is actively planning for the consolidation of its current data centers and is evaluating IaaS models to further transform, streamline and scalable operations.

#### Database Management

<AGENCY>’s internally developed central applications are based mainly on Sybase databases and reside on Sun Microsystems equipment running the Solaris Operating System. Microsoft SQL Server supports <AGENCY>’s COTS products (Siebel, Radia, Hercules, etc.) and is primarily based on servers running Microsoft Windows Operating System. <AGENCY> has selected Oracle as its next generation database management system to support both central applications and COTS products. The conversion from Sybase to Oracle is expected to be completed within 18 months.

#### Identity Management

<AGENCY> is implementing a phased identity management (IDM) solution that will eventually consolidate authentication and authorization information in the Corporate Directory using a COTS product. Services currently available under IDM include Unified Password, Single Sign- on, and Federated Identity. Identity Management relies upon the SUN JES product suite consisting of “Access Manager” and “Identity Manager” hosted on SUN Application and Web servers.

#### Transition to New Products and Systems

To minimize disruption to staff and customers, <AGENCY> prefers a gradual transition to new products and systems. In some cases, multiple versions of software may be available at the same time; for example, <AGENCY> currently uses both Microsoft Office 2003 and Office 2007 with Office 2003 being phased out. During the course of the contract, certain products may be removed from systems and standard menus and support for those products discontinued.

### Major Internal and External Applications

Descriptions of <AGENCY>’s major internal and external applications are provided in Appendix XXX.

# Objectives

## Support Objectives

The primary focus of this requirement is to ensure the security, confidentiality, integrity, availability, and restoration for the systems developed and operated by <AGENCY> XXX. This solicitation is also focused on acquiring security- and privacy-related leadership, guidance, and support. The Contractor will be responsible for developing the strategies and executing the transformation initiatives that will fundamentally alter the way <AGENCY>’s IT services are provided internally to employees and contractors and externally to its stakeholders and clients.

<AGENCY> must meet relevant directives issued by OMB, policy directives, and standards required by Government authority (e.g., TICs). <AGENCY> will also examine the feasibility and appropriateness of centralizing and consolidating data centers, moving applications to a virtual/hosted environment (i.e., SaaS), and moving infrastructure to a virtual/hosted environment (i.e., Infrastructure as a Service). The minimal objective of <AGENCY> is to maintain baseline security operations. Additional transformational objectives shall be to establish mechanisms for improving security services that meet or exceed regulatory requirements and industry best practices.

Prior to commencing ongoing activities the Contractor shall address baseline considerations:

* Quickly review, update, establish, and document security architectures for all platforms and service towers/ solutions creating formal baselines and measures.
* Quickly review, update, establish, and document security protocols, Security Technical Information Guides (STIGs), and Security Content Automation Protocols (SCAP) validation and compliance for all IT hardware and software.
* Quickly review, update, establish, and document processes for identifying vulnerabilities and facilitating appropriate changes across all information platforms and applications.

The Contractor shall maintain an adaptive posture, but establish methods for rigid analysis and implementation. At all times, security solutions and services shall meet <AGENCY> EA policies, standards, and procedures [see, Section [4](#_bookmark32) of this document].

## Partnership Philosophy

In addition to meeting the objectives listed above in Section XXX and the requirements outlined in this SOW, the Contractor is encouraged to:

* Provide for continuous improvements so as to consistently advance awareness and understanding of Security to <AGENCY>’s business and technical issues;
* Continuously seek to improve on the effectiveness and efficiency of the services delivered; and
* Work collaboratively with other Contractors, Government agencies, and business partners.

## Staffing

<AGENCY> desires leaders and experts capable of proactively identifying, promoting, implementing, and communicating the advancement of information security and privacy. As such, the Contractor is encouraged to:

* Provide a team of experienced resources that can fulfill a variety of activities ranging from subject matter disciplines and research to expertise and skills in planning and implementation. Desirable attributes include (but are not limited to): addressing regulatory impact and compliance (e.g., FISMA); systemic/integrated views in planning and managing changes across the enterprise; addressing methods for maturing areas such as vulnerability management, intrusion detection, and effectiveness of training and security policies; and other technical disciplines needed to attain objectives.
* Provide flexibility in resources assigned. That is, where appropriate, maintain continuity through a permanent mix of senior-, mid-, and junior-level staff experienced in supporting requirements in an environment similar to the size and complexity of the <AGENCY>. However, as technologies change, <AGENCY> expects that the Contractor will maintain alignment by adjusting permanent resources and/or providing ad hoc expertise for projects and other short-term assignments.
* Establish continuous support and continuity through cross-training to ensure there are no impacts due to planned or unplanned staff changes.
* Be proactive in establishing operational guides that document the <AGENCY> organization, responsibilities, and processes that can be used to train resources, transfer knowledge, and create the basis for knowledge management.

# TASKS AND DELIVERABLES

## Program and Project Management (CLIN 1)

The Contractor shall provide program and project management services for work required by this SOW. This includes, but is not limited to, leadership and management oversight, administration, planning, scheduling, and controls for projects. The Contractor shall be responsible for managing the work performed under this contract, supervising its personnel and Subcontractors, and taking appropriate corrective measures for all performance-related problems in the course of performing assigned duties. The Contractor shall proactively and routinely assess performance and provide recommendations on process improvement, organizational design, and systems implementation to enhance <AGENCY> security and privacy goals.

The Contractor shall assign a senior, experienced Program Manager and Deputy Program Manager to lead and oversee projects, products, and services performed under this contract. The Program Manager shall be responsible for directing and ensuring quality of work performed, briefing XXX executives, and providing thought leadership across a range of security and privacy subject areas. The Program Manager shall act as the central POC with the XXX senior leadership, COTR, and any other Government employees or other XXX Contractors at the direction of <AGENCY>. The Program Manager shall have direct accountability for the technical correctness, timeliness, and quality of services performed and products delivered.

### Program Management Plan (PMP) and Project Plans

The Contractor shall develop a PMP that outlines the approach to managing the work contained in this SOW. The PMP shall address the management and technical approach to delivering high- quality services within established timeframes. Additionally, the PMP shall reflect the concept of operations and phases by which transformation will occur. It is recognized that high levels of organizational maturity will take time and that project plans will require adjustment as policies are institutionalized and organizations adjust. As such, the primary role of the PMP is to aid the orderly transformation of all areas of scope through the use of programmatic tools and techniques.

At a minimum, project plans shall address critical activities, sources and resources, dependencies, budget estimates, key milestones, and schedules showing planned activities. Project plans shall also identify key stakeholders and organizations, and interface mechanisms to ensure all teams understand their inputs, outputs, and responsibilities.

#### Deliverables

* Draft PMP
* Final PMP
* Annual updates to the PMP
* Project Plans

### Quality Assurance Plan (QAP)

The Contractor shall develop and implement an integrated QAP. The QAP shall discuss the technical procedures and controls for evaluating and managing quality of work products and activities under this SOW. The QAP shall define measures and metrics aligned with capturing values on organizational performance, and as elements of security policy and management (resulting from this SOW) are applied.

#### Deliverables

* Draft program-level QAP
* Final program-level QAP
* Annual update of QAP

### Risk Management Plan (RMP)

The Contractor shall follow best practices and <AGENCY> guidance in establishing and implementing a program-level RMP, including the processes and artifacts for identifying, assessing, mitigating, and reporting on program-level risks. At the project level, risk management shall include, but is not limited to, the creation and maintenance of a Risk Register to support the identification, quantification, and ranking of all identified risks and tactics for management of each risk.

#### Deliverables

* Draft program-level RMP
* Final program-level RMP
* Annual update of the RMP
* Project-level Risk Registers
* Quarterly updates to project Risk Registers

### Project Monitoring and Control

The Contractor shall use Microsoft Project to simplify and automate, to the greatest extent possible, project planning and distribution of project schedules, including the capability to track and manage tasks and milestones. The Contractor shall provide a version control process for all project schedules that are required to be baselined. The Contractor shall provide a detailed report of the actual expenditures by project Work Breakdown Structure (WBS) element in sufficient detail to track actual expenses as a percent of the overall plan on a monthly basis. The Contractor shall prepare and submit weekly and monthly status reports that address the activities under this contract. The format of the reports shall be defined by the <AGENCY>. In addition to the weekly and monthly status reports, the Contractor shall prepare and submit ad-hoc analysis as directed by the COTR to support the management of contract and project schedules and costs.

#### Deliverables

* Monthly Program Status Report
* Weekly Project Status Report
* Other management reports as requested

### Meetings

To ensure that the current status, projected trends, and proposed future changes are fully understood by all parties, the Contractor shall prepare for, attend, and document the following scheduled meetings, as well as any ad-hoc or special project meetings.

* Daily Tag-Up: The Contractor’s Program Manager and Operations Manager will meet with senior XXX officials every morning to review any major issues.
* Weekly Status: The Contractor’s Project Managers will meet with the COTR or <AGENCY> task leads weekly to review project status and any issues.
* Monthly and Ad-Hoc Contract Reviews: The Contractor’s Program Manager will meet with the COTR and XXX senior management to review status of projects and contract performance issues.

#### Deliverables

* Meeting calendar
* Meeting materials including Action Items
* Meeting Minutes and Action Items

## Contingency Planning (CLIN 1)

OMB A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Automated Resources,” requires the preparation of plans for general support systems and major applications to ensure continuity of operations. The Contractor shall provide support in preparing for IT security contingencies (e.g., denial of service, intrusions, malware), and other eventualities and disruptions that have an impact on critical systems and business functions.

The Contractor shall use authoritative sources and standards (e.g., NIST 800-34) to prepare and plan for contingencies and disasters. At a minimum, the Contractor shall provide:

* Emergency response plans.
* Backup operations plans.
* Protection of systems for both critical and general support.
* Assurance that Federal Continuity Directives are addressed.

The Contractor shall provide the leadership and support required in planning sustainment activities necessary to ensuring that critical activities are prioritized correctly, event scenarios are examined, and considerations for readiness and alternatives are planned. Issues consist of, but are not limited to, tracking whether <AGENCY> information systems have mitigated their weaknesses on time using the appropriate processes, tracking ATO expirations, tracking completeness of annual requirements such as 800-53As and Contingency Plan Test Results, and validating the quality of <AGENCY> system artifacts.

Personnel shall possess knowledge of IT security requirements, technical security countermeasures, risk management methodologies, contingency planning, and data communications networking in unclassified and classified environments.

Personnel shall provide regular briefings to the ISO and XXX senior management upon the successful completion and subsequent updates of System Security Plans, Contingency Plans, FIPS 199, and E-Authentication Workbooks.

The Contractor shall:

1. Devise methodologies for testing <AGENCY> organizational readiness and/or compliance with regulations on a continual basis.
2. Assist functional groups in identifying risk to <AGENCY> operations and compliance with regulations (e.g., FISMA).
3. Assist <AGENCY> in executing an annual Information Security Performance Plan.
4. Asses the sufficiency of <AGENCY> enterprise-wide tools and processes used in Risk Management Systems (RMS), quality controls, and information assurance (IA).
5. As requested by the COTR, create ad-hoc briefings and reports pertaining to daily, weekly, monthly, and/or annual compliance to readiness activities.
6. Assist with updating and executing the <AGENCY> FISMA Program.
7. Review Certification and Accreditation (C&A) documentation as drafts are prepared.
8. Review and validate security artifacts to ensure that they are sufficient in preparing the <AGENCY> to address known contingencies.
9. Facilitate semi-annual service recovery and application contingency status reviews.
10. Perform semi-annual updates to service recovery plans.
11. Perform semi-annual updates to application contingency plans.
12. Perform semi-annual service recovery testing.
13. Provide inputs to security training as directed by COTR.

### Deliverables

* Service and Application Recovery Plans Reports and updates
* Risk Management Plans, Contingency Plans, and plan updates
* Updated Business Impact Analysis (BIA)
* Regular briefings and reports regarding status of contingency activities
* Documentation of Lessons Learned

## COMSEC Support (CLIN 1)

The Contractor shall provide personnel, cleared at the appropriate levels and possessing requisite training to provide <AGENCY> with technical and administrative support for COMSEC accounts at <AGENCY>. The Contractor’s COMSEC personnel shall have the custodial and management responsibility for all COMESEC customer support through walk-in service at the <AGENCY>’s XXX location, and via email, and telephone.

As part of its custodial responsibility, the Contractor shall coordinate updates and changes with the sponsoring Agency in performing equipment moves, coordinate the replacement of assets, maintain Agency documentation, and maintain up-to-date keys. Custodial personnel shall be available during the prime work hours of 8AM EST - 5PM EST and available on-call after hours.

The Contractor shall:

1. Maintain clearances and immediately report security incidents affecting the status of Agency assets or incidents that are detrimental the affairs of <AGENCY>.
2. Manage existing equipment and procure additional equipment as directed by the COTR.
3. Procure Top Secret capable equipment as directed by the Government as an Other Direct Cost (ODC).
4. Conduct quarterly validation testing of secure cell phones, fax machines, and email equipment.
5. Conduct annual training for ~10 individuals on the use of COMSEC capable equipment and in changes to security policies affecting custodial management.
6. Maintain and manage an Electronic Key Management System (EKMS) Local Management Device/Key Processor (LMD/KP) System Manager for:

* configuration management, software upgrades, and system equipment certification;
* troubleshooting and daily operational status;
* key ordering/transfer to sub-account LMDs; and
* associated security procedural directives and training issued by National Security Agency (NSA) national policy and National Reconnaissance Office (NRO).

1. Interface with the EKMS Help Desk and secure communications Contractors as required for all COMSEC activities.
2. Attend all training required and authorized by the COTR necessary to be in compliance with Agency policies.
3. Conduct inspection of secure communication facilities within <AGENCY> and those facilities that operate within the framework of <AGENCY>-controlled COMSEC programs at other federal and state agencies.
4. Evaluate inspections and approval from a physical security standpoint for the operation, maintenance, and storage of COMSEC equipment and/or material in accordance with NSTISS 4005, Safeguarding COMSEC Facilities and Materials.
5. Assist in the establishment of new COMSEC accounts within <AGENCY>.
6. Review Continuity of Operations (COOP) and exercise support requirements, providing COMSEC support for COOP exercises.
7. Serve as the officially appointed courier for all categories and classifications of COMSEC material and equipment.
8. When authorized by the COTR, attend national conferences and other professional forums with NSA, other Government or civil agencies, and the Department of Defense on IA, Information Security, Cryptographic Modernization Programs, and other COMSEC issues.
9. Keep accurate COMSEC training records for OIT and assist with COMSEC inquiries and investigations on physical insecurities and incidents involving <AGENCY> COMSEC accounts or cryptographic keying material for which <AGENCY> COMSEC account has been designated the Controlling Authority.

### Deliverables

* Quarterly evaluation of equipment and inventory status report to <AGENCY> COTR
* COMSEC Inventory Reports to Agency no less than every 6 months, or as required by Sponsoring Agency
* Semi-annual training course for required individuals (less than 10)
* Weekly COMSEC Destruction Report
* Monthly trouble ticket and service metrics report

## Vulnerability Management and TIC Performance Management (CLIN 3)

The Contractor shall lead efforts to collect and analyze intelligence regarding cyber threats and vulnerabilities, and direct and coordinate the response to such threats and vulnerabilities using the latest methods and tools available with the approval of the <AGENCY> ISO. The Contractor shall have responsibility for identifying, testing, and promulgating security patches as directed by the ISO. In cases where third parties develop, support, or maintain <AGENCY> applications and infrastructure, the security Contractor shall exercise vulnerability management activities through the COTR and/or ISO or other Government staff as directed. The main purpose of such activities is to be proactive and prevent <AGENCY> systems and data from exploitation. In support of these activities, The Contractor shall manage and enhance the vulnerability and patch management process for <AGENCY>. The Contractor shall also provide leadership and guidance to support the transition to the TIC provider and migration of vulnerability management to the TIC provider. The Contractor shall design an approach to periodically monitor, validate, and audit the service received from the TIC to ensure <AGENCY> policies have been implemented and the service provided by the TIC satisfies requirements and specifications that have been agreed upon with the <AGENCY>. The Contractor shall:

1. Maintain a current understanding of <AGENCY> IT systems and architecture, IT policies on use, access, refresh, configuration control, how cross-functional support is applied, and access by operational groups.
2. Monitor various information sources such as SCAP at NIST.GOV for specification and information on technologies.
3. Research external sources (including public, private, and classified sources) and peers’ information on threats and vulnerabilities and their solutions.
4. Develop the vulnerability and incident status portion of the Daily Tag-up Report using <AGENCY> vulnerability management tools.
5. Functionally manage and administer <AGENCY> Vulnerability Management tools and conduct scans on <AGENCY> COTS as well as internally developed systems.
6. Take immediate and appropriate counter measures upon knowledge or discovery of threats.
7. Immediately analyze threats and vulnerabilities to determine their severity level and impact on <AGENCY> systems.
8. Report high-level threats within 15 minutes and low-level threats and vulnerability findings within 4 hours to the ISSO and COTR.
9. Consult with the ISSO and COTR for determining the release of patches or before authorization is given to third parties.
10. Manage and enhance the vulnerability and patch management process for <AGENCY>.
11. Participate in patch management activities with Information Technology Help Central Services (ITHCS) and network administrators.
12. Periodically evaluate and recommend improvements to tools and procedures.
13. Collaborate with the ITHCS and network teams to resolve vulnerabilities.
14. Report procedures and requirements among the participating peers and approved forums.
15. Manage the <AGENCY> Acceptance of Residual Risk (AORR) process.
16. Monitor and audit service received by the TIC provider.

### Deliverables

* Security and Incident Reports for Daily Tag-Up meetings
* Quarterly evaluation of vulnerability and patch management tools and procedures
* Vulnerability Assessment and Priority Reports
* Standard Operating Procedures (SOPs) for the vulnerability and patch management process
* SOPs for AORR
* Monthly TIC performance management reports

## Certification and Accreditation (CLIN 2)

Compliant with NIST Publication 800-53 and Special Publication 800-53A the Contractor shall lead efforts to establish a standardized and repeatable process to assess the effectiveness of security controls in <AGENCY> information systems. The assessment methods and procedures shall be capable of determining if security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the organization.

The goal is to make use of standardized assessment procedures to promote more consistent, comparable, and repeatable security assessments within <AGENCY>. However, the assessment procedures in Special Publication 800-53A may be supplemented1 as needed based on an organizational assessment of risk. The Contractor shall identify needs for additional assessment procedures for those security controls not contained in NIST Special Publication 800-53.[[1]](#footnote-1)

The Contractor shall lead efforts to create, manage, and maintain the C&A documents and process at <AGENCY>. Knowledge of Department of Justice Cyber Security and Asset and Management (CSAM) tool is desired. As directed by the Government, the Contractor shall:

1. Design and execute a C&A activities program, including but not limited to, C&A artifact maintenance, continuous monitoring and Plan of Action and Milestones (POA&M) management support, testing C&A tools, analyzing <AGENCY> requirements, editing pertinent trainings, and supporting risk management with vulnerability management or other related duties that will attain a “GREEN” score.
2. Serve as primary certifier and liaison for all C&A efforts and ensure ISSOs complete a FIPS-199, PTA, E-Authentication Workbooks, CPs, CPTRs, SSPs, and 800-53As.
3. Personally deliver Risk Assessments (RAs), System Test and Evaluation (ST&E) Plans, Security Assessment Reports (SARs), and Authority to Operate (ATO) Letters.
4. Perform the C&A lifecycle for on-site applications.
5. Perform the C&A lifecycle for hosted applications at third-party locations.
6. Perform all phases of ST&E Planning.
7. Perform POA&M tracking and reporting.
8. Perform inventory and classification of information systems.
9. Provide risk assessment support of <AGENCY> applications.
10. Develop unified guidelines and procedures for conducting certifications and/or system- level evaluations of federal information systems and networks, including the critical infrastructure of <AGENCY>.
11. Ensure that IT systems have all security controls in place and that the all controls function properly in accordance with NIST 800-53A.
12. Assist with external/internal audits such as the OMB A-123 for designated systems.
13. Advise the Government on new standards and make recommendations on new IT security technologies to improve efficiencies.
14. Maintain the Requirements Traceability Matrix (RTM) with results of ST&E.
15. Perform Risk Analysis.
16. Maintain a Security Accreditation Report.
17. When required and authorized by the COTR, attend security training.
18. Advise ISSOs on successful completion of FIPS-199, PTA, E-Authentications, CPs, CPTRs, SSPs, and 800-53As.

### Deliverables

* Security Controls Validation Test Report (control tests performed in years not requiring a C&A).
* RA
* SSP
* SAR
* ST&E Plans
* POA&Ms – currently less than 50 annually
* Regular POA&M status reports
* Complete set of C&A documentation as required by NIST-800-37 and <AGENCY> during the 90-120 day timeframe, depending on system complexity– currently 7-10 systems annually
* ATO Letters
* Audit documentation as requested

## Privacy Services (CLIN 2)

<AGENCY> recognizes the importance of protecting the privacy of employees, customers, partners, and Contractors especially as it modernizes its IT systems. <AGENCY> seeks to leverage government and industry best practices to assess privacy protection needs and effectively identify and implement sound privacy practices to strengthen and establish a leading edge Privacy Program. A strong and multi-faceted privacy program helps an agency consider privacy when making business decisions and may include the fundamental building blocks of a robust program such as the elements of the Federal CIO Council Privacy Committee’s *Best Practices: Elements of a Federal Privacy Program.*

To support privacy program enhancement the Contractor should demonstrate leadership and knowledge of industry best practices in developing and enhancing privacy programs. Leadership and resources will enable <AGENCY> privacy program to fully meet the growing number of legal, regulatory, policy, technology, and operational challenges posed by an organization’s increasing demand for the collection and use of sensitive information. Challenges to privacy include the expanded use of web-based, social media technologies in existing information and communication models for individuals, government, and business. Privacy training and awareness programs are key elements of building a culture of privacy throughout an organization. Training programs reinforce the implementation of privacy policy, providing a critical element of an effective privacy program to improve privacy management and reduce the risk of privacy incidents.

Privacy issues must also be addressed when systems are being developed, and privacy protections must be integrated into the development lifecycle of these automated systems. The vehicles for addressing privacy issues in a system are a Privacy Threshold Analysis (PTA) for systematically assessing the privacy impacts of IT systems and a Privacy Impact Assessment. The PTA is performed to determine whether an activity involves personally identifiable information and whether a PIA is required and whether an existing System of Records Notice (SORN) covers a particular collection. The PIA process provides a means to assure compliance with applicable laws and regulations governing an individual’s privacy. The Contractor shall lead privacy impact assessments as directed by the COTR.

The Contractor shall assist in establishing a strategic privacy framework program with the aim of reducing privacy risks, while also fulfilling legal and regulatory requirements. Within the areas of program enhancement, risk management, information security, privacy training and reporting and compliance the Contractor shall:

### Privacy Program Enhancement

* Identify best practices and common activities.
* Identify innovative solutions to common problems.
* Identify policies, procedures, and privacy documentation consistent with applicable laws and regulations.
* Assess compliance with federal laws, regulations, and policies relating to privacy protection and effectively identify sound privacy practices.
* Evaluate legislative, regulatory, and related policy proposals implicating privacy issues.
* Facilitate the agency’s privacy compliance efforts by reviewing privacy procedures to ensure that they are comprehensive and current.

### Risk Management

* Plan, design, and conduct Privacy Threshold Assessments and Privacy Impact Assessments.
* Lead, write, and review Privacy Impact Reports.
* Identify any issues or risks to privacy.
* Develop plans and tactics to address issues exposed during the assessments.
* Evaluate new technologies, programs, online activities, contracts, regulations, and legislation for potential privacy impacts, and advise on implementation of privacy protections.
* Identify how privacy can be addressed from the beginning of program design and throughout the System Development Life Cycle (SDLC).
* Develop and implement systems or tools for assessing the privacy impacts of all new and existing systems and programs.

### Information Security

* Inform the agency of current statutory and regulatory privacy protection requirements for personally identifiable information.
* Coordinate agency privacy information and communication program with the agency’s security program to ensure a consistent privacy/security message across the agency.

### Privacy Training

* Identify appropriate training and education.
* Develop privacy training techniques and ensure that it addresses compliance with the Privacy Act, E-Government Act, other privacy-specific requirements and guidance, and organization policies, procedures.

### Privacy Reporting and Compliance

* Provide privacy program metrics and related information required to meet the agency’s Federal Information Security Management Act (FISMA) privacy reporting requirements.
* Provide support and documentation for the FISMA privacy reporting requirements.
* Facilitate and support Privacy impact reviews and briefings.

### Deliverables

* Privacy Threshold Analysis
* Privacy Impact Assessment Reports
* Privacy Impact briefings
* Privacy program assessment and recommendations for enhancement
* Plans and tactics to address privacy issues
* Privacy Act System of Records Notices (SORNs))
* Documentation support for the FISMA annual privacy reporting requirements
* Reports that identify key information assets and privacy implications, as well as the creation or revision of agency privacy policy

## Independent Security Assessment Review (CLIN 1)

Twice each year, <AGENCY> engages an independent third party to validate its security posture, the sufficiency of <AGENCY> security processes, and the effectiveness of its controls. The Contractor shall lead reviews and provide expert recommendations for improvements to <AGENCY> security processes and technology. The Contractor shall also provide recommendations on how to incorporate these improvements into project plans.

The Contractor shall:

1. Cooperate with personnel conducting the assessment and accommodate requests for documentation.
2. Observe and adhere to all security rules and restrictions governed by <AGENCY> policy, Non-Disclosure Agreements (NDA), and restrictions against the disclosure of classified information.
3. Analyze the findings of each Security Assessment and make recommendations for improvement to security processes and activities. Where a business case is necessary to the decision process, the Contractor shall identify participating resources/functions and provide the format/outline for the business case.

### Deliverables

* Documentation support as requested during the Independent Security Assessment.
* Analysis and recommendations for improvement based on findings of the Independent Security Assessment.
* Recommendations on incorporating improvements into project plans.
* Format and outline of business cases as necessary.

## Policy, P (CLIN 3)

The Contractor shall lead the development and enhancement of <AGENCY>’s IT privacy and security policies, plans, and SOPs with the goal of developing a secure <AGENCY> environment based on mature methods for rigid analysis, maintaining system integrity and IA, and a prescriptive and proactive posture.

Privacy and security policies and planning are intended to facilitate compliance by <AGENCY> organizations, third-party organizations supporting <AGENCY> systems, when exchanging data, or when accessing external systems and websites by communicating and promulgating standards, policies, and documentation concerning security protocols, Security Technical Information Guides (STIGs), and Security Content Automation Protocols (SCAP) validation and compliance for all IT hardware or software. The Contractor shall:

1. Assist in the development, and facilitate <AGENCY> approval, of IA and IT security documentation, including directives, policies, standards, processes, and procedures for governance use.
2. Maintain regular updates to the Management Directives and IT Security Handbooks addressing both unclassified and classified environments.
3. Collaborate in the development of <AGENCY> IT privacy and security policies and procedures in accordance with federal mandates.
4. Provide architecture guidance to <AGENCY> system owners as needed, participate in IT privacy and security meetings and briefings, attend EA meetings, and support ISSO briefings as required.
5. Create, update, and enhance privacy and security strategies, plans, and procedures.
6. Assist the <AGENCY> ISSO, Privacy lead and CIO in prioritizing security activities and identifying criteria for monitoring results.
7. Identify the impact of new Government laws/regulations and the implementation of new IT technologies on <AGENCY> IT security and privacy policy based on policy inquiry and questions received. Assist in the subsequent evolution of the policies.
8. Provide policy expertise and support in waiver/exception requests and policy inquiries.
9. Support IT security and privacy outreach efforts to enhance <AGENCY> enterprise-wide awareness.
10. Assist in the development of new <AGENCY> classified systems and COMSEC IT Security Policy.
11. Create, maintain, and continually update a Web portal for Policies and FAQs.
12. Maintain familiarity with Government law and directives for conversion into useful <AGENCY>-level policy and other governance documentation.
13. Assist in the development of training materials by providing input concerning new policies, user requirements, and metrics.
14. Provide audit support (e.g., OMB A-123, FISMA).
15. Provide support, coordination, and input for OMB and DHS data calls (e.g., TIC, DNSSEC) regarding <AGENCY>’s IT security and privacy policies.
16. Provide security assessments and analysis as requested by <AGENCY> and provide input for functional requirements (e.g., facility review, capability assessments, operational review, Contractor analysis).
17. Provide security resources for special projects as directed by the COTR.
18. Participate in Change Control Board (CCB) meetings and conduct IT security product reviews, research, and/or studies as directed and produce reports to the <AGENCY> CCB for review.
19. Perform feasibility assessments for implementing standards and security programs such as the ISO 27001standard. Provide reports discussing the benefits of implementation, including a Return on Investment analysis.
20. Conduct surveys and reports of historical policy impacts from incident logs, provide feedback to the COTR, and assist in the initiation of new policies and procedures accordingly.
21. Support the development of miscellaneous policy letters, memorandums, and monthly briefings and associated documentation for distribution as required.

### Deliverables

* Weekly progress reports
* Documented overall IA and IT security governance processes
* Regular updates to the Management Directives Handbook
* Regular updates to the IT Security Handbook
* Meeting support and documentation as requested such as presentation development and meeting minutes
* Documented security plans and procedures
* Recommendations for improving to security plans, policies, and procedures
* Security policy analysis and impact reports
* Maintain a Policy branch mailbox log and provide monthly status reports
* Regular updates to the Policies and FAQs Web portal
* Lead execution of OMB and DHS data calls related to security topics
* Reports on IT security product reviews, research, and studies as requested
* Standards and security program feasibility assessments and accompanying ROI analysis
* Additional support and materials as requested to support security training, outreach and awareness, audits, the CCB, and other relevant activities and efforts
* Conduct periodic surveys to understand user experience related to security issues

## FISMA Controls and Continuous Monitoring (CLIN 3)

FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, Contractor, or other source.

Within <AGENCY>, FISMA compliance is intended to ensure that <AGENCY> can pass federal regulatory requirements and achieve better compliance ratings. The Contractor shall provide the support services required to execute day-to-day FISMA operations and ensure that all FISMA activities are prioritized correctly, completed on schedule, and in accordance with the National Institute of Standards and Technology (NIST) SP 800-53 and NIST SP 800-171.

<AGENCY> policies. The Contractor shall research major <AGENCY> obstacles related to the federal changes to FISMA requirements and coordinate closely with the personnel responsible for the tasks listed in the Policy and Contingency sections of this SOW.

These issues consist of, but are not limited to, tracking whether <AGENCY> information systems have mitigated their weaknesses on time using the appropriate processes, ATO expirations, tracking completeness of annual requirements such as 800-53As and Contingency Plan Test Results, and validating the quality of <AGENCY> system artifacts. FISMA activities are mandated by, and must be executed according to, the <AGENCY>’s Information Security Performance Plan for each fiscal year.

The Contractor shall lead and perform continuous monitoring of system configuration components, conduct security impact analyses of changes to the system, execute ongoing assessment of security controls, and provide status reports. The Contractor shall perform regular scans and assess <AGENCY> assets that are connected to the <AGENCY> networks, and present timely reports to the security management team.

The Contractor shall provide leadership and subject matter expertise at all FISMA-related briefings and meetings. The Contractor shall:

1. Lead and execute day to day FISMA operations to improve <AGENCY>’s security posture.
2. Functionally manage the tools used to provide continuous monitoring of FISMA security control set (i.e., Tenable Security Center and NitroSecurity).
3. Provide quarterly recommendations to improve the continuous monitoring process to IT Security Manager.
4. Provide authoritative vulnerabilities remediation recommendations.
5. Perform tracking of elevated access.
6. Post updated information on results to the SharePoint as required.
7. Lead execution of periodic FISMA audits (no less than once per year) and provide feedback to functional groups on the issues affecting compliance by <AGENCY>.
8. Research the major obstacles related to federal changes affecting <AGENCY> compliance to FISMA requirements.
9. Review and validate security artifacts uploaded to the FISMA tool.
10. Advise and assist with changes to the FISMA Inventory and recommend changes to the Trusted Agent FISMA (TAF)/Risk Management Systems (RMS).

### Deliverables

* Periodic reports, defined by the annual <AGENCY> Information Security Performance Plan, POA&Ms, detailing the accuracy, quality, and timeliness of all artifacts uploaded in the FISMA tool. Reports shall detail the mitigation progress for system weaknesses to include trending analysis and non-compliance issues for all information systems throughout <AGENCY>.
* Security impact assessments as events occur.
* Daily, weekly, monthly, and annual status reports as required.
* Quarterly recommendations to improve monitoring processes.
* In-Progress Reports (IPRs) for projects and meeting summaries for submission to the ISSO and CIO.

## Intrusion Detection, Incident Response, and Forensic Analysis (CLIN 3)

The Contractor shall lead efforts to monitor automated intrusion detection systems and develop effective strategies for abating or mitigating associated risks and incidents that are identified by the systems. The Contractor shall monitor for vulnerabilities such as those that can be exploited by external and internal threats, users exceeding authority, and other forms of unauthorized access. The Contractor shall manage and enhance the computer incident response and intrusion detection process. The Contractor shall perform inappropriate material scans and conduct forensic analysis to examine digital media in a sound manner with the aim of preserving, recovering, analyzing, and presenting facts about the inappropriate material. The Contractor shall:

1. Manage and monitor <AGENCY> BlueCoat Content Management tools until content filtering is transitioned to the TIC.
2. Serve as the primary POC for Managed Security Service monitoring, alerts, etc.
3. Provide 24x7 monitoring and incident response capabilities, call escalation procedures, and Web-accessible audit logs.
4. Provide vulnerabilities remediation recommendations.
5. Assist in the deployment of additional intrusion detection capability.
6. Manage the backup for the <AGENCY> internal intrusion detection system SNORT®.
7. Provide support during computer security intrusion/incident investigations.
8. Support <AGENCY> implementation of desktop Host Intrusion Prevention Systems (HIPS), Control, and other desktop security management tools.
9. Establish the objectives and data to be searched to determine whether inappropriate material exists within the <AGENCY> network.
10. Establish target systems along with identifying any special considerations; determine <AGENCY> preferred scanning windows if applicable.
11. Create responses to audit Notice of Findings (NFR) and Provided by Client (PBC).

### Deliverables

* System administration status reports
* Develop responses to NFR and PBC audit findings.
* Incident status reports and recommendations for remediation tactics.
* Quarterly recommendations for blocked categories.

## Transition (CLIN 1)

### Transition In

The transition preparation and phase-in period shall be 45 calendar days. During this period, the Contractor shall plan and manage those activities necessary to transition service from the existing service provider. Immediately after the notice to commence work, the Contractor shall perform due diligence through inventory of all <AGENCY> assets, system configuration information, current operations, and documentation. The Contractor shall document and provide findings to the Government in a Transition Plan. The plan shall include what has been accomplished related to the transition and what remains outstanding, including any issues that need to be addressed. During the first half of the transition period the incumbent shall maintain responsibility for security and privacy operations. During the second half of the transition, the Contractor shall be responsible for maintaining the continuity of security and privacy operations and quality of service. Objectives for transition include:

* No break in current service levels.
* No delay in support for new and ongoing projects.
* Existing <AGENCY> projects shall continue as is unless changes are directed by the Government.

During the phase-in period, the Contractor shall organize, plan, and recruit personnel for remaining outstanding positions as well as mobilize resources, develop procedures, and accomplish all actions necessary to commence full performance of the services at the end of the transition period. During the phase-in period, the Contractor shall:

1. Establish project management procedures and review SOPs.
2. Recruit, hire, and on-board necessary personnel.
3. Attend post-award meetings as required.
4. Create SOPs for each functional area covered under this SOW unless otherwise provided by the Government. Content may include: Quality Control (QC), work assignments, approval authorities, workflow, functional relationships between the Government and the Contractor, functional relationships between the Contractors’ organizational elements (including Subcontractors), and any other information needed for efficient and uniform performance.

#### Deliverables

* Draft Transition Plan
* Final Transition Plan
* Staffing report
* Daily status report
* SOPs for each SOW functional area
* Updates to existing SOPs

### Disengagement of Services

In the event of termination for convenience or prior to expiration of the contract, the Contractor shall be responsive and assist in the transition of services to <AGENCY> or to subsequent Contractor(s), as appropriate. The Contractor shall coordinate and transfer all <AGENCY> management and technical data to other service providers, as directed. The Contractor shall identify a transition team to assist the Government and the follow-on Contractor(s) during the transition period.

The Contractor shall cooperate and comply with the arrangements made for the replacement and follow-on to the contract. The Contractor shall coordinate, and transfer management and technical data as required to the incoming Contractor and/or the Government. Performance objectives include, but are not limited to, open partnership and coordination with the Government and incoming Contractor(s); continuity of operations and services; transfer of products and services to the Government and/or to the follow-on Contractor. With respect to transitioning out of the contract, the Contractor shall:

1. Coordinate and transfer all management and technical data to the Government or other service providers as directed.
2. Identify a transition team to assist the Government and the follow-on Contractor(s) during the transition period.
3. Cooperate and comply with the arrangements made for the replacement and follow-on to the contract.
4. Recognize that “partial off-ramps” of services, as directed by <AGENCY>, are included within the scope of follow-on contracts.
5. Coordinate and transfer management and technical data as required to the incoming Contractor and/or the Government.
6. Ensure open partnership and coordination with the Government and incoming Contractor(s).
7. Provide for continuity of operations and services.
8. Successfully transfer products and services to the Government and/or to the follow-on contract.

# Standards and Common Practices

## Applicable Standards

The following standards will be followed, as applicable to the specific tasks for which they are intended.

* Continuous Improvement Program Assets - Contractor will use the CIP template for a given activity when one is available.
* Section 508 Standards.
* IT Security Policies.
* OMB Circulars:
* A-11, Part 7, Planning, Budgeting, and Acquisition of Capital Assets
* A-109, Major Systems Acquisitions
* A-123, Management Accountability and Control
* A-127, Financial Management Systems
* A-130, Management of Federal Information Resources National Institute of Standards and Technology (NIST) 800-37 Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems

## General Requirements

The Contractor shall perform all the management and administrative tasks to satisfy the requirement of this SOW while adhering to all <AGENCY> and Federal policies.

### Property Management

The Contractor is responsible for maintaining an inventory of the equipment in their possession.

### Electronic Communications with <AGENCY>

The Contractor shall be capable of communicating electronically using an <AGENCY> compatible e-Mail system to communicate with the COTR, the CO and Performance Monitors, as applicable.

All deliverables shall be submitted using secure electron means or by other means as directed by the ISO or COTR and if requested in hardcopy in formats compatible with standard <AGENCY> productivity products.

The Contractor shall comply with all applicable Government laws and regulations including the Clinger-Cohen Act; Paper Reduction Act; Paperwork Elimination Act; the Performance and Results Act; and, Section 508 of the Americans with Disabilities Act.

### After Hours Support and Emergency Requirements

Services critical to the XXX role in supporting the <AGENCY> mission e.g., IT testing, scheduled and unscheduled maintenance, problem resolution and upgrades) will require some work outside of the core service hours. When it is necessary for the Contractor to respond to unscheduled problems during non-core service hours, the Contractor shall:

* Acknowledge initial contact via email/telephone within 20 minutes. Off-hours contact will be via mobile devices (i.e., blackberry, phone, pager, etc.)
* Respond to emergencies or other activities that require the performance of services outside of the standard service hours.
* Respond on-site within 1 hour of initial contact, as necessary.

### Access to <AGENCY> Facilities

The Government has the right to restrict and control access to its facilities, property, and data, including those that are identified in this SOW. Access privileges will be tailored to individual Contractor personnel responsibilities. The Government will be the final authority in determining access privileges. The Government’s exercise of its right to grant and revoke the access of particular individual(s) to its facilities, or parts thereof, shall not constitute a breach or change to the Contract, regardless of whether said individual(s) are employed by the Contractor, and regardless of whether said individual(s) are precluded from performing work under the resulting Contract.

### Records Maintenance and Reporting

The Contractor shall create and maintain files (e.g., records, reports, and logs) documenting the processing of work and associated information. Federal laws, regulations, and the direction of the COTR shall govern access to this information.

The Contractor shall make files available to the COTR upon request within five (5) business days of receipt of the request. The Contractor shall maintain all records including files, documents, and working papers provided by the Government and/or generated for the Government in the performance of this SOW. these records shall be maintained in a format approved by the COTR. In the event of default, or non-performance, the Government will have immediate access to records in order to ensure mission support is not interrupted. All such records shall be turned over to the Government at the completion or termination of the Contract.

The Contractor shall respond to <AGENCY> requests for information, including scheduled (programmed) and ad hoc (un-programmed) requests, from the COTR. The Contractor shall refer all requests for support to the COTR if received from other Government personnel prior to responding. The Contractor shall submit to the COTR programmed and un-programmed information.

Upon notification by the COTR, the Contractor shall provide management and technical information including, but not limited to, technical evaluation of suggestions and/or alternatives, fact sheets, audits, Congressional inquiries, one-time reports, materials, equipment, facilities, property inventories and other listings, and equipment maintenance records.

All records, files, reports, and data deemed proprietary by the Contractor shall be marked accordingly. The Government will make the final determination of the appropriateness of proprietary claims by the Contractor.

### Government and Contractor Interfaces

To ensure smooth and cooperative operations, the Contractor shall continuously facilitate cross-team communications across the functional areas described in this SOW. Additionally, due to the need to manage this effort as an integrated function, and given the complexity of the networking structure and interdependence of the various systems used by <AGENCY>, the Contractor shall coordinate and work closely with other Contractors and with Government employees as specified by the COTR. The Contractor shall provide seamless, well-coordinated service delivery across Government and Contractor boundaries.

# Deliverables

The following base period deliverables have been identified with due dates. Due dates for other deliverables specified in the Statement of Work will be communicated by the COTR once the contract has commenced. Table 1 contains Single Instance Deliverables, Table 2 contains Transition Deliverables, Table 3 contains Recurring Deliverables.

Table – List of Single Instance Deliverables

| **Reference** | **Single Instance Deliverable** | **Due Date** |
| --- | --- | --- |
| [3.1.1](#_bookmark15) | Program Mgt Plan – Draft | 30 calendar Days After Contract Award (DACA) |
| [3.1.1](#_bookmark15) | Program Mgt Plan – Final | 45 calendar DACA |
| [3.1.2](#_bookmark16) | Draft Program Level Quality Assurance Plan | 30 calendar DACA |
| [3.1.2](#_bookmark16) | Final Program Level Quality Assurance Plan | 45 calendar DACA |
| [3.1.2](#_bookmark16) | Quality Assurance Plan – Quarterly Update | Quarterly |
| [3.1.3](#_bookmark17) | Draft Program Level Risk Mgt Plan | 30 calendar DACA |
| [3.1.3](#_bookmark17) | Final Program Level Risk Mgt Plan | 45 calendar DACA |

Table – List of Transition Deliverables

| **Reference** | **Transition Deliverables** | **Due Date** |
| --- | --- | --- |
| [3.11](#_bookmark30) | Draft Transition Plan | 5 business DACA |
| [3.11](#_bookmark30) | Final Transition Plan | 10 business DACA |
| [3.11](#_bookmark30) | Staffing Report | 15 business DACA |
| [3.11](#_bookmark30) | Daily Transition Status Report | Daily, by 10:00 AM |
| [3.11](#_bookmark30) | Updates to Standard Operating Procedures | 30 calendar DACA |
| [3.11](#_bookmark30) | Status Report of Open Siebel Requests | Daily, by 10:00 AM |
| [3.11](#_bookmark30) | Daily Transition Status Report | Daily, by 10:00 AM |
| [3.11](#_bookmark30) | Final Transition Report | 45 calendar DACA |

Table – List of Recurring Deliverables

| **Reference** | **Recurring Deliverables** | **Due Date** |
| --- | --- | --- |
| 3.1.1.1 | Updates to the Program Management Plan | Annually |
| 3.1.1.1 | Project Plans | As directed by COTR |
| 3.1.3.1 | Updates to the Risk Management Plan | Annually |
| 3.1.3.1 | Project-level Risk Registers | As directed |
| 3.1.3.1 | Updates to Project-level Risk Registers | Quarterly |
| 3.1.4.1 | Program Status Report | Monthly |
| 3.1.4.1 | Project Status Report | Weekly |
| 3.1.4.1 | Management Report | As directed |
| 3.1.5.1 | Meeting calendars for the Daily Tag-Up, Weekly Status Meeting, and Monthly and Ad-hoc Contract Reviews | As directed |
| 3.1.5.1 | Meeting materials, including Action Items, for the Daily Tag-Up, Weekly Status Meeting, and Monthly and Ad-hoc Contract Reviews | As directed |
| 3.1.5.1 | Meeting Minutes and Action Items for the Daily Tag- Up, Weekly Status Meeting, and Monthly and Ad-hoc Contract Reviews | As directed |
| 3.1.5.1 | Daily Tag-up Reports | Daily, by 9:00 AM |
| 3.2.1.1 | Service and Application Recovery Plans, Reports, and updates | Per Schedule (TBD) |
| 3.2.1.1 | Risk Management Plans, Contingency Plans, and plan updates | 90 DACA and quarterly thereafter |
| 3.2.1.1 | Updated Business Impact Analysis (BIA) | 180 DACA and semi-annually thereafter |
| 3.2.1.1 | Regular briefings and reports regarding status of contingency activities | As directed |
| 3.2.1.1 | Lessons Learned Reports | As directed by the COTR, and within 10 days following debriefs of event |
| 3.3.1.1 | COMSEC Asset Inventory Report | No less than every 6 months or as required |
| 3.3.1.1 | COMSEC Training Records | As directed by the Sponsor, but no less than every 6 months from DACA |
| 3.3.1.1 | Training course for required individuals | Semi-annually |
| 3.3.1.1 | COMSEC Incident Report | Per occurrence |
| 3.3.1.1 | COMSEC Destruction Reports | Weekly |
| 3.3.1.1 | Trouble ticket and service metrics report | Monthly |
| 3.4.1.1 | Security and Incident reports content for Daily Tag- Up meetings | As directed |
| 3.4.1.1 | Quarterly evaluation of vulnerability and patch management tools and procedures | As directed |
| 3.4.1.1 | Vulnerability Assessment and Priority Reports | As directed |
| 3.4.1.1 | Standard Operating Procedures (SOPs) for the vulnerability and patch management process | As directed |
| 3.4.1.1 | SOPs for AORR | As directed |
| 3.4.1.1 | TIC performance management reports | Monthly |
| 3.5.1.1 | Security Controls Validation Test Report (control tests performed in years not requiring a C&A) | As needed |
| 3.5.1.1 | Risk Assessments | As directed |
| 3.5.1.1 | Systems Security Plan (SSP) | As needed |
| 3.5.1.1 | Security Assessment Report (SAR) Security Assessment Report (SAR) | As needed |
| 3.5.1.1 | ST&E Plans | As directed |
| 3.5.1.1 | Plan of Action and Milestones (POA&M) | As directed |
| 3.5.1.1 | Regular POA&M status reports | As directed |
| 3.5.1.1 | Complete set of C&A documentation as required by NIST-800-37 and <AGENCY> during the 90-120 day timeframe, depending on system complexity | As directed |
| 3.5.1.1 | ATO Letters | As directed |
| 3.5.1.1 | Audit documentation as requested | As directed |
| 3.6.1.1 | Privacy Threshold Analysis | As directed – typically quarterly |
| 3.6.1.1 | Privacy Impact Assessment Reports | As directed – typically quarterly |
| 3.6.1.1 | Privacy Impact briefings | As directed – typically quarterly |
| 3.6.1.1 | Privacy program assessment and recommendations for enhancement | As directed - typically quarterly |
| 3.6.1.1 | Plans and tactics to address privacy issues | As directed - typically quarterly |
| 3.6.1.1 | Privacy Act System of Records Notices (SORNs) | As directed - typically quarterly |
| 3.6.1.1 | Documentation support for the FISMA annual privacy reporting requirements | Annually |
| 3.6.1.1 | Reports that identify key information assets and privacy implications, as well as the creation or revision of agency privacy policy | As directed - typically quarterly |
| 3.7.1.1 | Documentation support as requested during the Independent Security Assessment | Annually |
| [0](#_bookmark25).1.1 | Analysis and Recommendations based on findings of the Independent Security Assessment | No later than 30 calendar days upon receipt of Independent Security Assessment |
| 3.7.1.1 | Recommendations on incorporating improvements into project plans | Quarterly |
| 3.7.1.1 | Format/outline of business cases | As directed |
| 3.8.1.1 | Progress Reports | Weekly |
| 3.8.1.1 | Documented overall IA and IT security governance processes | Annually |
| 3.8.1.1 | Updates to the Management Directives Handbook | Annually |
| 3.8.1.1 | Updates to the IT Security Handbook | Annually |
| 3.8.1.1 | Meeting support and documentation | As directed |
| 3.8.1.1 | Documented security plans and procedures | Annually |
| 3.8.1.1 | Recommendations for improving to security plans, policies, and procedures  Security policy analysis and impact reports | Quarterly |
| 3.8.1.1 | Maintain Policy branch mailbox log and provide status reports | Monthly |
| 3.8.1.1 | Updates to the Policies and FAQs Web portal | As directed |
| 3.8.1.1 | Reponses to OMB and DHS data calls | As directed |
| 3.8.1.1 | Reports on IT security product reviews, research, and studies | As directed |
| 3.8.1.1 | Standards and security program feasibility assessments and accompanying ROI analysis | As directed |
| 3.8.1.1 | Additional support and materials as requested to support security training, outreach and awareness, audits, the CCB, and other relevant activities and efforts | Frequency is as needed with meetings. Due dates shall be determined by urgency and need. |
| 3.8.1.1 | Surveys summarizing user experience, violations, and recommendations | Quarterly |
| 3.9.1.1 | Periodic reports, defined by the annual <AGENCY> Information Security Performance Plan, POAMs, detailing the accuracy, quality, and timeliness of all artifacts uploaded in the FISMA tool. Reports shall detail the mitigation progress for system weaknesses to include trending analysis and non-compliance issues for all information systems throughout  <AGENCY>. | To be established by ISO and approved by COTR |
| 3.9.1.1 | In-Progress-Reports (IPRs) for projects and meeting summaries for submission to the ISSO and CIO. | Monthly |
| 3.9.1.1 | Security impact assessments | Within 10 calendar days of event’s occurrence |
| 3.9.1.1 | Recommendations to improve monitoring processes | 90 DACA and quarterly thereafter |
| 3.9.1.1 | Status reports | Daily, weekly, monthly, and annually as required |
| 3.1.10.1 | System administration status reports | Monthly |
| 3.1.10.1 | Incident status reports and recommendations for remediation tactics | Monthly or as requested |
| 3.1.10.1 | Recommendations for blocked categories | Quarterly |

# Acronyms

The table below contains a list of commonly used acronyms related to this agency, and the work to be performed.

Table – Appendix B - Acronyms

| **Acronym** | **Definition** |
| --- | --- |
| ASB | Administrative Systems Branch |
| ATO | Authority to Operate |
| C&A | Certification and Accreditation |
| CIO | Chief Information Officer |
| COMSEC | Communication Security |
| COOP | Continuity of Operations |
| COTR | Contracting Office Technical Representative |
| COTS | Commercial off the Shelf |
| CSAB | Customer Support Asset Management Branch |
| CSAM | Cyber Security and Asset Management |
| DACA | Days After Contract Award |
| DHS | Department of Homeland Security |
| DNSSEC | Domain Name System Security Extensions |
| EKMS | Electronic Key Management System |
| ESB | External Systems Branch |
| FISMA | Federal Information Security Management Act |
| HIPS | Host Intrusion Prevention System |
| IA | Information Assurance |
| IMB | Infrastructure Management Branch |
| ISO | International Standards Organization |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| LAN | Local Area Network |
| LMD/KP | Local Management Device/Key Processor |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NRO | National Reconnaissance Office |
| NSA> | National Science Foundation |
| OIRM | Office of Information & Resource Management |
| OMB | Office of Management and Budget |
| PIA | Privacy Impact Assessment |
| POAM | Plan of Action and Milestones |
| PMP | Program Management Plan |
| QAP | Quality Assurance Plan |
| QC | Quality Control |
| RDSB | Research Directorate Systems Branch |
| RMP | Risk Management Plan |
| RTM | Requirements Training Manual |
| SaaS | Software as a Service |
| SAPPB | Security Architecture, Policy & Planning Branch |
| SAR | Security Accreditation Report |
| SCAP | Security Content Automation Protocol |
| SLA | Service Level Agreement |
| SLO | Service Level Objective |
| SNORT® | Sourcefire® network reliability tool |
| SOP | Standard Operating Procedure |
| SOW | Statement of Work |
| SSP | System Security Plan |
| ST&E | Security Test & Evaluation |
| STIG | Security Technical Information Guide |
| TAF | Trusted Agent FISMA |
| TBD | To be determined |
| TCB | Telecommunications Branch |
| TIC | Trusted Internet Connections |
| WAN | Wide-Area Network |

Table – Appendix C - Glossary

| **Term** | **Definition** |
| --- | --- |
| Contractor | Synonymous in meaning with Service Provider or entity having responsibility for performance and contractual obligations |
| Cloud or Cloud Computing | In this meaning Cloud Computing is synonymous with SaaS or IaaS. It represents a virtual, hosted environment. |
| Infrastructure as a Service | Means utility-like IT services in a virtual environment providing shared resources, software, and computing platforms to <AGENCY>. |
| ISO 27001 | Refers to the International Standards Organization’s ISO/IEC 27001:2005 governing standards for information technology, security techniques, and systems used in information security management |
| Migration Contractor | The Service Provider who will provide migration and consolidation of security services to <AGENCY> and its various Branches. |
| Service Provider | Synonymous with source providing services defined within the SOW. |
| Software as a Service | Means hosted Applications via remote server which is owned and operated by the Hosting Service Provider |

1. Supplemental publications may be used, such as: *NIST Special Publication 800-26, Department of Defense (DoD) Policy 8500, Director of Central Intelligence Directive (DCID) 6/3, ISO/IEC Standard 17799, General Accounting Office (GAO) Federal Information System Controls Audit Manual (FISCAM),* etc. [↑](#footnote-ref-1)