1. **ARMY (General Fund Audit Readiness Support)**

As the subcontractor, Security Risk Management Solution (“SRMS”) provides IT security-related services to US ARMY which are compliant with the **Federal Information System Controls Audit Manual (**FISCAM), National Institute for Standards and Technologies (NIST) and Federal Information Processing Standards (FIPS), DoD Information Assurance Certification and Accreditation Process (DIACAP) and DoDI 8500.2, Information Assurance Implementation, Configuration Management auditing, reviews and reports and Information Assurance (IA) services.  SRMS is also providing services to ensure that all entity-wide application deliverables meet the requirements of the most current federal standards and guidance that are applicable. This includes Security Authorization and Accreditation, SA&A (formally referred to as C&A) activities and compliance. SRMS is also providing application security test and evaluation (ST&E), audits, reviews, and reports in support of the Security Authorization and Accreditation (SA&A) process, FISCAM processes, SISSU processes; and Enterprise Information Technology Data Repository (EITDR) certifications. We are conducting functional testing and ST&Es to support Security Authorization and Accreditation (SA&A) in the Prime Contractor’s provided dynamic testing environments.

Our security auditors identify vulnerabilities and control weaknesses and develop recommendations for remediation. We also support the ITA Audit Readiness and Continuous Monitoring Program by leveraging auditing best practice to assess implemented IA controls for compliance and effectiveness. Our team experience and skills utilized during these tasks require:

* In-depth understanding of security auditing methodologies, frameworks, principles, and best practices
* Experience developing information assurance control test procedures.
* Experience developing recommendations to remediate audit findings.
* Experience executing Audit Readiness Reviews, IS audits, DoD/IC Financial Statement Audits and Security Authorization and Accreditation (SA&A)
* Experience testing security, information assurance, and internal controls
* Strong knowledge of DoD polices, IA standards and principles.
* Strong knowledge of NIST SP800-53 and DIACAP standards
* Strong knowledge of FIACAM controls and OMB Circular A-123
* Experience with vulnerability assessment tools such as Nessus, Retina, and AppDective
* Understanding of security controls at all critical layers (network, application, OS, database, etc.)
* Experience writing at a "publication" quality level to communicate findings and recommendations to the client’s senior management team.
* Experience managing and accessing technologies to include: Windows, Unix, Mainframes, and SAP.

Day-to-day activities include conducting IT control assessments, identifying weaknesses, proposing tests, and implementing solutions. We participate in activities such as evaluating Access, Security, Configuration Management, Segregation of Duties, Contingency, and general Business Application controls using the Federal Information Systems Controls Audit Manual (FISCAM), NIST, and DIACAP methodologies. SRMS provides best practices on how to audit the access and configuration management controls efficiently and effectively. SRMS is also evaluating the design and effectiveness of technology controls throughout the business cycle to include identifying and communicating IT audit findings to senior management and the client to help identify performance improvements.

As a subcontractor, SRMS is also managing the staffing and technical execution involved with conducting numerous audits as part of the customer’s Security Authorization and Accreditation (SA&A) program. These tests included internal and external IT-related security tests; policy and procedure documentation review for compliance; and policy and procedure reviews and testing for verification of compliance and security assurance.

The following is a list of the referenced criteria during the policy, procedural and technical activities involved during the support of this contract:

* FISMA, FISCAM, FIPS 199 & 200,
* NIST S.P.s 800-18, 800-34, 800-37, 800-43, 800-53, 800-60 & 63
* Acceptable Risks Safeguards (ARS),
* Certification and Accreditation Methodology,
* System Development Life Cycle Framework,
* CP Procedures, Risk Assessment Methodology; and
* System Security Plan Methodology
1. **NIH (CIT-IAM Program Support)**

NIH Identity, Credential and Access Management Professional Services project, herein known as “NIH IAM Support.”  NIH’s Center for Information Technology (“CIT”) IAM Services. The Information Security Program in the NIH Office of the Chief Information Officer (OCIO) is responsible for coordinating all security activities across the entire NIH, including CIT.

As a subcontractor, SRMS supported NIH to manage the GAO Audit process through Audit Preparation, Audit Coordination and Response, and Audit Remediation. In support of this approach, SRMS provided a core team of qualified and experienced professionals that will support NIH with the following activities throughout the life of the project. SRMS’s support included a programmatic approach to support NIH review relevant policies, procedures, and systems, and develop remediation strategies for vulnerabilities. SRMS advised on a broad set of complex functional and technical domains, such as federal compliance, network security, policy and program management, identity and access management, configuration management or other areas relevant to the Audit.

SRMS supported NIH to manage the GAO Audit process through Audit Preparation, Audit Coordination and Response, and Audit Remediation. In support of this approach, SRMS provided a core team of qualified and experienced professionals that will support NIH with the following activities throughout the life of the project:

* Assist with conducting gap analysis for FISMA moderate GSS to identify potential high-impact, high-risk weaknesses.
* Establish plan to incorporate FISMA high controls based on newly established re-categorization by applying test case standards traceable to 800-53A rev 4.
* Help coordinate discussion with operational staff to assist with remediation strategies in preparation for pending GAO Cyber Security audit.
* Help assemble documents in preparation for response to audit and assessments findings which are uploaded into a Governance Risk and Compliance (GRC) tool called NIH System Authorization Tool (NSAT)
* Plan, implement, and support project management services that help NIH prepare for and respond to audit activities.
* Plan and support leadership briefings, planning sessions, meetings, and IC collaborations.
* Assemble documents in preparation for audit and assessments.
* Assemble documents in response to audit and assessment findings.
* Provide other administrative support for audits and assessments.

SRMS’s support include a programmatic approach to support NIH review relevant policies, procedures and systems, and develop remediation strategies for vulnerabilities. SRMS advised on a broad set of complex functional and technical domains, such as federal compliance, network security, policy and program management, identity and access management, configuration management or other areas relevant to the Audit.

1. **USAF (RMF Support)**

As a subcontractor, SRMS provided Advisory and Consulting Services to the US Air Force (AF) Chief Information Security Officer (AF CISO) in support of the Risk Management Framework (RMF).In that capacity, SRMS;

* Provided input and recommendation to SAF/CIO-A6 regarding Air Force (AF) policy related cybersecurity in support of National Institute of Standards and Technology (NIST) objectives.
* Assisted with assessing the design and operating effectiveness of NIST controls while proposing strategy and policies to support (AF) CISO addressing IT security.
* Assisted with calculating cyber defense posture scores for critical AF systems found on both unclassified and classified versions of the GRC tool called Enterprise Mission Assurance Support Service (eMASS)
* Assisted with establishing an organization-wide Risk Tolerance Baseline used for providing stakeholders with a centralized starting point for assessing risk.
* Helped with development of a full control mapping of DoD Information Assurance Certification and Accreditation Process (DIACAP) controls to risk management framework (RMF) controls.
* Assisted with working on “RMF Next” initiative to re-think the AF RMF process based on guidance from NIST SP 800-37 revision 2.
* Assisted the SAF/CIO-A6 with creating an enterprise strategy that drives requirements and processes for information system continuous monitoring (ISCM)
* Coordinated efforts to incorporate AF mission area owners (MAO) into A6 ISCM strategy based on information requirements for RMF utilizing swim lane process flows.
* Focused on a plan related to the Cyber Security Framework (CSF) and incorporating its capabilities regarding criticality and mission risk into current goals and objectives.
* Assisted with cyber security standards and plans to enable AF organizations to practice safe security techniques and technical solutions to protect AF data.
* Assesses the design and operating effectiveness of FISCAM Security Management (NIST) and RMF controls, proposes strategy and policies to support AF CISO Framework addressing AF entity level controls associated with IT Security.
* Supports the AF CISO with achieving FISCAM Security Management (NIST) objectives, providing cyber and network security technical and risk management expertise to AF CISO.
* Assists the Government in cyber security standards, security architectures, and plans to enable AF organizations to practice safe security techniques and technical solutions to protect AF data.
* Review innovative methods, procedures, techniques, and approaches to ensure security criteria, guidance, and methodology are applied to information systems and security devices being developed and acquired.
* Provides Enterprise Risk Management expertise and support to establish an Air Force wide risk management framework (RMF) to track enterprise level risks.
* Drafts point papers, reports, publications, meeting minutes, and other documents as required in support of execution of Security Management (NIST) objectives.
* Develops an acculturation strategy, to include recommended training, to assist the AF in the successful transition of FISCAM Security Management (NIST) objectives to the AF CISO framework to support entity level controls and appropriate enterprise risk management.
* Provides input and recommendation to SAF/CIO-A6 regarding AF policy related to IA training; formulates policy, tracks compliance, and assists in the support of FISCAM Security Management (NIST) objectives.
1. **FBI (Information Assurance Program Support)**
* Provided expertise to the FBI Information Assurance Program in the implementation and management of the IA procedures across the enterprise.
* Certified high visibility systems within the agency including Secret, Top Secret and Top- Secret SCI systems, in accordance with NIST and DCID 6/3 requirements.
* Coordinated the efforts of all stakeholders in Certification and Accreditation (C&A) or re-certification of information systems, ensuring timely completion of the C&A process utilizing Risk Vision GRC tool.
* Performed assessments of the System Security Plans (SSP), Risk Assessments (RA), Security Assessment Reports (SAR), Contingency Plans, and Plans of Action and Milestones (POA&M) management
* Assisted the Information Systems Security Manager (ISSM) with the implementation of IA security policies and coordination of ISSO activities such reviewing findings from Tenable Nessus and HP WebInspect scans to help coordinate risk mitigation strategies.
* Worked closely with system owners to ensure appropriate steps are taken to implement information security requirements for IT systems throughout their life cycle, from the requirements definition phase through disposal.
* Provided guidance to the ISSOs on the development and management of C&A documentation while coordinating security inspections and the testing and reviewing of security controls to make sure they are implemented properly and FISMA compliant.
* Reviewed System Security Plans (SSPs) and System Security Authorization Agreements (SSAA), Concepts of Operations (CONOPS) and Security Requirements Traceability Matrix (SRTM) to ensure data ownership and responsibilities are established for each information system.
1. **DLA, HHS, USDA (Information Assurance Program Support)**
* Applied security configurations using the Defense Information Systems Agency (DISA) Gold Disk Security Technical Implementation Guide (STIG) to the infrastructure at various military bases across the country.
* Updated system security plan (SSP), continuity of operations plan (COOP), risk mitigation plan,

operations and maintenance plan, and a technical assistance plan for a web-based application called Department of Health and Human Services (HHS) E-Induction: Online Induction for New Hires for the Office of Human Resources at the HHS.

* Designed a disaster recovery plan (DRP) for the United States Department of Agriculture (USDA) Foundation Financial Information System division’s network infrastructure.
* Performed risk assessment of the Financial Management Systems for the United States Agency for International Development (USAID) using OMB Core Financial Systems Requirements and the United States Marine Corps (USMC) by reviewing the technical security requirements and associated documentation.
* Supported the certification and accreditation (C&A) process for the Office of Management and Budget (OMB) MAX budget system. Support includes preparation of system security plan (SSP) and requirements traceability matrix (RTM) for MAX Community and Max Collect
* Recommend appropriate FIPS 199 impact level designations and identify appropriate security controls based on characterization of the general support system or major application.
* Developed a Plan of Action and Milestones (POA&M) of appropriate findings and related recommendations for corrective action and (2) determined the nature, timing, and extent of substantive testing that will be needed.
* Assisted the information systems security manager (ISSM) by ensuring policies and procedures are followed for processing all Protection Level (PL) 1 classified data in a secure environment.
* Participated in an annual company disaster recovery drill that demonstrates the ability to recover key areas of the research staff's network infrastructure as promised to government clients.
* Performed client security interviews as part of security control evaluations with various clients against a variety of standards, including NIST & FISMA guidelines.
* Gathered and coordinated technical information to develop SSAA's, Concepts of Operations (CONOPS) and Contingency Plans. Track and monitor POA&Ms to ensure vulnerabilities are mitigated as scheduled in the IATO/ATO accreditation letters Used Lumension’s Patchlink Security Management Console to scan multiple networks for vulnerabilities (DEV, TEST, and PROD)
* Managed patch process according to our system development life cycle (SDLC) plan (DEV, TEST, and PROD)
* Administered Microsoft Windows Servers (Windows 2003/2008)
* Ran routine scans using Tenable Nessus, Microsoft Baseline Security Analyzer (MBSA), and NMAP looking for vulnerabilities for system configurations, websites, and open ports.
* Administered active directory security via group policies in three physically separate, distinct environments (DEV/TEST/ PROD) following industry best practices.
* Managed web application creation in SharePoint and implemented portal security according to industry best practices.
* Managed/installed Cisco Security Agent HIDS on all servers in DEV, TEST and PROD environments.
* Administered virtual sessions for software developers using VMware infrastructure client.
* Managed internal certificate authority (CA) as well as third party server certificate administration.