SCOPE OF WORK
FOR
RISK MANAGEMENT FRAMEWORK (RMF) SUPPORT SERVICES

25 May 2023
Version 2.0.4

1.0 GENERAL

1.1 BACKGROUND

The United States Coast Guard (USCG) depends on information systems to carry out their missions and business functions in support of six major operational mission programs: Maritime Law Enforcement, Maritime Response, Maritime Prevention, Marine Transportation System Management, Maritime Security Operations, and Defense Operations. An "information system" is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [44 USC 3502].

The USCG further categorizes "information system" by type, such as Platform Information Technology (PIT), PIT System, and Operational Technology (OT). Examples of USCG information systems include, but are not limited to computing systems; cyber-physical systems; industrial/process control systems; environmental control systems; Supervisory Control and Data Acquisition (SCADA); Programmable Logic Controllers (PLC); weapons systems; command, control, communications, intelligence, surveillance, reconnaissance, and navigation systems; motor/engine controls; power generation systems; power distribution systems; propulsion control systems; devices and information technology products such as smart phones and tablets; and embedded devices/sensors. For the purposes of this document, the term "information system" or "system" refers to any type categorization descriptor used in practice by the USCG, and includes systems connected to the Non-Classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), systems deployed in commercial cloud environments, and off-network systems.

"Cybersecurity" (which replaced the term Information Assurance [IA]) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Risk Management Framework (RMF) for Information Systems and Organizations, provides a system lifecycle approach for security and privacy, and is integral to the implementation of the Federal Information Security Modernization Act (2014). The RMF is mandatory for federal government use, and promotes near real-time risk management and ongoing information system authorization through the implementation of continuous monitoring processes; provides senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the information systems supporting their core missions and business functions; and integrates cybersecurity into the enterprise architecture and system development life cycle. The seven step process of the RMF includes preparation, categorization, selection, implementation, assessment, authorization, and monitoring.

The USCG requires contractor support to perform the RMF tasks that are the responsibility of the Information System Security Officer, Information System Security Engineer, and the Security Control Assessor, to also include cybersecurity compliance assessment, management, and reporting for the USCG systems. The services provided by these roles are required to properly implement the RMF and are applicable to the system from time of acquisition through decommissioning and disposal. In the past, these standard RMF services have been provided through several disparate contracts. The desire is to consolidate these contracted RMF services under a single contract. This organizational approach to acquire these standard cybersecurity services will align contracting activities, reduce the contract management overhead, and allow for greater efficiency to award new work when warranted.

1.2 SCOPE

This Indefinite Delivery Indefinite Quantity (IDIQ) contract is established for Contractor provided cybersecurity Risk Management Framework (RMF) services for USCG systems. All effort will be performed at the Individual task order level and will be issued on a Firm-Fixed Price (FFP) basis. During performance of the IDIQ contract, the Contractor shall provide the USCG with RMF support aligned to the Information Assurance roles described below.

The Contractor shall provide Information System Security Officer (ISSO) and Alternate ISSO (AISSO) services, Information System Security Engineer (ISSE) services, Security Control Assessor (SCA) services, and Cybersecurity Compliance and Readiness Services as described below to meet the requirements of the USCG Cybersecurity RMF process and cybersecurity of USCG Information Systems. The Contractor shall furnish all the necessary personnel, materials, equipment, facilities, travel and other services required to satisfy all task order requirements.

1.2.1 Task Area One: Information System Security Officer (ISSO) Services

(a) Serve as the designated ISSO for assigned systems.
(b) Lead the RMF process for assigned programs, organizations, systems, or enclaves.
(c) Generate and maintain the RMF documentation package that meets all Department of Defense (DoD) requirements and is tailored to a specific system to include but not limited to; Security Categorization Determination, Implementation Plan, System Security Plan (SSP), Configuration Management Plan (CMP), Incident Response Plans (IRP), Contingency Plans (CP), Authorization documentation, IT Security Plans of Action & Milestones (POA&Ms), Scorecards, Security Assessment Reports (SAR), Continuous Monitoring Strategy, Hardware/Software lists, Threat Models, Cybersecurity Strategy, Network Topology, Network Cybersecurity Boundary Diagrams, and Data Flow Diagrams using Government prescribed tracking and processing tools.
(d) Ensure that all DoD Information System (IS) cybersecurity-related documentation is current and accessible to properly authorized individuals.
(e) Interpret system designs and diagrams for the purposes of identifying data interconnections, interfaces, protocols, and data types in order to select appropriate security controls to remediate or minimize Cybersecurity risk exposure to the Coast Guard.
(f) Provide support and develop a connection approval package such as an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), Service Level Agreement (SLA), and so forth, for systems that require connectivity to any type of USCG Local Area Network (LAN) (i.e. DoD Information Network (DoDIN), CGOne, SIPRNet).
(g) Develop plans and perform testing to evaluate compliance with all applicable DoD and industry security requirements, standards, and best practices.
(h) Utilize Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG)/Secure Requirements Guides (SRG) assessments including leveraging automation as much as possible to gain efficiencies.
(i) Perform Security Readiness Reviews (SRR) for the Operating Systems and applications.
(j) Perform automated scans and analysis using Security Compliance Checker (SCC) DISA Security Content Automation Protocol (SCAP) benchmarks or current DoD approved tools.
(k) Perform automated scans and analysis using the Assured Compliance Assessment Solution (ACAS)/Nessus or current DoD and Department of Homeland Security (DHS) approved tools.
(l) Maintain the continuous monitoring process and ensure all systems are compliant with DoD and USCG security guidelines, and DISA STIGs.

(m) Maintain process and procedures, in coordination with the government, that enable the organization to adhere to Requests for Modification (RFM) while remaining compliant with the overall RFM organizational process.
(n) Participate in system change management boards/reviews, as necessary.
(o) Conduct Security Impact Assessments (SIA) as part of the RFM process to determine if there are any impacts to implemented security controls.
(p) Ensure that all Assessment and Authorization (A&A) packages are completed and submitted in time to prevent Authorization To Operate (ATO) expiration.
(q) Initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered, and ensure that a process is in place for authorized users to report all cybersecurity-related events and potential threats and vulnerabilities to the ISSO.
(r) Review, update and publish all cybersecurity artifacts to support unclassified (including Chief Financial Officer (CFO)), and classified IA efforts within USCG prescribed tools and maintain any security relevant artifacts including site or organizational Cyber Security Plans and Common Control Catalogs.
(s) During all DHS Systems Engineering Life Cycle (SELC) phases, develop documentation and provide any required information for all levels of classification in support of the A&A process.
(t) Provide support and collaboration to external inspections, evaluations, audits, and assessments as applicable for supported systems.
(u) Manage and track all POA&Ms created by the organization to address identified weaknesses, vulnerabilities, and audit/assessment findings from creation to closure. Coordinate with other organizations as needed in the processing and management of the POA&Ms. This includes validation of POA&M content submitted by the area of responsibility (AOR) for weakness remediation; ensuring POA&Ms are submitted via proper channels; providing reports and status tracking of remediation efforts; work with the AOR as needed to ensure items are completed in a timely manner and to gather appropriate artifacts for closure; and identifying POA&Ms that will need waivers or risk acceptance.
(v) Develop and coordinate Contingency Plan (CP) training/testing as required by DoD and USCG policy annually on or before the expiration date of the previous annual test.
(w) Coordinate annual Disaster Recovery (DR) Failover testing for systems with a DR presence and document results of testing to present to the government as needed.
(x) Maintain Host Based Security System (HBSS) compliance for assigned systems.
(y) Review exception and exclusion requests and provide recommendation for government approval.
(z) Monitor and remediate rogue devices.
(aa) Review system HBSS reports.
(bb) Review applicable system logs in accordance with USCG or DoD security policies and security configuration guidance.
(cc) Request system-related audit triggers to monitor and correlate daily records at least once per week.
(dd) Review system audit records and intrusion detection data to assist ISSOs in identifying security incidents.
(ee) Analyze any potential threat vectors across disparate internal related systems.
(ff) Coordinate any security incident forensic analysis with Coast Guard Cyber Command (CGCyber) Cyber Security Operations Center (CSOC) Incident Response Service Line.
(gg) Report any system related log data integrity issues or gaps to the government.

1.2.2 Task Area Two: Information Systems Security Engineer (ISSE) Services

(a) Serve as the Information Systems Security Engineer (ISSE) providing technical input, recommendations, and assistance with the implementation of both higher and granular-level cyber security approaches, methods and solutions that incorporate and maintain compliance to requirements resulting from laws, regulations, and other pertinent guidance.
(b) Participate in acquisition meetings (PMR, PDR, CDR, etc.), concept of operation (CONOP) working groups, change boards, technical exchange meetings and other similar activities.
(c) Design and develop security requirements that drive down risk while maintaining operational capability.
(d) Work between architecture-level and implementation-level engineering meetings to maintain a system-wide view of security functions and apply risk mitigation strategies at the appropriate level.
(e) Provide guidance on work against program requirements and goals. This includes participating in technical discussions, trade studies and working groups, and conducting research on industry best practices for potential implementation.
(f) Interface with various Government stakeholders to explain security requirements, risks and mitigations relative to their priorities of cost and schedule to ensure an acceptable risk tolerance.
(g) Evaluate newly identified threats and vulnerabilities to customer information systems to ascertain the need for additional safeguards and develop timely implementation strategies to reduce risk.
(h) Enforce the design and implementation of trusted relationships among external systems and architectures.
(i) Assess proposed changes to customer information systems, their operation environment, and mission needs for impacts to cybersecurity architectures and continued compliance with cybersecurity requirements.
(j) Provide inputs to development teams responsible for designing and developing organizational information systems and upgrading legacy systems.
(k) Employ best practices when implementing security requirements for information systems including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques.
(l) Keep abreast of current and new security technologies and threats to better support the customer in maintaining cybersecurity resilience.
(m) Identify integration issues related to the implementation of new systems within the existing infrastructure; recommend mitigation and/or resolution options as appropriate.
(n) Assist in the design of systems and networks that encompass multiple enclaves to include those with differing data protection/classification requirements
(o) Provide assessments of USCG Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) deliverables for purposes of providing Independent Verification and Validation (IV&V) for all USCG Acquisition Programs. Support will include metrics that provide detailed data on independent assessment of technical feasibility; cost and schedule reasonableness; review of deliverable documents; and assessment of requirements, architecture and standards in deliverable documents and products.
(p) Support DevSecOps activities as required for sustainment of cybersecurity dashboards, and providing guidance on vulnerability guardrails/thresholds for applications.

1.2.3 Task Area Three: Security Control Assessor (SCA) Support Services

(a) Support the development, and review of the plan to assess the security controls.

(b) Assess the security controls in accordance with the assessment procedures defined in the security assessment plan
(c) Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment
(d) Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.
(e) Review, validate, and develop RMF authorization recommendations for USCG information systems to be submitted to the Authorizing Official.
(f) Provide a summary of failed controls in Risk Assessment tab in eMASS.
(g) Recommend updates to the POA&M based on the assessment results.
(h) Provide traceability of all vulnerabilities from raw assessment results to the POA&M.
(i) Prepare and submit the Security Authorization Package with program assistance.
(j) Recommend policies and procedures to meet security control requirements.
(k) Brief branch, division and department head on the status of current and future validation efforts.
(l) Support the continuous monitoring program as necessary.

1.2.4 Task Area Four: Cybersecurity Compliance and Readiness Services

1.2.4.1 General

(a) Participate as directed in Integrated Process Teams (IPTs), Design Reviews, and Working Groups to provide input on system security risks, independent cost estimates, cross-classification boundary security technologies, Platform IT packages, and other considerations which may either promote or hinder certification of new systems.
(b) Provide assistance with the destruction of removable media.
(c) Support Cybersecurity strategic planning activities to evaluate enterprise services through the assessment of priorities and risks.
(d) Demonstrate the ability to convey complex cybersecurity data to a wide variety of Government audiences.
(e) Demonstrate oral and written communication skills.

1.2.4.2 Vulnerability Management

(a) Review all vulnerabilities identified through regularly scheduled and ad-hoc scanning, assign and track remediation responsibility, and track identified vulnerabilities through remediation via the regular patching cycles or until a POA&M is created for tracking.
(b) Identify any vulnerabilities that remain on the system after a period of time and notify designated patch manager to engage to determine how the finding will be disposed.
(c) Coordinate and maintain the DHS' and DOD's vulnerability database accounts.
(d) Coordinate with ISSOs to advise and facilitate resolution of all Cybersecurity and Information Security (INFOSEC) issues.
(e) Conduct and evaluate vulnerability scans, including Information Assurance Vulnerability Management (IAVM) compliance, using USCG prescribed tools recurring by the end of each month, and as necessary as directed by the government.
(f) Develop and maintain procedures to track IAVM compliance, and remediation responsibilities (e.g., patching oversight) for future POA&M development.
(g) Utilize standard software tools to conduct vulnerability scans of networks and databases.
(h) Conduct ad hoc remediation vulnerability and compliance scans.

(i) Ensure that 95% authenticated ACAS vulnerability scan rate is achieved and maintained.
(j) Coordinate services with CGCyber Vulnerability Assessment Team (VAT) to ensure service levels are maintained and available.
(k) Ensure that all assets within scanning tools are assigned to the appropriate boundaries to ensure that complete and accurate scanning is occurring.
(l) Provide scan results to the ISSO's and AISSO's, as well as information system administrators.
(m) Manage and coordinate scanning credentials to ensure all environments are accessible by the scanners and sensors.
(n) Provide false-positive (FP) management ensuring there is a means to submit a FP claim, process that claim through proper validation, and coordinate with CGCYBER for submission of DISA tickets if warranted. Prevent the FPs from continuously being analyzed, but be able to revalidate and dispose of periodically.

1.2.4.3 Knowledge and Metrics Management

(a) Develop and maintain matrices to track and analyze trends in IA readiness and compliance.
(b) Utilize tools and tracking mechanisms that must automate reporting and data collection of INFOSEC associated vulnerabilities.
(c) Collaborate with the government to develop metrics to provide the Cyber Health for information systems based on mandated reporting and supplemental risk scorecards.
(d) Track and report status on all official authoritative orders. These orders can originate from JFHQ-DoDIN, US Cyber Command, CG Cyber Command, and generally take the form of Operational Orders (OPORDs), Task Orders (TASKORDs), Fragmentation Orders (FRAGOs) applicable to released TASKORDs or OPORDs, ALCOASTs or Time Compliant Technical Orders (TCTOs).
(e) Maintain awareness of all policy that provides input to IA requirements and facilitates standards and guidance distribution and updates to IA stakeholders.
(f) Respond to ad-hoc IA data calls as directed by the government.
(g) As security requirements change, assist in preparation, review, and update policies and procedures for compliance with DHS, DoD and USCG requirements.
(h) Provide data analysis, metrics development, and reporting for cybersecurity areas such as Inventory and Asset Management, Vulnerability remediation AORs, IAVM tracking, and so forth.

1.2.4.4 Command Cyber Readiness Inspection (CCRI) Support

Provide support to Scheduled and Limited Notice (LN) Command Cyber Readiness Inspections. This support coverage includes all C5I systems/assets within scope of the particular CCRI and may include traveling to sites scheduled for inspections to aid as needed. Areas of support include, but are not limited to:

(a) Site Scoping.
(b) Vulnerability Per Host (VPH) Determination.
(c) Artifact Gathering and Staging.
(d) POA&M Support.

1.2.4.5 Privileged User Account Management

(a) Provide coordination of the USCG Privileged User Management Program (PUMP) process across all applicable staff members at all places of performance.
(b) Ensure compliance with the overall PUMP program administered by the USCG.
(c) Annually verify Admin Access accounts.

1.2.4.6 Cross Domain Analysis and Evaluation

(a) Identify Cross Domain requirements, evaluation of candidate solutions, recommendations for integration approaches including security considerations, generation of documentation for certifications, accreditations, and approvals related to Cross Domain Devices and the facilitation of processing Cross Domain Solution tickets.
(b) Provide documentation and analysis support as needed to determine need for High Assurance Guards (HAGs) and Controlled Interface Devices (CIDs) for use on USCG assets.
(c) Provide production, documentation, and development support for the development of Controlled Interface for use on assets to include: Rule Set development; Acknowledge/Not Acknowledge (ACK/NAK) Channel set-up; develop Message Analysis and Generation Tables; engineering support for CDS Controlled Interfaces.

1.3 APPLICABLE DOCUMENTS

The following documents provide mandates, policy, specifications, standards, or guidelines that apply to performing the work described in this document:

Table 1 Applicable Documents

REFERENCE	DESCRIPTION / TITLE
FISMA	Federal Information System Modernization Act (2014)
P.L. 93-579	Public Law 93-579 Privacy Act, December 1974 (Privacy Act)
EO 13526	Classified National Security Information
32 CFR Part 117	National Industrial Security Program Operating Manual (NISPOM)
OMB A-130	Managing Information as a Strategic Resource
OMB M-05-22	Transition Planning for Internet Protocol Version 6 (IPv6)
OMB M-19-03	Management of High Value Assets
CJCSI 6510.01E	Information Assurance and Support To Computer Network Defense
DoDD 8140.01	Cyberspace Workforce Management
DoDI 8500.01	Cybersecurity
DoDI 8510.01	Risk Management Framework for DoD Systems
DoD 8570.01-M	Information Assurance Workforce Improvement Program
DHS BOD 18-02	Securing High Value Assets
DHS MD 103-01	Enterprise Data Management Policy

REFERENCE	DESCRIPTION / TITLE
DHS MD 140-01	Information Technology Security Program
DHS MD 11042.1	Safeguarding Sensitive But Unclassified (FOR OFFICIAL USE ONLY) Information
DHS MD 11056.1	Sensitive Security Information (SSI)
DHS Instruction 102-01-103	Systems Engineering Life Cycle (SELC)
DHS Instruction 102-01-004	Agile Development and Delivery for IT
DHS Policy Directive 4300A	Information Technology System Security Program, Sensitive Systems
OIG-09-65	The DHS Personnel Security Process
COMDTINST M5000.10 (series)	USCG Major System Acquisition Manual (MSAM)
COMDTINST M5000.11 (series)	USCG Non-Major System Acquisition Manual (NMAP)
COMDTINST 5500.18	Coast Guard Trusted Associate Sponsorship System (TASS)
FIPS 199	Federal Information Processing Standards Publication (FIPS) 199 - Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
NIST SP 500-267	USGv6 Profile
NIST SP 800-18	Guide for Developing Security Plans for Information Technology Systems
NIST SP 800-30	National Institute of Standards and Technology (NIST) Guide for Conducting Risk Assessments
NIST SP 800-35	Guide to Information Technology Security Services
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800-44	Guidelines on Securing Public Web Servers
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
NIST SP 800 53B	Control Baselines for Information Systems and Organizations

REFERENCE	DESCRIPTION / TITLE
NIST SP 800-61	Computer Security Incident Handling Guide
NIST SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems
NIST SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
NIST SP 800-153	Guidelines for Securing Wireless Local Area Networks (WLANs)
NIST SP 800-160 Vol 1	Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
NIST SP 800-171	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
NIST SP 800-171A	Assessing Security Requirements for Controlled Unclassified Information

1.4 IT SERVICE DELIVERY

The Contractor must adopt, apply, and help institutionalize the IT Delivery Standards of the Defense Enterprise Service Management Framework (DESMF) and the TBM value-management framework – informed and enabled by best practices and norms from bodies of knowledge such as the Information Technology Infrastructure Library (ITIL®), Control Objectives for Information and Related Technologies (COBIT®), the Capability Maturity Model Integration (CMMI®), Six Sigma, International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 20000, ISO/IEC 27001, and Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK®).

2.0 CONTRACTOR PERSONNEL

2.1 QUALIFIED PERSONNEL

The Contractor must provide qualified personnel to perform all requirements specified in this Scope of Work, including the functional and technical services that are the responsibility of the following roles that are required to support of the DoD RMF process:

- Information System Security Officer (ISSO)
    - The ISSO is an individual assigned responsibility for maintaining the appropriate operational security posture for an information system.
- Alternate Information System Security Officer (AISSO)
    - The AISSO assists in the day-to-day duties required to safeguard the information system as assigned by the ISSO.
- Information System Security Engineer (ISSE)
    - The ISSE applies scientific, engineering, and information assurance principles to deliver trustworthy systems that satisfy stakeholder requirements with their established risk tolerance.
- Security Control Assessor (SCA)
    - The SCA is responsible for conducting a comprehensive assessment of implemented security controls and enhancements to determine the effectiveness of the controls.

The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. Contractor personnel performing cybersecurity functions must meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel must be appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the performance period. Per DoD Information Assurance Workforce Improvement Program, DOD 8570.01-M (series), waivers and exceptions for Contractor certifications will not be granted.

Contractors that access USCG IT must also follow USCG Cybersecurity guidelines and provisions and may be required to complete a System Authorization Access Request (SAAR) DD-2875.

2.2 CONTINUITY OF SUPPORT

The Contractor must ensure that the contractually required level of support for this requirement is maintained at all times. The Contractor must ensure that all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor must provide e-mail notification to the Contracting Officer's Representative (COR) prior to employee absence. Otherwise, the Contractor must provide a fully qualified replacement.

2.3 KEY PERSONNEL

Key personnel are Contractor personnel in positions that the Government considers to be essential to the performance of this contract. Before replacing any individual designated as Key by the Government, the Contractor must notify the Contracting Officer (KO) no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed

substitute(s). All proposed substitutes must possess qualifications equal to or superior to those of the Key person being replaced, unless otherwise approved by the Contracting Officer. The Contractor must not replace Key Contractor personnel without approval from the Contracting Officer. The following Contractor personnel are designated as Key for this requirement. Note: The Government may designate additional or different Contractor personnel as Key at the time of individual task order awards.

- Program Manager
- Task Order Project Manager(s)

2.4 PROGRAM MANAGER

The Contractor must provide a Program Manager who must be responsible for all Contractor work performed under this Scope of Work. The Program Manager must be a single point of contact for the Contracting Officer and the COR. The name of the Program Manager, and the name(s) of any alternate(s) who must act for the Contractor in the absence of the Program Manager, must be provided to the Government as part of the Contractor's proposal. The Program Manager is further designated as Key by the Government. During any absence of the Program Manager, only one alternate must have full authority to act for the Contractor on all matters relating to work performed under this contract. The Program Manager and all designated alternates must be able to read, write, speak and understand English. Additionally, the Contractor must not replace the Program Manager without prior approval from the Contracting Officer.

2.5 PROJECT MANAGER

The Project Manager(s) for operations and technical oversight will be responsible for the day-to-day Task Order operations of the contracted functions at all locations covered by a contract task order. This position will be focused on scheduling personnel, staffing levels, providing appropriate measurement criteria on a daily, weekly, monthly, quarterly, and annual basis. This position is responsible for coordinating all aspects of onboarding and departing contractor personnel, including coordinating with the Command/Division Security Office and Property Control Officer. This position will be responsible for ensuring the day-to-day operations are aligned to meet the USCG goals and targets, and for analyzing statistical data to optimize staffing. The Project Manager will be responsible for overseeing the proper operation of Task Order resources including but not limited to the tools used to support the contracted functions. The Project Manager will be responsible for making continuous improvement recommendations to the COR on the operation of the contracted functions.

The Project Manager must be available to the COR via telephone between the hours of 0800 and 1600 EST (*UTC -5*), Monday through Friday, excluding Federal holidays, and must respond to a request for discussion or resolution of technical problems within 2 hours of notification.

2.6 EMPLOYEE IDENTIFICATION

Contractor employees visiting Government facilities must wear an identification badge that, at a minimum, displays the Contractor name, the employee’s photo, name, clearance-level and badge expiration date. Visiting Contractor employees must comply with all Government escort rules and requirements. All Contractor employees must identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

Contractor employees working on-site at Government facilities must wear a Government issued identification badge. All Contractor employees must identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

2.7 EMPLOYEE CONDUCT

Contractor's employees must comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor must ensure Contractor employees present a professional appearance at all times and that their conduct must not reflect discredit on the United States or the Department of Homeland Security. The Project Manager must ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

2.8 REMOVING EMPLOYEES FOR MISCONDUCT OR SECURITY REASONS

The Government may, at its sole discretion (via the Contracting Officer), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

3.0 OTHER APPLICABLE CONDITIONS

3.1 SECURITY

The performance of this Contract requires the safeguarding of classified and Sensitive but Unclassified (SBU) information. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

Classified information is U.S. Government information which requires protection in accordance with Executive Order 13526, "Classified National Security Information," and supplemental directives. The Contractor shall abide by the requirements set forth in DD Form 254, Contract Security Classification and the National Industrial Security Program Operating Manual (NISPOM), 32 CFR Part 117, for protection of classified information as directed by the Federal Acquisition Regulation (FAR) 52.204-2, Security Requirements (Mar 2021). The maximum level for this IDIQ is up to SECRET.

Specific Task Orders will included standard security requirements to access classified related information, along with the associated DD Form 254, as applicable. Access to all classified information is based on a strict need-to-know principle. Contractor personnel will be performing specific classified related tasks based on the stakeholders' requirements. The Contractor will be required to access classified information; participate in classified meetings; access classified IT/IS; and may include only physical access to classified areas to support specific delivery tasks.

The Contractor's facility must have a current Facility Clearance (FCL) at the SECRET level for the overall conditions of this Contract at the time of award. Any subcontractors identified for approval must possess a FCL at the appropriate classification to support classified related tasks.

Contractor personnel must possess U.S. Citizenship and must have a current background investigation to obtain a final Personnel Clearance (PCL) at the SECRET level based on mission support. Persons determined by the Government to be a substantial risk to U. S. national security interests will not be employed under the Contract.

Contractor personnel shall maintain their security clearance eligibility for the duration of the Contract. All designated Contractor personnel working this contract must have a Classified Information Non-Disclosure Agreement (SF-312) properly executed by their contracting company's Facility Security Officer (FSO) and file with their clearance granting authority. There is no requirement for the Contractor to process or store classified information at the company-owned facilities.

The Contractor shall provide a Visit Authorization Letter (VAL), equivalent ot the USCG Visit Access Request (VAR), to the place of performance. All requests shall contain the information required by the NISPOM and shall not exceed the completion date of the contract, or a 12-month period, whichever is shorter. Additionally, the VAL shall note the applicable Government COR or Technical Assistant (TA) responsible for coordinating the visit so that the host location can verify "Need-to-Know," as necessary.

Contractors who work in a DHS/USCG installation and/or Government-leased facilities and are embedded or integrated within a program or activity, shall report all adverse information, suspicious contacts, and other reportable incidents to the local Command Security office.

Any misconduct/wrongdoing of a Contractor, modification to the contract, or changes to the company ownership status which could have an adverse impact upon national security must be reported immediately by the Contractor to the Contract Officer or a Contract Officer Designated Representative.

Contractor personnel working on-site at Government facilities shall comply with all installation security requirements and all security regulations and directives for this Contract.

Contractor performance may require OCONUS support for CG missions. Any travel overseas for classified support shall abide by the International Security Requirements as directed within the NISPOM and any additional directives by USCG.

3.1.1 Facility and Computer Access

3.1.1.1 Security Risk and Background Investigation

The requirements office anticipates the following:

Check Applicable Box	Tier Investigation	Risk	Form
X	1	Low Risk, Non-Sensitive, Physical/Logical Access (HSPD-12 Credentialing)	SF85
	2	Moderate Risk, Public Trust	SF85P
X	3	Non-Critical Sensitive, L, Confidential and Secret Information	SF86
	4	High Risk, Public Trust	SF85P
	5	Q, Top Secret, Compartmented Information, Critical Sensitive, Special Sensitive	SF86

All Contractor personnel working under this contract, at a minimum, must have a favorable fingerprint check and have the minimum Tier 1 investigation initiated or completed in order to obtain a DoD Common Access Card (CAC).

The Contractor shall require regular physical access to the U.S. Government facilities/IT systems under this acquisition, so Contractor personnel shall undergo a security check and obtain a CAC.

Contractors are required to return all CACs to an appropriate CG sponsor representative when no longer performing required contract tasks. This CG sponsor shall be their onsite CG supervisor, assigned Trusted Associate Sponsorship System (TASS) Trusted Agent (TA) or COR. The Prime Contractor shall be responsible for ensuring all Contractors (including subcontractors) return each CAC to the proper CG representative.

3.1.1.2 Trusted Associate Sponsorship System (TASS)

(a) "Contractor employee" means an employee of a firm, or an individual, under contract or subcontract to the Coast Guard to provide services who also requires one or more of the following:

- Physical access to multiple Coast Guard facilities or multiple federally controlled facilities on behalf of the Coast Guard on a recurring basis (a minimum of 2 times per week and/or 8 times per month) for a period of 6 months or more.

- Remote access, via logon, to Coast Guard network using Coast Guard-approved remote access procedures.
- Both physical access to Coast Guard facility and logical access, via logon, to Coast Guard networks on-site or remotely. Access to the Coast Guard network must require the use of a computer with Government-controlled configuration or use of Coast Guard-approved remote access procedure in accordance with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide.

(b) Homeland Security Presidential Directive (HSPD)-12 mandates a Federal standard for secure and reliable forms of identification for Federal employees and contractor employees. The Common Access Card (CAC) is a personal identification card for the Department of Defense/Uniformed Services and complies with HSPD-12. The Coast Guard has instituted the CAC as its HSPD-12 compliant personal identification card for contractor and subcontractor employees who are required to access a Coast Guard, Department of Defense (DOD), or other federally-controlled computer information system and/or facility, or need public key infrastructure (PKI) authentication to perform their contractual duties. The Trusted Associate Sponsorship System (TASS) is the automated application process for obtaining a CAC.

(c) Contractor and subcontractor employees working pursuant to this contract who are required to access a Coast Guard, DOD, or other federally-controlled computer information system and/or facility, or need PKI authentication to perform their contractual duties must use TASS to obtain a CAC.

(d) The Contracting Officer Representative (COR) or Assisting Contracting Officer Representative (ACOR) is the TASS Trusted Agent (TA) and initiates contractor accounts in the TASS, approving, returning, or rejecting CAC applications (as applicable); re-verifying assigned contractors every six months; revoking contractor and employee eligibility for a CAC.

(e) The TA ensures that contractor personnel satisfy the security requirements for CAC issuance prior to creating the CAC application in TASS. Current investigative requirements must be verified according to Commandant Instruction COMDTINST 5500.18, Coast Guard Trusted Associate Sponsorship System. The initial CAC issuance requires a favorably adjudicated Tier 1 investigation (equivalent or higher) or a Tier 1 background investigation (BI) (equivalent or higher) package that has been successfully scheduled with the investigative service provider (ISP) and a FBI fingerprint check with favorable results. The TA and Sponsor or other appropriate Federal Government representative must coordinate with the unit BI Verifier (Command Security Officer /Trusted Agent Security Manager) or the U.S. Coast Guard Security (SECCEN) to confirm the appropriate investigation has been favorably adjudicated or scheduled at the ISP with favorable FBI fingerprint results.

(f) The COR or Contracting Officer provides such forms to, or requests such information from, contractor employees that may be necessary for obtaining a CAC via the TASS. The Contractor submits completed forms and information as directed by the COR or Contracting Officer. Contractors are responsible for the accuracy and completeness of the information submitted and for any liability resulting from the Government's reliance on inaccurate or incomplete information.

(g) Contractor employees who are declined via the TASS are ineligible to perform work under this contract.

(h) When an employee with a CAC is no longer performing work under this contract, the employee must return the CAC to the COR/TA or Contracting Officer on the same day the employee stops working.

(i) The contractor must insert this clause in all subcontracts when a subcontractor's employee is required to access a Coast Guard, DOD, or other federally-controlled computer information system and/or facility, or need PKI authentication to perform contractual duties.

3.1.2 Special Categories

Actual knowledge of, generation, or production of NATO information is not required for performance on the Contract/task orders. However, Contractor personnel may require an account to access the Secret Internet Protocol Router Network (SIPRNet). Information managed under the "NATO-SECRET" caveat can be accessible via SIPRNet. Contractor personnel will require a NATO security briefing and the requisite security read-on due to NATO information residing on the SIPRNet. The Contractor will not access, download, or further disseminate any special access data (i.e., intelligence, NATO, and so forth) outside the execution of the defined contract requirements. Other classified systems may be required; and shall follow guidance of the cognizant agencies.

Contractor personnel requiring SIPRNet access must have a final SECRET clearance to obtain a SIPRNet account.

The Contractor shall adhere to the USCG rules and procedures of handling non-SCI material at the USCG government facility and/or sponsoring agency facility if access is needed to non-SCI.

The Contractor personnel requiring access to non-SCI information must be U. S. citizens; and have been granted at least a Final SECRET personnel clearance by the U. S. Government, prior to being given access to such information released or generated under this Contract.

3.1.3 Contractor Personnel Training

The Contractor shall ensure that all Contract employees with security clearances meet the prescribed security training required by the NISPOM.

All Contractors with security clearances shall comply with Insider Threat Training requirements per NISPOM. Additionally, the Contractor shall report threat-related incidents and behavioral indicators to their regional Cognizant Security Office under Defense Counterintelligence and Security Agency (DSCA) and the affected USCG Command program/project.

On-site Contractor personnel are required to attend and participate in the USCG Security Education and Awareness Training program as appropriate to the responsibilities associated with assigned duties. This also includes Government requirements training participation in rules, practices, procedures, and systems.

3.1.4 Safeguarding Sensitive Information

Contractor personnel shall safeguard and handle all sensitive information in accordance with the DHS HSAR Class deviation 15-01 clauses as applicable for proper handling and safeguarding of the security of all such USCG information, as defined in the terms and conditions of this Contract.

In accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, Contractor personnel shall safeguard this information against unauthorized disclosure or dissemination. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

3.1.5 Security Deliverables

Contractor shall provide a Training Plan within 45 days after call order award detailing how procedures are implemented for employee security briefings and certification that appropriate employees have executed a current SF-312 according to the NISPOM.

The Contractor is responsible for controlling and safeguarding For Official Use Only (FOUO) information in accordance with DHS MD 11042.1. The Contractor shall provide an OPSEC Plan within 45 days after call order award detailing how Sensitive But Unclassified/For Official Use Only material shall be handled, discussed, disseminated and protected by their employees.

3.1.6 Requirements for Providing Hardware, Software, and Services

All hardware, software, and services provided must be compliant with DHS MD 140-01 Information Technology Security Program and DHS Sensitive Systems Handbooks 4300A for Sensitive But Unclassified or 4300B for Classified Systems.

3.2 DHS-USCG ENTERPRISE ARCHITECTURE COMPLIANCE

All solutions and services shall meet DHS and USCG Enterprise Architecture (EA) policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) and USCG EA requirements:

- All developed solutions and requirements shall be compliant with the HLS and USCG EAs.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile and with the USCG IT Products and Standards Inventory.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to USCG Enterprise Architecture Division (EAD) and DHS EAD for review, approval and insertion into the USCG and DHS Data Reference Model and Mobius.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and application) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U. S. Government Version 6 (USGv6) Profile (NIST SP 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

3.3 PERIOD OF PERFORMANCE

The ordering period for this contract will not exceed sixty (60) months. The specific performance periods will be stipulated in each Task Order. The USCG may issue Task Orders at any time during the 60 month contract ordering period.

3.4 PLACE OF PERFORMANCE

The Contractor must provide on-site contract support, unless otherwise stated in individual Task Orders, which could additionally include travel to other facilities and vessels (air and sea) both CONUS and OCONUS. Physical locations include but are not limited to the following sites:

- USCG Headquarters, 2703 Martin Luther King Jr. Ave, SE, Washington DC
- USCG Surface Forces Logistics Center (SFLC), 2401 Hawkins Point Road, Baltimore, MD
- USCG SFLC Alameda Detachment, Coast Guard Island, Alameda, CA
- USCG C5ISC, 7323 Telegraph Rd, Alexandria, VA
- USCG C5ISC, 4000 Coast Guard Blvd, Portsmouth, VA
- USCG C5ISC, 408 Coast Guard Drive, Kearneysville, WV
- USCG Aviation Logistics Center (ALC), 1664 Weeksville Rd, Elizabeth City, NC

3.5 HOURS OF OPERATION

Contractor employees must generally perform all work between the hours of 0600 and 1800 EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees must be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this Scope of Work. Task Orders must specify hours of operation based on individual Task Order requirements.

3.6 TRAVEL

Contractor travel may be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the FAR 31.206-Travel Costs. The Contractor must be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

3.7 GENERAL DOCUMENTATION REQUIREMENTS

The Contractor must provide all written documentation and reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Microsoft Office Applications).

3.8 INTELLECTUAL PROPERTY

All Contractor-developed processes, procedures, documentation, photography, electronic data, all other forms of data and information collected by the Contractor in supporting the award must be considered Government property and must be provided to the Government at the end of performance in accordance with FAR Clause 52.227-14. In addition, Government property must be available for review by the COR (or other designated staff) at any time, and must be furnished to the Government as directed by the COR (or other designated staff).

3.9 PROTECTION OF INFORMATION

Contractor access to information protected under the Privacy Act is required under this Scope of Work. Contractor employees must safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

Contractor access to proprietary information is required under this Scope of Work. Contractor employees must safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. The Contractor must sign a non-disclosure statement on behalf of the company, if applicable, and must ensure that all staff, including all sub-contractors and consultants, assigned to or performing on this contract execute and adhere to the terms of the Non-Disclosure agreement (DHS Form 11000-6). Assignment of staff who have not executed this statement or fail to adhere to this statement must constitute default on the part of the Contractor.

Pursuant to DoDM 5200.01, the contractor must provide adequate security for all unclassified DoD information passing through non-DoD information systems including all subcontractor information systems utilized on contract. The contractor must disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

3.10 SECTION 508 COMPLIANCE

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it must be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT must conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions must be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

3.10.1 Section 508 Requirements for Technology Services

1. When developing or modifying ICT, the Contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation must occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.

2. When modifying, installing, configuring or integrating commercially available or government-owned ICT, the Contractor must not reduce the original ICT Item's level of Section 508 conformance.
3. When developing or modifying electronic documents and forms provided in a Microsoft Office or Adobe PDF format, the Contractor must demonstrate conformance to the applicable to the applicable Section 508 standards (including WCAG Level A and AA Level 2.0 Success Criteria) by conducting testing using the test methods published under "Accessibility Tests for Documents" at https://www.dhs.gov/compliance-test-processes.
4. When developing or modifying software functions of ICT, the Contractor must demonstrate conformance to the applicable Section 508 standards (including the requirements in Chapter 5 and WCAG 2.0 Level A and AA Success Criteria). When the requirements in Chapter 5 do not address one or more software functions, the Contractor must demonstrate conformance to the Functional Performance Criteria specified in Chapter 3. The Contractor must use a test process capable of validating conformance to all applicable Section 508 standards for software functionality delivered pursuant to this contract. The Contractor may utilize the DHS Trusted Tester Methodology for Web and Software Version 4.0 as a component of the overall test process used. This version of the test process provides partial test coverage of the Section 508 standards that apply to software. If the Contractor uses this test process, the Contractor must address the test coverage gaps through additional test procedures. Information on the DHS Trusted Tester Methodology for Web and Software Version 4.0, including coverage against the applicable Section 508 standards for software as well as gaps that need to be addressed through other test methods, related test tools, and training is published at https://www.dhs.gov/trusted-tester.

3.10.2 Section 508 Deliverables

1. Section 508 Test Plans: When developing or modifying ICT pursuant to this contract, the Contractor must provide a detailed Section 508 Conformance Test Plan. The Test Plan must describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.
2. Section 508 Test Results: When developing or modifying ICT pursuant to this contract, the Contractor must provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.
3. Section 508 Accessibility Conformance Reports: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror must provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR must be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR must be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

4.0 GOVERNMENT FURNISHED RESOURCES

The Government will provide the workspace, equipment and supplies necessary to perform the on-site portion of Contractor services required in this contract, unless specifically stated otherwise in this work statement.

Government furnished equipment and resources provided will normally be the necessary equipment/office space to accomplish tasking associated with executed Task Orders, and existing business process documentation, as necessary to perform the tasks described therein.

The following list of standard supplied Government Furnished Equipment, which is not all inclusive, include the following types of equipment and services to the Contractor's on-site support staff:

- Office space
- Desks
- Chairs
- Computer Workstations
- Licensed copies of project required software
- Telephones
- Conference rooms
- Access to printers
- Access to facsimile

Government Furnished Resources will be further specified at the task order level.

5.0 CONTRACTOR FURNISHED PROPERTY

The Contractor must furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in section 4.0 and by any more specific requirements documented at the individual Task Order level.

If necessary, and at the discretion of the Government and specified at the individual Task Order level, the Government may provide the approved Contractor personnel the ability to remotely access the Coast Guard's network in order to perform tasking off-site. This remote access capability will require compliant hardware and software, and internet service capability provided by the Contractor.

6.0 GOVERNMENT ACCEPTANCE PERIOD

The COR will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail notification to the Contractor that the deliverable has been accepted.

6.1 The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

6.2 All other review times and schedules for deliverables shall be agreed upon by the parties at the Task Order level. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

7.0 ACRONYM GLOSSARY

Table 2 Acronyms

ACRONYM	DESCRIPTION
A&A	Assessment and Authorization
ACAS	Assured Compliance Assessment Solution
ACK/NAK	Acknowledge/Not Acknowledge
ACR	Accessibility Conformance Report
AISSO	Alternate Information System Security Officer
ALC	Asset Logistics Center
ALCOAST	All Coast Guard
AOR	Area of Responsibility
ATO	Authorization To Operate
BI	Background Investigation
C5ISC	Command, Control, Communications, Computers, Cyber, and Intelligence Service Center
C5ISR	Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Reconnaissance
CAC	Common Access Card
CCRI	Command Cyber Readiness Inspection
CDR	Critical Design Review
CFO	Chief Financial Officer
CGCyber	Coast Guard Cyber Command
CID	Controlled Interface Device
CMP	Configuration Management Plan
CND	Computer Network Defense
CONOP	Concept of Operations
COR	Contracting Officer Representative
CP	Contingency Plan
CP	Contingency Plan
CSOC	Cyber Security Operations Center
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DR	Disaster Recovery

ACRONYM	DESCRIPTION
DSCA	Defense Counterintelligence and Security Agency
EA	Enterprise Architecture
EAD	Enterprise Architecture Division
EIT	Electronic and Information Technology
eMASS	Enterprise Mission Assurance Support Services
EST	Eastern Standard Time
FAR	Federal Acquisitions Regulations
FBI	Federal Bureau of Investigation
FCL	Facility Clearance
FFP	Firm Fixed Price
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FOUO	For Official Use Only
FP	False Positive
FRAGO	Fragmentation Order
FSO	Facility Security Officer
GFE	Government Furnished Equipment
GFR	Government Furnished Resources
HAG	High Assurance Guard
HBSS	Host Based Security System
HLS	Homeland Security
HSPD	Homeland Security Presidential Directive
HVA	High Value Asset
IA	Information Assurance
IAVM	Information Assurance Vulnerability Management
ICT	Information and Communications Technology
IDIQ	Indefinite Delivery Indefinite Quantity
INFOSEC	Information Security
IPT	Integrated Process Team
IPv6	Internet Protocol version 6
IRP	Incident Response Plan
IS	Information System
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISP	Investigative Service Provider
ISSE	Information System Security Engineer
ISSO	Information System Security Officer
IT	Information Technology
IV&V	Independent Verification and Validation
JFHQ	Joint Forces Headquarters

ACRONYM	DESCRIPTION
KO	Contracting Officer
LAN	Local Area Network
LN	Limited Notice
MD	Management Directive
MOU	Memorandum of Understanding
MSAM	Major System Acquisition Manual
NATO	North Atlantic Treaty Organization
NIPRNet	Non-Classified Internet Protocol Router Network
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NMAP	Non-Major System Acquisition Manual
OCONUS	Outside [the] Contiguous United States
OPORD	Operational Order
OT	Operational Technology
PCL	Personnel Clearance
PDR	Preliminary Design Review
PIT	Platform Information Technology
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PMR	Project Management Review
POA&M	Plan of Action and Milestones
PUMP	Privileged User Management Program
RFM	Request for Modification
RMF	Risk Management Framework
SAAR	System Authorization Access Request
SAR	Security Assessment Report
SBU	Sensitive But Unclassified
SCA	Security Control Assessor
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCC	Security Compliance Checker
SCI	Sensitive Compartmented Information
SECCEN	US Coast Guard Security
SELC	System Engineering Life Cycle
SFLC	Surface Forces Logistics Center
SIA	Security Impact Assessment
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SP	Special Publication
SRG	Secure Requirements Guide

ACRONYM	DESCRIPTION
SRR	Security Readiness Review
SSI	Sensitive Security Information
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TA	Trusted Agent or Technical Assistant
TASKORD	Task Order
TASS	Trusted Associate Sponsorship System
TCTO	Time Compliant Technical Order
TRM	Technical Reference Model
USCG	United States Coast Guard
VAL	Visit Authorization Letter
VAR	Visit Access Request
VAT	Vulnerability Assessment Team
VPH	Vulnerability Per Host
WCAG	Web Content Accessibility Guidelines
WLAN	Wireless Local Area Network