

UNCLASSIFIED



ENTERPRISE SECURITY AND OPERATIONS

24 OCT 2024

UNCLASSIFIED

Table of Contents

1.	General Information.....	3
2.	Title of Project	3
3.	Background.....	3
4.	Objectives.....	3
5.	Scope	3
6.	Performance Requirements	3
6.1.	Task Area 1: Physical Security	4
6.2.	Task Area 2: Police	5
6.3.	Task Area 3: Information Security.....	8
6.4.	Task Area 4: Personnel Security	11
6.5.	Task Area 5: Insider Security Program	13
7.	Contractor Personnel Qualifications/Experience.....	16
7.1.	Junior Level.....	16
7.2.	Mid-Level.....	17
7.3.	Senior Level.	18
7.4.	Expert Level.	20
8.	Security Requirements	21
9.	Reporting Requirements	21
10.	Period of Performance	22
11.	Government Furnished Property	22
12.	Travel.....	22
13.	Place of Performance	23
14.	Duty Hours.....	23
15.	Contract Personnel Requirements – Key Personnel	24
16.	Security Requirements	24
17.	Information Security.....	24
18.	Annual Training	24
19.	Contracting Office Representative (COR).....	24
20.	Non-Disclosure Requirements (NDA).....	25

1. General Information

This is a non-personal services contract to provide *Enterprise Security and Operations Support*. The Government shall not exercise any supervision or control over the service providers performing the services herein. Such service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

2. Title of Project

Enterprise Security and Operations

3. Background

The United States Government's (USG) Defense Intelligence Agency (DIA) is required to provide Enterprise Security and Operations Support to prevent, detect, protect and respond to threats to sensitive information from unauthorized access to information and or data through Physical Security, Information Security (InfoSec), Personnel Security and Insider Security Program.

4. Objectives

The objective of the Indefinite Delivery, Indefinite Quantity (IDIQ) is to acquire Enterprise Security and Operations labor support to deliver multi-disciplined security solutions and mitigations to protect DIA and enterprise partners globally. The Contractor(s) shall provide skilled, experienced professional security specialists personnel to support service related tasks across five (5) mission areas that includes Physical Security, Police, Information Security, Personnel Security, and Insider Security Program for the Defense Intelligence Agency (DIA). This effort will deliver to DIA worldwide coverage for security enabling services.

5. Scope

The scope of this IDIQ includes the full range of geographic effort that includes any component of DIA where contractor-provided security services are required. As a combat support organization, DIA's mission involves direct support to operational or deployed forces. The capability to rapidly respond to requirements for on-site security activities worldwide forms a key part of this effort. Task Requirements

6. Performance Requirements

There are five (5) mission areas, that will require support from multiple labor categories based on Task Order (TO) requirements. The experience and education for each level is in Section 6. Currently, the mission area labor categories total thirty-one (31) with the following breakout:

- Mission Area #1 Physical Security (5 labor categories)
- Mission Area #2 Police (9 labor categories)
- Mission Area #3 Information Security (4 labor categories)
- Mission Area #4 Personnel Security (7 labor categories)
- Mission Area #5 Insider Security Program (6 labor categories)

6.1. Task Area 1: Physical Security

Labor categories within the physical security mission task encompass the physical protection of sensitive or classified information, personnel, facilities, installations, other sensitive materials, resources, or processes against criminal, terrorist, or hostile intelligence activities. Within this task area, contractor personnel shall develop security policy and design, develop, evaluate, and sometimes install protection systems and devices to ensure the Government that sensitive information, equipment, and other material are not compromised, nor vulnerable to sabotaged, stolen, misused, or subjected to terrorist, malicious mischief, or other acts of willful interference. Contract personnel shall perform physical security tasks that require inspection, analysis, and evaluation of new and existing security systems to identify known vulnerabilities, determine and recommend appropriate mitigation strategies and conduct evaluations and tests of sensitive or classified information, personnel, facilities, and installations. In addition, contract personnel are required to perform comprehensive security assessments to determine and validate the adequacy of security and management control systems; monitor the process how sensitive material is handled and used; recommend the appropriate mitigation strategy after assessment has been completed and corrective action where security requirements are not being observed; and document the findings and recommendations to determine the appropriate solutions.

The following 5 labor categories are further explained between 6.1.1 through 6.1.5

- SCIF Accreditation and Inspection Specialist
- SCIF Facility Security Design Specialist
- Physical Security Specialist
- Physical Security IT Database Management Specialist
- Anti-terrorism/Force Protection Specialist

6.1.1 SCIF Accreditation and Inspection Specialist: Contractor personnel shall support government personnel in the SCIF accreditation process to include reviewing various SCIF security documents related to SCIF design, construction, and operations in accordance with DoD/IC policy and where appropriate, make recommendations to the government accreditation official to ensure accreditation. In addition, contract personnel shall conduct reviews of the SCIF Fixed Facility Checklist, TEMPEST Addendum, and other supporting documents to ensure compliance with policy during the inspection process.

6.1.2 SCIF Facility Security Design Specialist: The Contractor personnel shall integrate security considerations and systems as a function of the SCIF facility security design, construction, acquisition planning, and execution process to include identifying security vulnerabilities and implementing preventive measures to ensure the completion of the construction process or delivery of a system and/or product.

6.1.3 Physical Security Specialist: Contractor personnel shall perform physical security work to inspect, analyze, and evaluate new and existing security systems. During this process, contractor personnel shall determine whether or not the system is providing adequate protection; assess the adequacy of the security and management control systems; monitor the manner in which sensitive material is handled and used; recommend appropriate corrective action and adjustments

where security requirements are not being observed; and document the findings and recommendations.

6.1.4 Physical Security IT Database Management Specialist: The Contractor shall Provide support to ongoing inspections through updating records within the security database SASO and the IC SCIF Repository with outcomes from recent inspections and official changes that are required, including the ability to identify technical information gaps within the records, and clearly articulate information shortfalls to customers. The Contractor shall improve the current inspection model for SCIFs within DIA, DoD and DAS; accomplished through assisting teams in prioritizing inspections and offering informed immediate responses to customer inquiries. The Contractor shall increase security inspections for DIA, DoD and DAS SCIFs; accomplished through facility inspections independently and or in collaboration with Government Security Officers, and assist in decreasing the number of SCIFs that have not been recently inspected and furthering the ability of Office of Security to accomplish its responsibilities.

6.1.5 Anti-Terrorism/Force Protection Specialist: The Contractor shall conduct inspections and assessments of all government facilities to ensure protection from loss, unauthorized disclosure, espionage, terrorism, sabotage, natural disaster, or compromise of information or material which is considered vital to national defense and security, as well as to the privacy of individuals and entities. In addition, the inspections and assessments conducted includes protection of the agency's, personnel, and premises from intrusion, trespass, acts of violence, theft, or fire.

6.2. Task Area 2: Police

Labor categories within the Police mission task are concerned primarily with the physical protection of sensitive or classified information, personnel, facilities, installations, or other sensitive materials, resources, or processes against criminal, terrorist, or hostile intelligence activities. Contract personnel shall assist DIA conduct law enforcement and physical security services in furtherance of the protection of life, property and information. The following 9 labor categories are further explained between 5.2.1 through 5.2.9

- Site Rover and Relief Guard
- Guard Shift Supervisor
- Access Control Guard
- Security Operations Controller
- Access Control Specialist
- Canine Explosive Specialist
- Firearm Instructor
- Threat Management Specialist
- Police Operations Specialist

6.2.1 Site Rover and Relief (SRR): The Contractor shall provide and maintain mobile security presence to deter, prevent, and report all criminal activities and/or violations of DIA policies and regulations. The Contractor is required to respond to all Security Operations Controller (SOC) dispatch alerts for incidents and crisis response. The Contractor shall provide first response and

communicate the results of the assessment conducted back to the SOC along with any request for reinforcement or additional emergency services (fire, ambulance, hazmat, canine, EOD, etc.). In the event of imminent danger to life, the officer(s) will take immediate action in accordance with the appropriate Emergency Procedures and Use of Force Policy as prescribed in DIA Police SOPs. The Contractors shall conduct outside exterior foot patrols inside the perimeter of the fence line to ensure the security of perimeter fence and gate and ensure that the building entrances/exits are secured. The Contractor shall conduct interior foot patrols, checking SCIF boundaries, exit doors, basement doors, and roof accesses are secure. A check of all Automated External Defibrillators (AED) will be conducted by each shift every day. The Contractor shall will remain vigilant at all times and report all safety hazards, security vulnerabilities, electrical/mechanical damages/failures, and any odd or suspicious activities. The Contractor is required to respond to any miscellaneous requests for service in safeguarding lives, information, and property and aid with security procedures, general information, and directions to the general populace.

6.2.2 Guard Shift Supervisor (GSS): The Contractor shall provide daily support to the day-to-day operational management of the Access Control Guards (ACG). The Contractor shall be responsible for the day-to-day aspects of personnel management including training, scheduling, access coordination, management of resources that includes reassignment of personnel due to unexpected absence. As requested, the Contractor shall provide relief to the ACG.

6.2.3 Access Control Guard (ACG): The Contractor shall provide positive personnel identification and control through the verification of identification media. The Contractor shall monitor compliance of government established rules and regulations (32CFR). The Contractor shall take every necessary precautionary action to protect the health and safety of persons, and promptly assess all situations that involves a security violation being breached and or vulnerabilities discovered and prepare a plan of action to correct and mitigate unsafe conditions, procedures, or activities, if possible, and notification to the government of such conditions so that repairs or corrections thereto can be accomplished. The Contractor is responsible for scanning all incoming correspondence for hazardous material. The Contractor shall ensure the proper administrative control and operation of systems and equipment (screening devices, i.e., metal detectors, x-ray machines, sterilization equipment, radiation detection devices) designed for the management of property, deliveries, packages, and controlled/prohibited items and activities. The Contractor shall monitor access to all facilities by ensuring and validating positive personnel identification and control through the production, issuance and verification of identification media.

6.2.4 Security Operations Controller (SOC): The Contractor shall be responsible for monitoring the alarms of secure facilities by ensuring security personnel are alerted to the areas of the facilities where interior and exterior alarms are stationed and positioned twenty-four (24) hours, seven (7) days a week. The Contractor shall acknowledge and document the working condition of all daily security alarms. The Contractor shall maintain detailed legible alarm logs, monitor closed circuit television systems, intrusion detection systems, fire alarm systems and dispatch

UNCLASSIFIED

personnel as necessary. The Contractor shall respond to and handle all emergency calls and provide immediate assistance if requested by the Government needed.

6.2.5 Access Control Specialist: The Contractor shall monitor and maintain control of all entry access into and from DIA facilities by ensuring personnel identification throughout the production, issuance, and verification of identification media. The Contractor shall operate and ensure the proper administrative control of equipment designed for the management of property, deliveries, packages, and controlled/prohibited items. The Contractor shall monitor their compliance with all DIA's established rules and regulations. The Contractor shall promptly correct all related, documents and or reports of all identified unsafe conditions, procedures, or activities to the Sponsor/COR. The Contractor shall provide access control and related administrative processing support to include operating and maintaining manual and computer-based access control systems, databases, and equipment. The Contractor shall provide security services to DIA Visitor Centers to include processing visitors into secure facilities in accordance with site procedures. As often as possible, the Contractor shall conduct random inspections, in accordance with DIA's regulations, policies, directives to ensure prohibited items aren't introduced into DIA's facilities. The Contractor shall routinely Operate and monitor walk through metal detectors (both fixed and portable), X-ray equipment, and other site-specified equipment. ACS conduct package inspections of personnel entering/departing a facility in accordance with post/position orders. The Contractor shall monitor closed circuit television systems, intrusion detection systems, fire alarm systems and execute site-specific Security Services Standard Operating Procedures (SOPs).

6.2.6 Canine Explosive Specialist: The Contractor shall assemble a Canine Explosive Detection Team, comprised of a highly trained Explosive Detection Canine dog with an experience handler, to provide deterrent/detection capability against illegal and potentially life-threatening activities directed against DIA employees, visitors, information, programs and property. The Contractor's functional responsibilities requires conducting inspections of delivery vehicles and cargo delivered at the DIA loading dock; daily routine inspections of personnel entering DIA facilities, including vehicles and property. The Contractor shall conduct explosive detection sweeps of designated areas; clearing suspicious vehicles, packages and items discovered on or adjacent to DIA property. In addition, the Contractor shall periodically conduct roving patrols of perimeter areas for deterrent/protection purposes.

6.2.7 Firearms Instructor: The Contractor shall provide instructions to DIA personnel regarding firearms that shall include instructions on handguns, rifle, less lethal shotguns, and all related authorized weapons. The Contractor shall instruct personnel on the assembly and disassembly of firearms and related equipment. The Contractor shall conduct firearm proficiency tests in accordance with Federal/DoD requirements for handgun, rifle, and less lethal weapons authorized for carry. The Contractor shall serve as the Range Safety Officer ensuring employees adhere to Police Department range and firearm safety procedures. The Contractor shall ensure the Government that repairs of all department owned firearms are coordinated, with the manufacture/repairer, documented and maintained as needed. The Contractor shall collaborate with the Government conducting and maintaining a legible record log of all firearms and

ammunition inventories. The Contractor shall assist the Government with the performance of basic maintenance, upkeep, scheduling, inspections, and accountability for all departments indoor range and outdoor training facility to include maintenance and repairs for targets and props. The Contractor shall serve as the instructor providing training using basic police defensive tactics and use of impact weapons as well as training regarding driver programs. The Contractor shall assist the Government with developing analyzing and evaluating training requirements.

6.2.8 Threat Management Specialist (TMS): The Contractor shall provide operational support to the DIA Police program monitoring suspicious activities and suspicious persons that pose a security threat to DIA personnel property, or information. The Contractor is required to conduct routine database queries and protective intelligence analysis and threat assessments to ensure the safety of the DIA workforce. The Contractor is required to perform routine database queries and protective intelligence analysis, including data threat assessments to determine and verify the correct data to be used to perform the proper corrective action necessary to ensure the safety of the DIA workforce.

6.2.9 Police Operations Specialist: The Contractor shall assist the Activity Supply Coordinator (ASC) in maintaining 100% accountability for all inventoried police property and ensure the Government 100% compliance with firearms, radio communications and sensitive equipment inventory requirements. The Contractor shall work as the liaison with embedded shift supply officers to conduct ongoing inventory supply inspections to ensure the Government adequate reserves or surplus of critical supply items are maintained and can facilitate police equipment and uniform outfitting for police readiness and new hires. The Contractor shall assist DIA Police staff in coordinating police radio network repairs, GSA fleet records maintenance for assigned police vehicles and maintain coordination with eight (8) geographically separated facility area commanders to ensure timely scheduled maintenance and repair of assigned GSA fleet vehicles.

6.3. Task Area 3: Information Security

The following labor categories identified in the information mission task area includes a wide range of duties that contains classification, declassification, and protection of classified national defense and other sensitive information controlled by Federal agencies. Performance of this task requires identifying information that requires protection and assigns the level of protection required. The information (documents, materials, devices, industrial processes, systems, etc.) is commonly and closely contained within Federal facilities and systems including, industrial facilities, academic institutions, and other governmental organizations (foreign governments), or other designated locations.

The following 4 labor categories are further explained between 6.3.1 through 6.3.4

- Industrial Security Specialist
- Program Security Specialist
- Classification Management Specialist
- Security Awareness and Education Specialist

UNCLASSIFIED

The Contractor shall provide security guidance and conduct reviews of all DD-254s issued to contract company's providing contract support to DIA. The Contractor shall review the Contract Management System (CMS) to approve and decline if necessary request additional information associated with the Acquisition Planning Record. The Contractor shall assist the Contracting Officer (CO) in advising and introducing representative's industry (Director of Security and Facility Security Officers) and accurately prepare and submit DD Form 254s and provide security guidance to government security officials as required. The Contractor shall verify the proper Cage Code(s), Facility Clearance level and safeguarding levels within the Defense Security Service Industrial Security Facility Database for industry, awarded a DIA contract, including sub-Contractors identified by the prime to provide contract support to DIA. The Contractor shall perform their assigned daily tasks and work as the liaison between DIA stakeholders and industry partners through the pre-award phase of a contract to ensure compliance and verification of all security requirements of the Statement of Work (SOW), DD-254 and associated addendums. The Contractor shall conduct security briefings and training to ensure DIA stakeholders that all required security information and data has been identified, properly vetted and can be verified in the solicitation, SOW, DD-254 and addendums.

6.3.1 Industrial Security Specialist: The Contractor shall provide security guidance, and conduct reviews and verification of the DD-254 that outlines security requirements for handling classified information, facility changes of the contractor, the appropriate level of security protection, contract modification(s), personnel changes including foreign ownership concerns for personnel of DD-254s issued to contract company's providing contract support to DIA. The Contractor shall review the Contract Management System (CMS) to evaluate/approve/decline or request additional information associated with the Acquisition Planning Record. Assisting the Contracting Officer, Contracting Officer. The Contractor shall advise representatives to the industry (Director of Security and Facility Security Officers) and accurately prepare and submit DD Form 254s and provide security guidance to government security officials as required. The Contractor shall verify all associated Cage Code(s), Facility Clearance and safeguarding levels within the Defense Security Service Industrial Security Facility Database for industry, which have been awarded a DIA contract, including Subcontractors identified by the prime to provide contract support to DIA. The Contractor shall perform as a liaison between DIA and industry partners to ensure the appropriate level of compliance of security requirements within the Statement of Work, DD-254 and addendums. The Contractor shall perform and conduct security briefings and training identifying the required security information is identified in the solicitation, SOW, DD-254 and addendums.

6.3.2 Program Security Specialist: The Contractor shall provide support to the government Program Security Officer (PSO). The assigned PSS Contractor is responsible for program security and execution of all security policies and requirements for specified Special Access Programs (SAPs), compartments, sub-compartments, and projects. The Contractor shall draft, review, verify, edit, whenever necessary, and submit all incoming and outgoing security documentation to accredit facilities and automated information systems (AIS) in accordance with applicable policies. The Contractor shall conduct and support periodic security inspections of cleared facilities to ensure compliance with the Technical Specifications for Construction and

Management of SAP Sensitive Compartmented Information Facilities, the National Industrial Security Programs Operating Manual (NISPOM), the NISPOM supplemental, and in accordance with any related unique requirements of various classified programs. When necessary, the Contractor is required to Travel within the United States (CONUS plus Alaska and Hawaii, but not the U.S. Territories) to conduct and support facility inspections. The Contractor shall draft and maintain standard operating procedures (SOP), including Security Classification Guides (SCGs) and other related essential security documents and records. The Contractor shall prepare and implement a security education program for assigned personnel tailored to support programs.

6.3.3 Classification Management Specialist: The Contractor shall perform detailed analysis of classification standards, regulations, policies and procedures including quick issue resolution. The Contractor shall provide expertise support applying classification, control marking, and information dissemination principles knowledge. The Contractor shall generate, track, coordinate and respond to all related action items in a timely manner. The Contractor shall conduct research and assist DIA leadership with protection guidance products for DIA Information Security program. The Contractor shall identify and assess associated sources for classification determinations. The Contractor shall demonstrate their expertise familiarity of the SCI working environment, IC and DoD regulatory guidance including providing assistance with the implementation and education of policies, procedures, and methods for such functions and activities as: delegation and exercise of classification authority; development of classification guides, document marking, safeguarding, and use; physical storage and control; transmitting, transferring, reproducing, downgrading, and destroying classified information. The Contractor shall demonstrate their ability and capability to work independently without assistance on tasks identified by customer(s) and apply critical thinking skills that are essential to the development of new and innovative solutions.

6.3.4 Security Awareness and Education Specialist: The Contractor shall provide and apply knowledge as it relates to the security disciplines in response to the workforce as well as leadership inquiries. The Contractor shall prioritize, according to complexity, critical impact, and difficulty, generate, track, coordinate and respond to action items in a timely manner. The Contractor shall demonstrate to DIA leadership their ability to communicate clearly and concise through written, oral and non-traditional means of communication.

The Contractor shall develop and design security awareness products for workforce use. The Contractor shall demonstrate their experience ability and expertise to develop and provide security briefings and course instruction to small and large groups in formal and informal settings. The Contractor shall demonstrate their experience and familiarity of the SCI working environment and provide IC and DoD regulatory guidance. The Contractor shall assist with the implementation and education of policies, procedures, and methods for such daily functions and activities as: the delegation and exercise of classification authority; the development of classification guides, the classification documentation marking, safeguarding, and use; physical storage and control; and transmitting, transferring, reproducing, downgrading, destroying classified information, and other general security topics as needed. The Contractor shall

demonstrate ability to work independently on tasks identified by customer and apply critical thinking skills in the development of innovative solutions.

6.4. Task Area 4: Personnel Security

Labor categories in the personnel security mission task area include a wide range of assures the loyalty, reliability, suitability, and trustworthiness of applicants, employees, and others who work with, will work with, or have access to sensitive or classified information and material.

The following 7 labor categories are further explained between 6.4.1 through 6.4.7

- Security Support Specialist
- Personnel Security Adjudicator
- Investigative Support Specialist
- Security Screening Specialist
- Polygraph Specialist
- Polygraph Scheduling Specialist
- Personnel Security Analytical Support Specialist

6.4.1 Security Support Specialist: The Contractor shall provide customer service that includes guidance and assistance to DIA and external agency customers. The Contractor shall process all outgoing clearance certifications messages. The Contractor shall process incoming visit certifications and validating SCI accesses of visitors. The Contractor shall perform various processes for badging functions and updating personnel security systems. The Contractor shall schedule and conduct SCI indoctrinations/debriefs and uploading related documents. The Contractor shall Process Personal Electronic Devices (PED) and systems access requests. The Contractor shall implement a badging process that includes issuance of badges and in some locations the issuance of CACs; submitting outgoing clearance requests; process systems access requests; respond to numerous requests for status updates and other routine security questions; identify element personnel that require updating of their polygraphs and investigations. The Contractor shall train part-time unit security officers in the use of security databases and tools.

6.4.2 Personnel Security Adjudicator: The Contractor shall assist the Government in assessing, vetting and certifying the trustworthiness of DIA and designated DoD-affiliated personnel for access to sensitive compartmented information, through case management, adjudication and due process. The Contractor shall review all forms for accuracy, compliance and process security clearance documentation for personnel security investigations and clearances. The Contractor shall maintain, sustain and secure all adjudicated personnel security records including databases used in the personnel security process. The Contractor shall develop recommendations with adequate and sufficient supporting rationale of data to enable the Government to decide whether to grant, deny, or revoke a security clearance or eligibility to occupy sensitive positions. The Contractor shall check and validate the status of pending cases and maintain consistent and legible suspense logs for accurate record keeping. The Contractor shall prepare written reports and briefings as required.

6.4.3 Investigative Support Specialist: The Investigative Support Specialist shall assist in an array of sensitive and complex personnel security investigations related to the personnel security investigative and vetting standards. The Contractor shall provide investigative, analytical, and administrative support in the operation of DIA's Personnel Security Program, updating ongoing DIA investigations database and controls access of sensitive information, preparing investigative files, to include proper handling, filing, retention, and retiring of investigative reports (such as classified information with bilateral diversion and financial investigations); information includes personnel information, database queries, and equipment inventories. The Contractor shall conduct database and Internet research in support of personnel security investigations, searches for information used in case analysis to developing investigative leads, including background checks on names, phone numbers, and telephone activity from sources such as investigative reports and various news media outlets. Completes investigative activities to include personnel security interviews. The Contractor shall draft and submit all related Investigative Reports and document security vetting interviews in accordance with DIA standards.

6.4.4 Security Screening Specialist: The Security Screening Specialist shall conduct personnel security screening of DIA civilian applicants requiring access to sensitive government information or secure worksites. The Contractor shall assess all individual's reliability and loyalty to United States. This requires collecting personal information from individuals, with their consent and vetting information from law enforcement, intelligence agencies and other sources. The Contractor shall conduct Polygraph sessions to determine clearance and access eligibility (initial and continuing) for the Agency's workforce as well as for other Agency needs. The Contractor shall administer polygraph examinations in accordance with federal and DIA policies, practices and procedures to applicants, civilian employees, military assignees, Contractors, consultants, agency-affiliated personnel, and other personnel approved by DIA to undergo such examinations. The Contractor shall utilize testing techniques, formats, forms, and procedures, which have been approved by DIA. The Contractor shall provide valid, reliable, and timely examinations including examining products in accordance with federal and DIA policy. The Contractor shall perform duties as the Polygraph Specialist and is required to have graduated from the Psychophysiological Detection of Deception (PDD) Program taught by the National Center of Credibility Assessment (NCCA) or be a graduate of a program taught by NCCA that is equivalent. The Contractor, is required to have attained and maintained Federal Polygraph Continuing Education Certification Program (FPCECP) standards. The Contractor's body of work requires strict adherence to the highest Federal ethical standards. The Contractor shall conduct pre-test, data collection, test data analysis or posttest phases in accordance with federal and DIA policies, practices, and procedures. The Contractor shall establish and maintain effective working relationships with DIA personnel. The Contractor shall communicate effectively with individuals from diverse backgrounds, or with reasonable accommodations. Write legally admissible statements on all examinations. The Contractor shall prepare a comprehensive and confidential polygraph reports. The Contractor shall effectively evaluate and score accurately polygraph charts to achieve precise suitability and analysis information. The Contractor shall operate, maintain, and calibrate polygraph instruments. The Contractor is

required to perform other duties as assigned in accordance with the terms and conditions of the scope of work of the contract.

6.4.6 Polygraph Scheduling Specialist: The Contractor is required to perform and schedule polygraph sessions in support of DIA's Personnel Security Program. The Contractor shall perform its day-to-day operation of managing and consistent scheduling to ensure DIA leadership that no inconsistent scheduling gaps occur when scheduled examinee(s) cancels or fails to show up for their appointment. The Contractor shall accurately enter verified information, incorporate any necessary corrections, enter and upload all data into pertinent databases, both internal and external to the agency. The Contractor shall be responsible for the collection and maintenance of all polygraph metrics as defined by the Agency, utilizing databases and spreadsheets to accurately track all scheduled planned maintenance. The Contractor shall coordinate with other State and local Agency offices and other federal agencies to determine the validity and accuracy of any data related to a Subject. The Contractor shall respond expeditiously to any telephonic, email, or in-person communicated inquiries administratively related to polygraph sessions, in accordance with DIA security procedures. The Contractor shall prepare, edit, format, and finalize outgoing correspondence; transmit applicable correspondence electronically, via facsimile, or make delivery using an authorized distribution or mail-handling center.

6.4.7 Personnel Security Analytical Support Specialist: The Contractor shall provide administrative security personnel support by employing sources with various skill sets and experiences in order to serve as the focal point for administrative security functions in support of national security. The Contractor shall research and examine all applicable policies related to personnel security and Insider Security Program and personnel security risk mitigation while at the same time establish and maintain an electronic database repository library source for gathering and storing these policies. The Contractor shall compose and review written security memorandums, written with proper grammar and spelling accuracy and in compliance with the DIA writing style guide. The Contractor shall maintain the personnel security mission calendar and coordinate with other administrative support to schedule meetings and mitigation panels with senior DIA officials. The Contractor shall provide their assistance in building briefing and power point presentations.

6.5. Task Area 5: Insider Security Program

Labor categories in the Insider Security Program mission task area include a wide range of experience in Security, Counterintelligence (CI), Law Enforcement (LE), Computer Network Defense (CND), and other expertise necessary to identify anomalous behavior indicative of an Insider Security Program. These labor categories identify behavior indicative of a potential threat using host-based Insider Security Program detection, analysis and correlation tools, developing a comprehensive picture of the event.

The following 6 labor categories are further explained between 6.5.1 through 6.5.6

- Security Incidents Specialist
- Insider Security Program Detection Analyst

- Insider Security Program Detection Senior Analyst
- Case Coordination Support Specialist
- Insider Security Program Risk Management Analyst
- Insider Security Program Analytical Support Specialist

6.5.1 Security Incident Specialist: The Contractor shall manage all resolution of security incidents reported by DIA affiliates and personnel through multiple forums including the DIA Counterintelligence and Security Incident Reporting Systems; advising appropriate internal and external appropriate authorities; assisting with security incident-related investigations; resolving and coordinating with DIA security leadership to plan and execute resolutions of security incidents; perform maintenance of incident logs and provide security guidance as required in accordance with DoD Manual 5200.01, DoD Information Security Program. The Contractor is required to have day-to-day working knowledge and experience of Microsoft Office Suite, specific particularly Outlook, Word and Excel. The Contactor performing the duties and responsibilities of the Security Incident Specialist shall have proven written and oral reporting skills, interpersonal skills, including the ability to articulate through verbal and or written communication at all levels of the organization and customers across geographically dispersed sites.

6.5.2 Insider Security Program Detection (ITD) Analyst: The Contractor shall perform multi-disciplinary analysis and submit in the form of a written report based on findings discovered of the analysis performed in support of DIA's Insider Security Program. The analysis performed by the Contractor, shall include but not limited to, Insider Security Program, Security, Counterintelligence (CI), Law Enforcement (LE), and Computer Network Defense (CND) to identify anomalous behavior revealing of an Insider Security Program; and uses host-based Insider Security Program detection, analysis and correlation tools to develop a comprehensive depiction of the potential threat. The Contractor shall collect(s), review(s), interpret(s), correlate(s) and analyze(s) when necessary employee related data to identify abnormal behavior and habits that results in activities indicative of a potential Insider Security Program; and employs host-based Insider Security Program detection tools to monitor employee user activity on government information technology systems. The Contractor performing the duties of the Insider Security Program Detection Analyst shall utilize a variety of databases to conduct research regarding employees whose behavior may potentially pose a security risk to DIA and prepares alerts and assessments documenting findings in accordance with ITG standard operating procedures (SOPs) and business practices. The Contractor shall join forces in a collaborative effort with Insider Security Program detection tool engineers and behavior modelers to prioritize and strategize in improving lead identification. The Contractor shall interact with and assist Security, CI, LE, and Inspector General (IG) entities in support of formal investigations and/or inquiries to resolve Insider Security Program related matters, employee misconduct, or violations of the law. At all times, the Contractor shall maintain the highest professional standards regarding personal conduct while performing work on the contract.

6.5.3 Insider Security Program Detection Senior Analyst: The Contractor shall perform the same position description as an Insider Security Program Detection Analyst. The Contractor shall

serve as the on-site program manager for ITD analyst contract personnel, overseeing administrative matters, including, but not limited to, scheduling, timecard certification and submission, leave schedules (in consultation with the Government) and nomination packages for contract personnel as vacancies occur. The Contractor shall monitor and take all preventative and or corrective measures necessary (in consultation with the Government) to maintain productivity and quality of work of each contractor, to ensure that the overall performance of the analysis is kept at a high standard of delivering professional and accurate results in accordance with ITG standards and timelines.

6.5.4 Case Coordination Support Specialist: The Contractor shall provide Insider Security Program case coordination support in support of DIA's Insider Security Program mission. The Contractor shall be responsible for all aspects of Insider Security Program case coordination, records management, security, CI, LE and/or IG to assist in ITG case coordination. The Contractor shall collect and review all related incoming correspondence, referrals, and alerts for dissemination to council members, action elements, or other DIA officials as appropriate, while documenting actions accordingly. The Contractor shall produce and disseminate council meeting agendas and briefs agenda items to DIA officials, as required. In addition, the Contractor shall produce and disseminate meeting minutes correspondence that identifies due outs to council members and action elements. The Contractor shall maintain and update all case files accordingly. The Contractor shall create security case files and validate and ensure that all personal information is correct, accurate and PII protected. The Contractor shall update employment and personal information as needed, using information from personnel and other database sources. The Contractor performing the duties of the Case Coordination Support Specialist in this position shall review all incoming correspondence and updates case files and/or internal database profiles, as appropriate. The Contractor shall periodically review a case files to ensure that all information placed in files have been properly documented, vetted and updated as needed. The Contractor shall obtain pertinent information from DIA and Intelligence Community databases or other sources of information to update files. The Contractor shall ensure the DIA stakeholders that all case files are appropriately updated and all pertinent reports and correspondence are attached to case files. The Contractor shall process all security vetting requests and provide the appropriate response in a timely manner. The Contractor shall document alleviating requests on internal database profiles. The Contractor shall provide a written and verbally brief leadership on the current status of security case updates or timelines produce case metrics information upon request.

6.5.5 Insider Security Program Risk Management Specialist: The Contractor shall provide Insider Security Program support and personnel security, risk management analyst support as part of DIA's personnel Security Program. To support this effort the, analyst shall employ various skill sets and experience personnel including, but not limited to Insider Security Program, security, CI, LE, Intelligence Analyst and/or Risk Management Analyst to assist in personnel security risk management. The Contractor shall utilize all official authorized Government approval and authorized access to a variety of intelligence and non-intelligence databases to review assess, and gather information to conduct the proper research to prepare comprehensive written products providing a summary of research, that includes analytical

methodologies to form a reasonable conclusion and assessment of the potential Insider Security Programs to DIA's mission. The Contractor shall present to the DIA Government personnel their assessment of intelligence and non-intelligence information gathered to present their best strategy to mitigate all the identified Insider Security Program and vulnerabilities of DIA. The Contractor is required to collaborate at any given time with intelligence, LE, CI, and security professionals to identify and assess all known and unknown Insider Security Program trends. The Contractor shall assist with security vetting request, reviewing available information from a variety of DIA and non-DIA sources, including relevant and definitive information to the USG lead to make the final decision and determine the correct course of action.

6.5.6 Insider Security Program Analytical Support Specialist: The Contractor shall provide continuous administrative oversite support to DIA's Insider Security Program by employing the appropriate contractor personnel with the necessary skill sets and experiences deemed necessary to serve as the focal point for administrative security functions in support of national security. The Contractor's responsibility will require researching applicable policies related to Insider Security Program and risk mitigation and maintains a repository of these policies. The Contractor is responsible for all written and review of security memorandums, and ensure the Government proper grammar, spelling accuracy, that is legible and in compliance with the DIA writing style guide. The Contractor shall maintain at all times an Insider Security Program mission calendar and coordinates with other administrative support to schedule meetings and mitigation panels with senior DIA officials. The Contractor shall assist Government personnel with building briefing and power point presentations.

7. Contractor Personnel Qualifications/Experience

7.1. Junior Level

- Demonstrates working knowledge of the concepts involved in the specific functions outlined in the specified labor category description.
- Knowledgeable of and demonstrates ability to apply IC and DoD classification guidelines and procedures.
- Demonstrates ability to work semi-independently with oversight and direction.
- Demonstrates ability to use logic when evaluating and synthesizing multiple sources of information. Demonstrates understanding of security functions meaning, importance, and implications.
- Demonstrates ability to produce timely, logical, and concise security reports, documents, assessments, studies, and briefing materials in formats including Microsoft Office tools (e.g., Excel, Word, PowerPoint, etc.), electronic/ soft copy matrices and / or web-enabled formats.
- Demonstrates ability to communicate complex issues clearly in a concise and organized manner both verbally and non-verbally, with strong grammar skills. Demonstrates proficiency using Microsoft Office tools.
- Demonstrates ability to use knowledge of the basic security principles, concepts, policies, practices, and methods of security administration in one or more labor categories.

- Demonstrates ability to recognize nuances and resolve contradictions and inconsistencies in information.
- Demonstrates working knowledge processing requests for personnel or facility security clearances and assure that all required information is provided, requesting missing information from the originators, and granting clearances when derogatory information is absent.
- Demonstrates understanding personnel investigations to identify the presence or absence of derogatory information and, with more experienced specialists, reviewing the impact of various kinds of derogatory information on the granting, denying, or revoking of security clearances.
- Demonstrates understanding of onsite physical or industrial security inspections or assistance visits and assisting in the evaluation of findings and development of recommendations for changes.
- Demonstrates understanding of information security guidance and identifying the nature of issues involved, and researching guidelines to identify the general policies and procedures that apply to their solutions.
- Desired Experience: Minimum 3 years of experience administering security functions relevant to the specific labor category, with at least a portion of the experience within the last 2 years.
- Desired Education: Bachelor's degree in an area related to the labor category from a college or university accredited by an agency recognized by the U.S. Department of Education. An additional 4 years of experience in the specific labor category, for a total of 7 years of experience in the specific labor category, may be substituted for a Bachelor's degree.

7.2. Mid-Level

- Meets all qualifications experience and education at the Junior Level
- Demonstrates comprehensive mission knowledge and skills that affirms completion of all developmental training and experiences for the labor category
- Demonstrates ability to communicate understanding from information that may be incomplete, indirect, highly complex, seemingly unrelated, and / or technically advanced.
- Demonstrates ability to use knowledge of criteria, equipment, or techniques for at least one labor category (personnel, physical, etc.) to resolve well-defined questions or conditions.
- Demonstrates ability to work independently with minimal oversight and direction.
- Demonstrates ability to collaborate and work with other IC members on information sharing, driving collection, and addressing analytic disputes and conflict resolution.
- Demonstrates ability to use knowledge of standardized applications or established variations in security criteria involving considerations such as clearance level required, adjudication of security clearances when clear-cut derogatory information is present in the investigative information, nature of materials or information to the

protected, cost-benefit relationships for security devices or equipment systems, and similar considerations.

- Demonstrates ability to determine eligibility for access to classified or sensitive information and recommending personnel security clearances/accesses in the presence of minor derogatory information (e.g., traffic violations, misdemeanors at least 5 years in the past, and similar situations).
- Demonstrates ability in inspecting facilities where security processes and methods are known to the employee, Security Programs are operated effectively, and there is no history of significant violations and deficiencies.
- Demonstrates ability in advising facility security personnel on matters required clear-cut explanations of regulations and procedures.
- Demonstrated ability in collecting information, interviewing workers, observing physical conditions and related activities concerned with violations and compromises.
- Desired Experience: At least 8 years of experience administering security functions relevant to the specific labor category with at least a portion of the experience within the last 2 years.
- Desired Education: Bachelor's degree in an area related to the labor category from a college or university accredited by an agency recognized by the U.S. Department of Education.

7.3. Senior Level.

- Meets all experience and education of the Mid-level position.
- Demonstrates in-depth knowledge and understanding of the labor category activities required to meet mission requirements.
- Demonstrates mastery of wide range of security concepts, principles, and practices to review independently, analyze, and resolve difficult and complex security problems. Such work situations may involve, for example: conflicting testimony or sources and degrees of significant information in clearance adjudication cases; overlapping and conflicting requirements within a single facility or for a geographic region; agreements with other organizations, agencies or with foreign governments for security resources and responsibility sharing; interpreting new policy issuances for application in a variety of environments and locations; adjudicating complex personnel security clearances and/or developing guidelines for applying general criteria covering derogatory information that requires extensive experience and personal judgment to resolve; or planning and recommending the installation of multilayered security systems which may involve personnel access controls, physical protection devices, monitoring equipment, security forces, remote alarm equipment, and other measures.
- Demonstrates ability to apply knowledge of Security Program interrelationships to coordinate the objectives and plans of two or labor categories; make accommodations in study or survey recommendations to allow for differing program requirements; develop and/or implement procedures and practices to cover multiple

UNCLASSIFIED

security objectives; provide advice to inter-agency or inter-organization committees and groups to identify and resolve, or to assign responsibilities for resolving, security issues; or to perform similar work. The work at this level requires knowledge of a broad range of security program relationships, or significant expertise and depth in one of the highly specialized areas of security.

- Demonstrates ability to apply policy direction to specific operating requirements and developing guidance for applying security policy, procedures, techniques, equipment, and methods to a variety of work situations and various degrees or levels of security controls.
- Demonstrates ability to apply knowledge in responding to problems or questions involving implementation of security guidelines at lower levels and in inspecting operating security programs for adequacy, efficiency, and need for improvement.
- Demonstrates ability in interpreting policy originating from higher organizational levels (or national policy), developing local policy and implementing instructions, providing authoritative interpretations and guidance to management officials and other security specialists at the same and lower levels, and for resolving issues involving conflicting security requirements.
- Demonstrates ability to work independently and with minimal oversight.
- Demonstrates ability to use knowledge of a great variety of state-of-the-art security equipment and devices in planning and implementing protective methods and security procedures. These include: fencing variations; a variety of alarm and detection devices; closed circuit television systems; locking devices for doors, windows, vaults, and gates; shielding for cables carrying ADP, communications, and other electronic impulses that might be translatable or make a facility vulnerable to penetration; computer security software; personnel control systems such as various visual and electronic badging systems; and other approaches that are designed for or applied to protecting personnel, equipment, facilities, information, processes, or signals.
- Demonstrates knowledge to consider and apply several alternatives security processes according to the security requirements for highly specific situations, availability of materials, relationships with other protective programs, and cost/benefit considerations.
- Demonstrates knowledge in administrative processes such as the status of funds for a security project; the schedule and rate of progress in construction projects; overlapping requirements to protect the security of the organization as well as the privacy and reputation of individuals in sensitive, delicate, or controversial situations. Such broad range projects often involve specialists in other security.
- Desired Experience: Minimum 12 years of experience related to the specific labor category with at least a portion of the experience within the last 2 years.
- Desired Education: Master's degree in an area related to the labor category from a college or university accredited by an agency recognized by the U.S. Department of Education; or have Bachelor's degree related to the labor category from a college or

university accredited by an agency recognized by the U.S. Department of Education and an additional 5 years of related senior experience, for a total of 17 years, as a substitute to the Master's degree.

7.4. Expert Level.

- Meets all experience and education of a Senior Level
- Demonstrates ability to define problems, manage studies and surveys to collect and analyze data to provide advice and recommend solutions.
- Demonstrates mastery of a major area of security specialization or demonstrated mastery of general security administration programs, use comprehensive knowledge of security policy requirements to function as technical authorities in assignments requiring the application of new theories and developments to security problems not susceptible to treatment by accepted security methods, technology, or procedures. In addition to mastery of the specialty area, employees at this level use knowledge of other security specialties in resolving major conflicts in policy and program objectives.
- Demonstrates extensive ability to provide strategic advice, technical guidance and expertise to a major area of security specialization or demonstrated mastery of general security administration programs, use comprehensive knowledge of security policy requirements to function as technical authorities in assignments requiring the application of new theories and developments to security problems not susceptible to treatment by accepted security methods, technology, or procedures. In addition to mastery of the specialty area, employees at this level use knowledge of other security specialties in resolving major conflicts in policy and program objectives.
- Demonstrates knowledge of other security specialties in resolving major conflicts in policy and program objectives.
- Demonstrates knowledge in applying key decision-making and policy-developing responsibilities in very difficult assignments such as planning for significantly new or far-reaching security program requirements, or leading or participating as a technical expert in interagency study groups for resolving problems in existing security systems and programs requiring innovative solutions.
- Demonstrates knowledge in advising top level agency security and subject-matter managers on new developments and advances in security techniques in the specialty area.
- Demonstrates knowledge in recommending methods for enhancing efficiency of security systems through modifications and applications of evolving technology; evaluating and making recommendations concerning overall plans and proposals for major agency and interagency security projects; and implementing national level guidance in agency standards, guidelines, or policies for major security programs.
- Minimum 20 years of experience conducting analysis relevant to the specific labor category with at least a portion of the experience within the last 2 years.

- Desired Education: Master's degree in an area related to the labor category from a college or university accredited by an agency recognized by the U.S. Department of Education.

8. Security Requirements

The Contractor shall possess a Top Secret (TS) facility security clearance. Contract employees shall be United States (U.S.) citizen possess and maintain a final TS personnel security clearance issued by the Office of Personnel Management (OPM), the Defense Industrial Security Clearance Office (DISCO), or another government agency for contract personnel providing support to referenced contract in accordance with DoD 5200.2-R (DoD Security Program), DoD 5105.21, Vol 1-3 (Sensitive Compartmented Information Administrative Security Program), and Intelligence Community Policy Guidance number 704.1 (Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information). The Facility Security Officer (FSO) or Contract Special Security Officer (CSSO) must ensure that contract personnel who have been nominated to support the referenced contract have completed actions to take an ownership or servicing role within DISS under its CAGE Code. The FSO or CSSO is required to verify that the nominated contractor possess a final Top-Secret clearance based upon a current Single Scope Background Investigation (SSBI)/Tier 5 (T5), Periodic Re-investigation (PR)/Tier 5 PR (T5 PR) or Phased Periodic Re-investigation (PPR). If the current investigation is out-of-scope, the FSO or CSSO must have initiated a PR/T5 PR and it must be reflected in DISS prior to submitting an SCI nomination.

9. Reporting Requirements

9.1 Picture ID Cards/Site Access Records Report (Refer Addendum 1. CDRL 001): The Contractor shall keep daily legible security logs of all the activities, start/end shifts and cumulative house, and location of personnel accessing DIA site/facility and provide copies monthly to the COR, AO or designee via encrypted electronic file. This documentation will be required for compliance with the CAP and the Sensitive Compartmented Information Facility (SCIF) accreditation and shall be maintained in electronically and I hard copy form.

9.2 Inspection/Observation Reports (Refer Addendum 1. CDRL 002): The Contractor shall provide monthly site report via secure encrypted electronic data file. Reports shall be vendor format as approved by the Authorizing Official (AO) approved CSP. Security incidents or non-compliance events shall be immediately reported to SSM, local security office, AO or designee. The COR shall be notified in writing within 24 hours of an issue. This documentation will be required for compliance with the CSP and the Sensitive Compartmented Information Facility (SCIF) accreditation and shall be maintained in electronically and in hard copy form.

9.3 Security Incidents Reports (Refer Addendum 1. CDRL 003): The Contractor shall use secure communications when submitting security incidents reports; initial and monthly will be send to both the COR and AO designated security office as identified in the CSP. Initial incidents shall be reported immediately to the designed security office, AO, designee and followed up in writing within 24 hours. All document and reports will be required for compliance with CSP and

Sensitive Compartmented Information Facility (SCIF) accreditation and will be maintained electronically and in hard copy form. All reports shall be in vendor format as part of the approved CSP.

9.4 Financial Status Report- Monthly (Refer Addendum 1. CDRL 004)

9.4.1 Financial Status- Expenditures and labor aligned with the PMP detailed monthly burn projections and expenditures at the Contract Line-item Number (CLIN)/ Accounting Classification Reference Number (CLIN/ACRN) level.

9.4.2 Monthly excel spreadsheet provided during the kick-off meeting from the Government. Format shall not change unless the government PM/COR notifies the contractor in writing. Report provided to the COR, AO or designee.

9.5 Contractor Activity Report (CAR)- Monthly (Refer Addendum 1. CDRL 005): To ensure transparency and accountability, the Contractor is required to submit activity reports on a monthly basis. Each report should include the following components: Date of Report, Reporting Period, Activities Completed, Ongoing Activities, Issues and Challenges, FTE (Filled/Vacancies).

10. Period of Performance

The period of performance shall be for one 5-year (60 months) ordering period. Individual orders will have funded and executed according to the terms and conditions of each order.

11. Government Furnished Property

The Government will contractor employees at their assigned Government work locations with the standard office furniture, equipment, and supplies that are necessary and required to perform their duties.

12. Travel

- CONUS/OCONUS travel may be required in the performance of this contract. All travel shall be approved in writing by the COR prior to making any reservations. Contractors shall consult the Defense Travel Management Office website (www.defensetravel.dod.mil) prior to traveling to obtain updated per diem rates for the locality to which they are traveling.
- Travel costs will be allowed to the extent that they are reasonable and allocable and determined to be allowable under Federal Acquisition Regulation (FAR) 31.205-46. Travel by air will be reimbursed at the actual cost incurred and will not exceed the lowest customary standard coach, or equivalent fare offered during normal business hours.
- As prescribed in FAR 31.205-46(a), travel costs for lodging, meals, and incidental expenses are limited to the maximum per diem rates in effect at the time of travel set forth in the Federal Travel Regulation (FTR); the Joint Travel Regulations, Volume 2, DoD Civilian Personnel, Appendix A; or the Standardized Regulations (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas." IAW FAR

52.216-7, the contractor may submit to the COR, in such form and reasonable detail as the representative may require, an invoice or voucher supported by a statement of the claimed allowable cost for performing this contract.

- The per diem allowance will not be allowed when the period of official travel is ten (10) hours or less during the same calendar day. Travel by privately owned vehicle will be reimbursed at the current GSA approved mileage rate. Current travel policy and per diem rates may be obtained at the following Internet site:
<http://www.defensetravel.dod.mil/site/perdiem.cfm>
- Travel Reimbursement: Only those travel costs incurred by the contractor for contracted personnel assigned and working under this SOW for the following expenses: 1) Contractor employee airline tickets, per diem, and miscellaneous incidental expenses. Such transportation costs incurred will be reimbursed at actual costs in accordance with the JTR. Per Diem is not authorized within the designated AOR unless prior written approval is granted by the COR. Per Diem is authorized during pre-deployment training. Only per diem and travel costs shall be reimbursed; incidentals and miscellaneous expenses will not be reimbursed. Regardless of amount, all travel costs shall be documented via copies of the original travel receipts, to be provided with the invoice requesting payment, providing the following information: Traveler's name, date and place (city, town, or other similar designation) of the expenses, purpose of the trip, and expense incurred.
- Local travel, within 50 miles of duty location, will not be reimbursed.

13. Place of Performance

All Contractor employees shall perform work at CONUS Government work locations in the Washington, DC National Capital Region (NCR). The NCR is defined as falling within the area contained by the legal borders of: The District of Columbia; Arlington, Fairfax, Loudon, Prince William, and Stafford counties in Virginia (including incorporated cities) and Prince George and Montgomery Counties in Maryland. Tampa, Florida, Alabama, OCONUS Government work locations in Afghanistan, and other OCONUS Government and CONUS locations to meet support to combatant commanders.

14. Duty Hours

All Contractor employees shall be required to work a 40-hour work week that may include shift work, weekends, holidays and/ or 24/7/265 to accommodate the Government's needs on first, second and third shifts. Hours and shifts are subject to change due to the need to meet mission requirements. Occasionally, compressed work schedules will be required. If invoked, compressed work schedules will be communicated from the Contracting Officer or their representative. Performance may follow a Monday through Thursday or Monday through Friday work pattern with start/end times ranging anywhere within a 24-hour period (ex. 0400-1230, 1330-2200). The Government reserves the right to adjust the work schedules as mission dictates by providing a 24-hour advanced notice.

14.1 Overtime Support: Overtime will be handled on a case-by-case basis and will be charged to the XXX CLIN. Overtime requires pre-approval from the Government, unless for an unplanned emergency. In the occurrence of an unplanned emergency, the Contracting Officer shall be informed at the beginning of the next business day.

14.2 Surge Support: Surge Support may require off shift working hours, evenings, weekends and holidays working hours. All surge/emergency work done outside the predetermines standard work week will be considered over & above and will be paid at the over and above rates established in the Task Order. Emergency personnel will be on call and response 24/7/265 to emergency situations relating to life, safety, health or exceptional damage to government equipment. All emergencies shall be coordinated through COR & Contractor PM with a phone call notification. The Contracting Officer shall be informed at the beginning of the next business day. The Contractor is required to prepare and submit to the Contracting Officer within 24 hours of an emergency a detailed written report describing the incidents.

15. Contract Personnel Requirements – Key Personnel

There are no “Key Personnel” positions in support of this contract. Key Personnel may be specified at the order level.

16. Security Requirements

If applicable, see DD Form 254 for Security Guidance. Additional security requirements for contractor employees will be detailed in each TO other.

17. Information Security

All persons performing work under this contract shall protect and safeguard information in accordance with DoD, (as applicable) and DIA directives, instructions, and procedures. These same persons shall immediately report any deviation or violation of this guidance, or any unusual or suspicious activity to the DIA Security Office. These same persons shall aid and full cooperation in any subsequent investigations or inquiries conducted by DIA or other governmental agencies.

18. Annual Training

All contractors serving under this contract are required to take all DIA mandatory training.

19. Contracting Office Representative (COR)

The Government COR will provide general instructions on limitation and deadlines, and us responsible for the administration of the IDIQ in compliance with the contract to include inspection and acceptance of deliverables. Contracting Officer (KO) designated Administrative Contracting Officer Representative (ACORs) have the same authority as the Contracting Officer Representative (COR). The COR will be designated at the TO level.

20. Non-Disclosure Requirements (NDA)

All Contractor personnel are required to sign, prior to beginning performance, a non-disclosure agreement in accordance with DFARS 227.7103-7 and/or a DSS Non-Disclosure agreement. The Contractor is bound by all NDAs signed by its employees. In the event a contractor employee violates any of the terms and conditions of the NDA, the Contractor shall be considered in breach of the contract. This could result in a termination for default.

21. Contract Data Requirements List (CDRL)(s)

- At a minimum the deliverables identified in table 1 below of this Statement of Work shall be delivered by the Contractor in accordance with the terms and conditions of the awarded contract.
- All deliverables, shall be delivered at the task order level in accordance with their respective requirements.
- The Contractor shall adhere submitting only those deliverables deemed accepted by the Government. The Contractor shall provide electronic and hard copies of the pre-award and post award documentation for review, approval, and appropriate action. Electronic copies shall be delivered via email attachment to the CO and COR as appropriate. The electronic copies shall be compatible with Microsoft (TBD) or other applications as appropriate and mutually agreed to by both parties.
- Once created, deliverables and work products are considered the property of the Government.
- All deliverables shall be deemed acceptable if the document adequately covers all required topics, meets general quality measures, and professionally prepared in term of accuracy, clarity, format, and timeliness. Quality measures, as set forth below, shall be applied to each work product received from the Contractor.
 - a. **Accuracy:** Documents shall be accurate in presentation, content, and style;
 - b. **Clarity:** Documents shall be clear and concise;
 - c. **File Editing:** Documents shall be editable by the government;
 - d. **Format:** Documents shall be transmitted via mutually agreed upon media; and
 - e. **Timeliness:** Documents shall be submitted on or before scheduled due date.

22. Financial Management

The Contractor shall provide a based on detailed estimates of the cost to complete each project; and provide monthly updates to the ODA based on reasonable assumptions in terms of cost, schedule, and performance including quality and most importantly security.

23. CONTRACTOR FDDDONTRACTOR NON-DISCLOSURE AGREEMENTS

Contractor shall complete and sign a Non-Disclosure Agreement (NDA). The Contractor shall enforce NDAs and will be held accountable by the Government for violations of the NDAs committed by its contractor employees during their performance of the contract.

24. Identification of Non-Disclosure Requirements

Identification of Non-Disclosure Requirements Because of interrelationship of contractor workforce assigned to ODA, all contractors assigned to an ODA contract shall sign a non-disclosure agreement in accordance with DFARS 227.7103-7 and/or an ODA NDA prior to starting work on this task. The NDA will be provided to contractor employees during orientation. Contractor employees must also comply with all ODA policies, rules, regulations and standard operating procedures. The contractor is bound by all NDAs signed by its employees. If a contractor employee violates any of the terms of the NDA, the contractor will be considered in breach of contract. This could result in a termination for default.

25. Contractor Information Security

Contractor Information Security Performance under the contract may require that the Contractor access data and information sensitive to another government agency, another government contractor, or of such nature that its dissemination or use other than as specified in this contract would be adverse to the interests of the Government or others. Neither the Contractor, nor its contractor employees, shall divulge or release any information developed or obtained during contract performance, except to specifically authorized Government personnel or upon written approval of the Government Contracting Officer. The Contractor shall not use, disclose or reproduce any sensitive contract information that bears a restrictive legend, other than as specified in this contract. Any question on the release ability of information, or doubt regarding a person's authority requesting any information, shall be addressed to or reported to the Government Contracting Officer. The Contractor shall direct to the Government Contracting Officer all inquiries, comments, or complaints arising from matters observed, experienced, or learned as a result of, or in connection with, its performance of this contract, the resolution of which may require dissemination of official information. The Contractor shall not release any information (including photographs, files, public announcements, statements, denials or confirmations) on any part of the subject matter of this contract, on any phase of any Government program, or regarding any individuals, without the prior written approval of the Government Contracting Officer.

26. Dress and Appearance

Contractor employees shall present a professional appearance in accordance with dress, appearance, safety, and environmental standards in accordance with and consistence with the

Contractor corporate and Client dress and appearance policy.

27. Government Furnished Training

Prior to assignment of Contractor personnel, the government shall provide, at government expense, certain government specific orientation training. This training will typically include an eight-hour orientation to the government, policies, and procedures; a twenty-four-hour specialized training program on the government security equipment systems; and a period of on-the-job training (OJT).

28. Contractor Furnished Materials, Equipment, Training, Supplies, Clothing and Equipment

- a. General: The Contractor shall be required to provide services, training, materials, supplies, clothing and equipment required to comply with this SOW unless designated as government property in this SOW. The Contractor shall be responsible for providing the resources needed to satisfy the requirements of the job functions as described within this SOW (space, computer equipment, phones, office supplies) when performance is located within Contractor provided facilities.
- b. Firearms and Ammunition: Firearms shall be furnished by the contractor to equip each armed guard while on duty. Personal owned weapons are prohibited. Attachment A specifies amount and type of ammunition, including additional rounds for contingency. Appropriate and ample supplies of firearms maintenance equipment (cleaning solvents, lubricating oil, rods, brushes and patches, and other normal maintenance tools) shall be provided by the contractor and at the contractor's expense. The contractor's employees shall inspect their assigned firearms at the commencement of each tour of duty. The Contractor shall provide a list of all firearms that will be used or stored on the premises and must be able to account for all firearms at all times. Ammunition for authorized firearms shall be provided by the contractor. The contractor shall provide a GSA approved Class V weapons storage safe to be placed at each site of performance for storage of contractor-provided firearms. Additional cartridges of ammunition shall be provided, stored, and secured in the weapons storage safe on-site by the contractor to accommodate emergencies.
- c. Identification: The Contractor shall ensure that each of the Contractor's employees assigned to this contract possesses an appropriate picture identification card or badge identifying him/her as an employee of the Contractor. This ID shall be carried at all times when the employee is on duty in government facilities. The ID will need to be coordinated with the government to ensure there are no conflicts between the Contractor identification and the government. The government may provide appropriate identification badges, emblems, or patches, which will be used in addition to identification issued by the Contractor. The Contractor shall ensure that all government-issued badges or identification documents are returned to the government immediately when employees are on extended absence from the program, terminated from the contract, or at contract expiration. These

items shall only be used for government sanctioned activities and remain the property of the United States Government (USG).

29. Transportation

The Contractor shall ensure that its employees arrive at their designated duty positions on time. Parking will be available to Contractors performing at all DIA facilities.

30. Uniforms

The Contractor shall ensure that its employees present a professional, clean appearance at all times. Security officers shall maintain uniforms, insignia, accessories, and equipment in a serviceable manner. The Contractor shall obtain uniforms, inclement weather gear, and other apparel. At a minimum, the Contractor shall have available for use for each employee the following uniform items:

- Armor, Body **N1J06 Level IIIA**
- Armor, Body, Shell
- Armor, Hard Plate
- Armor, Soft Plate
- Badge
- Baton
- Belt Keepers
- Belt, Duty, black, waist
- Belt, Web
- Boots: black
- Boots: Steel toe (for construction access)
- Cap, Wool
- Cap, Summer (expendable)
- Cap, Winter (expendable)
- Coat. Car w/hood
- Coat, Rain: yellow, security
- Earplugs (for construction access)
- Flashlight: with batteries
- Glasses: safety (for construction access)
- Gloves
- Handcuff case: black.
- Handcuffs: black or silver, S&W
- Hard Hat: White, OSHA approved (for construction access)
- Holder, ASP Baton
- Holder, Flashlight: pouch type
- Holder, Key Ring
- Holster, Dual Retention: black
- Identification name tags: worn over the breast shirt pocket.
- Jacket, Cruiser: black/navy blue

- Key: Handcuff
 - Magazine Case: black
 - Pants: black/navy blue
 - Pants, Weather
 - Radio Clip
 - Shirt, Turtleneck
 - Shirts, Long Sleeve: black/navy blue
 - Shirts, Short Sleeve: black/navy blue
 - Shoulder patches: lettered to indicate the identity of the contractor shall be worn on the right shoulder of the uniform jacket and shirt.
 - Vest, Safety: construction, type 2 (for construction access)
 - Vest, Safety: range
 - Pepper spray: Oleoresin Capsicum (OC) canister
- ** BDUs are optional uniforms with COR prior approval

31. Contractor Furnished Training

Prior to entering on duty and annually after that, all personnel will be required to complete the Department of Homeland Security and Federal Protective Service certification standards training as outlined in the Security Guard Information Manual (SGIM), attend Customer Service and OPSEC Security Awareness training.

- a. The Contractor will implement management training course for Program Manager and security personnel in lead positions. This training will be at the expense of the Contractor.
- b. In addition to CPR, first aid and AED training, the Contractor will provide any training required by the appropriate municipality, county, state or other government entity where services are being provided. This training will be at the expense of the Contractor. Currently the minimum training requirements are:
 - 16-hour initial DCJS certification (core subjects)
 - 04-hour DCJS annual recertification
 - 04-hour initial CPR certification
 - 04-hour CPR annual recertification
 - 04 hour initial first aid
 - 04-hour first aid recertification (every three years)
 - 16 hours Basic Firearms Training
 - 08-hour Annual Firearms Recertification
 - 08-hour Handcuff/Search
 - 08-hour ASP Baton Training
 - 04-hour OC Spray Training

The government firearms facilities and ranges will not be available for use by the Contractor.

- c. The contractor will implement a post training course for all security personnel. This training plan should detail initial post training for anyone starting or switching posts. Training must be at a minimum annual, and training reports shall be provided. This training will be at the expense of the Contractor.
- d. A certification of completion of all required training shall be submitted by the Contractor to the COR for each Contractor employee prior to be assigned to this contract. The Contractor shall ensure that all personnel are fully trained and ready for deployment before they are assigned to a task.

32. Standards of Conduct and Performance:

General Conduct:

- a. The Contractor shall ensure all Contractor employees assigned fully understand and comply with all aspects of this SOW and the applicable agreement.
- b. The Contractor shall be responsible for maintaining employee competency, conduct appearance, and integrity; and shall be responsible for taking such disciplinary action, with respect to the Contractor's employees, as may be necessary. The Contractor shall ensure all Contractor employees adhere to government accepted standards of conduct and performance that reflect credit on themselves, their employer, and the government. Personnel shall not wear excessive jewelry or body marking to include tattoos that can be seen on the neck and face areas or on the hands and wrists. Two ear rings are allowed as long as they do not interfere with a professional look. Nose, lip, cartilage, visible nipple, and tongue rings are prohibited. The government, at its discretion, may direct the Contractor to immediately remove any employee(s) from the work site who have been disqualified for either suitability or security reasons, who are found to be unfit to perform duties, or who have failed to comply with acceptable standards of conduct, competency, or integrity. Neglect of duties will not be condoned. This includes, but is not limited to, sleeping while on duty, unreasonable delays or failures to carry out assigned tasks, conducting personal affairs or recreational activities during duty hours, refusing to render assistance or cooperation in upholding the security of the government facilities, operations, or personnel and participation in disruptive activities which interfere with normal and efficient operations.
- c. The Contractor shall ensure all Contractor employees fully understand and comply with rules and regulations governing sexual harassment and unlawful discrimination against individuals or groups on the basis of race, color, religion, sex, and national origin.
- d. The Contractor's employees shall be on government facilities only for performance of contractual duties and not for other activities such as political or charitable activities, offerings, sales, marketing, personal visits or other purposes not related to agreement performance.

Grooming Standards:

Hair: Shall be clean, neat, and combed at all times. The length and bulk of the hair may not be excessive or present a ragged, unkempt, or extreme appearance. Hair must be arranged so it does not fall over the eyebrows, extend below the bottom edge of the collar, or block any range of view (direct and peripheral) of the guard. Guards with longer hair lengths must wear their hair up for safety reasons, or tied back in a ponytail or similar style.

Hairstyles that do not allow guards to wear headgear properly are prohibited. When tied back, the hair may not reach below the middle of the back to prevent entanglement with the duty weapon and for safety reasons. Multiple braiding is authorized. If hair extensions are used in the braiding of the hair, the extensions must have the same general appearance as the individual's natural hair. Braided hairstyles will conform to other listed guidelines. It is to be understood that wearing a ponytail or similar style may still constitute a level of risk to the wearer and as such the wearer assumes that level of risk. Hair accessories such as barrettes, pins, clips, or bands must be unadorned inconspicuous in color and placement. Beads or similar ornamental items are not authorized. Hair ornaments that do not blend with hair's natural color are not permitted. Extreme, eccentric, or faddish haircuts or hairstyles are not authorized. If a guard uses dyes, tints, or bleaches, the officer must choose a natural hair color. Colors that detract from a professional appearance are prohibited.

Male Guards: Face shall be clean shaven or may have facial hair that maintains a tidy and professional appearance. Beards or goatees must be worn in conjunction with a connecting mustache and must not exceed 1/4" in length. The appearance of all facial hair must be shaped and trimmed above the neckline. Mustaches and sideburns are acceptable as follows. Mustaches are to be kept neatly trimmed and may not extend below the corner of the mouth or above the lower level of the nose. Sideburns are to be neatly trimmed and extend no lower than the lowest part of the ear. Sideburns must be of a constant width, and end with a clean-horizontal line.

Jewelry: Neck chains and bracelets of any kind may not be worn where visible to the public. Rings may be worn, but must not detract from the official appearance of the guard and/or inhibit the performance of required duties. No headphones, ear buds, or other listening devices may be worn on the ears except those devices approved by a doctor such as a hearing aid. Male Officers may not wear earrings.

Female Guards: Fingernails must be clean and neatly trimmed. Female officers must trim nails to a length that does not detract from the official appearance of the guard, presents a safety concern, or inhibits the performance of required duties. Nail polish that detracts from the uniform, or that is extreme, is prohibited. Nail designs and multi-tone colors are prohibited.

Males and Females: Cologne and perfumes shall not be overbearing or strong, and should be sparingly used. Dress and appearance grooming standards shall be strictly enforced at all times.

33. Criminal Liabilities

- a. The Contractor and/or its employees may be subject to criminal actions as allowed by law and/or immediate removal from the work site in certain circumstances. These include, but are not limited to the following:
 1. Violations of Federal Law or the Rules and Regulations governing government protected property, 32 CFR 1903.
 2. Falsification or unlawful concealment, removal, mutilation, or destruction of official documents or records or concealment of material facts by willful omission from official documents or records.
 3. Unauthorized use of government property.
 4. Failure to cooperate with government officials, federal law enforcement officers or local law enforcement authorities during an official investigation.
 5. Disorderly conduct, use of abusive or offensive language, quarreling, intimidation by word, actions, or deed.
 6. Being under the influence of intoxicants, drugs, or substances that produce similar effects.
 7. Disseminating Law Enforcement sensitive information to unauthorized individuals.

34. Technical Requirements

- a. Enforcement Limitations: Contractor personnel have no federal authority to arrest; detain; or enforce laws. Contractor personnel are not authorized to act as federal agents or law enforcement officers. The Contractor shall immediately notify appropriate representatives of the government when law enforcement actions may be required.
- b. Deadly Force: Deadly force is defined as a degree of force that is likely or intended to cause death or great bodily harm. Deadly force is primarily a concern for persons authorized to carry and use firearms in the performance of their official duties. The use of deadly force is authorized only for the protection of one's self, government personnel and other persons under government auspices when threatened with death or serious physical injury and deadly force is necessary to prevent that harm. Deadly force is to be used only as a last resort. Deadly force shall not be used solely to protect classified information. Deadly force may be used if, during the application of non-deadly force to protect or prevent the loss of property or classified information, the life of the person applying non-deadly force or the life of another person under government auspices becomes directly endangered. All means of non-deadly force will be attempted before resorting to the use of deadly force.
- c. The government will develop, issue, and maintain post orders, procedures, and special instructions as may be necessary to inform Contractor personnel of their specific duties for each requirement. Instructions and orders shall not be removed from government property, reproduced, or copied in any manner unless authorized, in writing, by the COR. The government expects Contractor personnel to provide and

maintain professional customer service at all times. Contractor personnel shall be vigilant and alert while on duty. Contract personnel shall be physically able to meet all requirements outlined in Section 8. General Qualifications.

35. Transition Plan

- a. A final Transition/Start-Up Plan shall be delivered no later than 10 business days after the effective date of the contract. The plan shall describe the contractor's detailed approach and timeline for staffing the project and taking full responsibility and accountability for all tasks without disrupting critical ongoing activities, including any databases. Upon completion of the transition/start-up period, the following Project Management Review (PMR) shall contain a section summarizing the activities of the transition/start-up period including the successes and failures.
- b. The Government expects all personnel to be available within the planned transition/start-up schedule stated herein. These are minimum levels of FTE and the contractor shall meet or exceed the designated minimum FTE level and time frame.
- c. From date of award, SCI Nominations will be submitted within the below schedule: Within 5 days, all key personnel shall be nominated. Within 10 days, 50% of staff shall be nominated. Within 60 Days, 95% of staff shall be nominated and once reached, staffing level of 95% maintained throughout the contract.

36. Services required.

- a. General. The contractor shall provide trained employees at all times to perform the services as prescribed by the contract and Officer's Duty Book during all twenty-four (24) hour shifts. In the event of an inconsistency the contract takes precedence over other documents.
- b. Post Duty Assignment. Perform the duties outlined in the Officer's Duty Book which has been prepared for the post on all applicable shifts. This book defines the basic work to be performed including the exact hours of duty. Except for emergencies, no deviations shall be made. All Post Duty Assignments are prepared by the Contracting Officer's Representative (COR) or their designated representative. If authorized by the Contracting Officer (CO), the COR may modify, amend, and/or revise Post Duty Assignments to change shift start and stop times provided the change has no impact on the contractor's cost. Such changes shall not require modification (Amendment) to the basic contract. Changes which increase or decrease the total number of man-hours specified; increase or decrease the amount of equipment, supplies, etc.; or otherwise affect the contractor's cost must be made by the CO through a written modification (amendment) to the contract. The COR may request temporary additional services. The contractor shall provide a cleared replacement guard for each employee in the event of absence, i.e., during employee vacations, sick leave, medical emergencies, and lunch periods. Additionally, Guard Force personnel are required to provide mandatory personnel and facility physical security protection for assigned

UNCLASSIFIED

personnel regardless of US Government shutdowns, inclement weather, facility power outages etc. Guard Force personnel must remain on duty at the site until properly relieved by on coming Guard, regardless or not if scheduled shift has ended. The Defense Programs Support Activity (DPSA) must be continually manned at all times due to the sensitive nature of the work being performed at this facility.

c. Typical Duties. Post assignment duties include but are not limited to the following:

- (1) Entrance Control Post. Operate and enforce a system of personnel identification. Perform package inspection when directed to do so by the Officer's Duty Book.
- (2) Roving Patrol. Make patrols in accordance with routes and schedules established in the Officer's Duty Book.
- (3) After Hour Inspection. Perform daily physical walk through of building space every two hours after normal duties hours. Document and log findings/results of physical walkthrough inspections. Document and confiscate all prohibited items and dangerous weapons.
- (4) Escorting Visitors. Guard Force will provide security escort on an as needed basis for all visitors, vendors and facilities projects on an as need basis.
- (5) CCTV Security Operation Center. Provide 24 hour, 365 days a year manning. Monitor, document and log all fence perimeter alarms, facility IDS alarms and monitor all construction and maintenance being performed outside the building or on the property by vendors. Report all suspicious personnel or unauthorized vehicles parked near the facility to shift supervisor and Government Security personnel
- (6) Metal Detector Screening. Conduct announced and unannounced metal detector and prohibited items screening for all assigned and visiting personnel by utilizing stationary and hand-held metal detection equipment.
- (7) Traffic Control. Direct traffic (vehicle and pedestrian), control parking, etc., as prescribed in the Officer's Duty Book.
- (8) Security and Fire Systems. Monitor and operate building fire alarm and intrusion detection systems and other protection devices of building equipment.
- (9) Building Rules and Regulations. Observe building occupants and visitors and enforce compliance with posted rules and regulations.
- (10) Force Protection. Take appropriate action in response to civil disorders, terrorist threats, hostage conditions, and other adverse circumstances. Examples of such action include engagement of hostile forces, detaining and searching personnel, and summoning necessary fire, rescue, and other police personnel.

UNCLASSIFIED

- (11) Law and Order. Maintain law and order within the areas of assignment. Exercise judgment and use discretion in dealing with emergencies and security violations encountered.
- (12) Unauthorized Access. Discover and detain persons attempting to gain and/or gaining unauthorized access to the property and notifying local law enforcement as is necessary.
- (13) Facility Exercises. Participate in scheduled facility exercises i.e., Shelter in Place, Emergency Evaluation, Continuity of Operations Program etc.
- (14) Personnel Security Screening. Ensure that prohibited items are not introduced into the facility. Guard Force will screen all personnel for prohibited items which include weapons, firearms of any type, ammunition, explosive devices, illegal drugs and alcohol and specific Portable Electronic Devices (PEDs), which include personally-owned photographic, video, and audio recording equipment, and personally-owned computers and associated media. The introduction of prohibited items will be enforced in accordance with current policy.
- (15) Facility IDS Alarms. Guard Force Personnel will inform Facilities and Information personnel of a problem arises with the Intrusion Detection Systems (IDS) facilities alarms.
- (16) Cardiopulmonary Resuscitation (CPR). All Guard Personnel will be trained and certified to conduct CPR, to include certification in the operation of defibrillators.
- (17) Hazardous Conditions. Report daily potentially hazardous conditions and items in need of repair.
- (18) Reports and Records. Prepare required reports on accidents, fires, bomb threats, unusual incidents and unlawful acts and provide these reports to those officials specified by COR.
- (19) Civil Disturbances. Perform such other functions as may be necessary in the event of situations or occurrences such as civil disturbances, attempts to commit espionage, sabotage, or other criminal acts adversely affecting the security and/or safety of the Government, its employees, property and the general public lawfully in buildings or on the grounds under control of the Government.
- (20) Emergencies. In case of an emergency condition requiring immediate attention, the COR may divert uniformed personnel from their normal assigned duties to meet the condition and summon appropriate assistance as may be required. This diversion may be for a duration of up to four (4) hours, without authorization from the CO. Immediately notify the designated Government official or agency, as applicable, of action taken. No additional cost shall be charged the Government for the diversion, and

this nature shall be reported in accordance with procedures outlined in the Officer's Duty Book.

(21) Vehicles Inspections. Duties shall include conducting inspections of all vehicles and personnel entering and exiting installations including or as directed. Entry and exit inspections are authorized to prevent or deter the unauthorized entry of personnel; illegal drugs; explosives; weapons; privately owned photographic, video, and audio equipment; privately owned computers and associated magnetic media; and other prohibited items, as well as the unauthorized exit of government property from the facility. This type of inspection involves looking inside the vehicle passenger and cargo compartments, under the seats, and in the glove compartment. The operator and all occupants will be asked to exit the vehicle, and the operator will be requested to open all doors and storage compartments. All packages, boxes, bags, backpacks, and briefcases will be opened and inspected. Guard Force personnel will use their discretion in having persons not exit their vehicles in inclement weather, if persons are handicapped, or if it is otherwise impractical to do so.

37. Accountability for Government Property

All property furnished by the Government under this contract shall remain the property of the Government. Upon termination of the contract, the contractor shall render an accounting of all such property which has come into his possession under this contract. All equipment issued by the Government to the contractor will be issued on a Government Property Hand Receipt, or other similar issue document. Any property furnished by the Government to fulfill contracted requirements which is lost or damaged, resulting from improper use or negligence by the contractor's employees, shall be repaired or replaced by the Government and the cost of such repairs or replacement shall be deducted from the contractor's invoice.

38. Use of Government Property

Government property (to include telephone) shall be used for official Government business only in the performance of this contract. Government property will not be used in any manner for any personal advantage, business gain, or other personal endeavor by the contractor or the contractor's employees.

39. Safeguarding Government Property

The Contractor shall take all reasonable precautions, as directed by the Government, or in the absence of such direction, or in accordance with sound industrial practices, to safeguard and protect Government property.

40. Malfunctioning of Government Property

The Contractor shall be responsible for reporting to the COR the malfunctioning of any Government equipment used by the contractor or the contractor's employees.

41. Items to be furnished by the Contractor.

- a. Firearms and ammunition. Appropriate and ample supplies of firearms, upkeep, maintenance equipment (cleaning solvents, lubricating oil, rods, brushes and patches, and other normal maintenance tools and storage facilities outside the facility identified in this contract. Personal weapons will not be used.
 - (1) Firearms shall be handled in a safe and prudent manner. Loading and unloading of ammunition and the cleaning of the firearm will not take place in/or on the grounds of the facility identified in this contract.
 - (2) The Contractor shall provide a list of serial numbers of firearms to be used on the premises to the COR prior to the contract performance date. The list shall be kept current.
- b. Uniforms. Uniform type and wearing of same shall conform as outlined below.
 - (1) The color of the contractor's guard force uniforms shall be a color in general use by large guard or police organizations. All employees performing under this contract shall wear the same color and style of uniform. Appropriately styled feminine uniforms shall be worn by female members of the guard force.
 - (2) Appropriately lettered breast and cap badges, indicating the jurisdiction from which police authority is obtained, shall be worn as part of the uniform (providing such authority is grantable under state and local laws). Shoulder patches lettered to indicate the identity of the contractor shall be worn on the shoulder of the uniform jacket and shirt. Identification name tags shall be worn over the breast shirt pocket.
 - (3) The color of shoes will match the color of leather equipment accessories.
 - (4) The contractor shall, prior to the contract performance date, submit to the COR documentation that the following items of uniform and equipment have been issued each employee. The COR is responsible for ensuring that the uniforms furnished under this contract comply with the standards contained this Statement of Work. No guard may enter on duty until he/she has a complete uniform (including accessories meeting the standards contained in this contract).
 - (5) Health and Physical Fitness Requirements. The contractor shall insure that all employees assigned are well proportioned in height and weight, and in good general health without physical defects or abnormalities which would interfere with the performance of duties.

42. Quality Control

The contractor shall establish a complete Quality Control Program assuring the requirements of the contract are provided as specified. Within ten (10) calendar days after award, the successful contractor shall submit a copy of the Quality Control Program, in contractor format, to the COR for approval. The program shall include, but not be limited to, the following:

- a. Quality Control Inspection Check Lists to conduct inspections which shall include, as a minimum, equipment checks, uniforms and appearance checks, attendance and/or sign in/out checks, post order, certification and company identification card(s) checks, overall security performance checks.
- b. Quality Control Inspection Reports shall be prepared by approved Quality Control Monitors and remain on file at the contractor's facility for inspections made during the entire contract period. Inspection Reports shall be made available to the Government during the term of the contract.
- c. Announced inspections shall be conducted at guard posts at least once every two (2) weeks and unannounced inspections shall be conducted at least once per month. Follow-up inspections whether announced or unannounced shall be conducted in a timely manner and as necessary.

43. Disciplinary Actions

Contractor will be responsible for all employee disciplinary actions. COR will inform contractor of all infractions. Contractor will replace employees with more than 3 reported minor infractions, i.e., late for duty, incomplete/sloppy uniforms, etc., with fully cleared employees.

44. Contractor Mobilization

The Contractor's mobilization period shall commence upon contract award and continue for thirty (30) days. Immediately following the contract award date, the Contractor shall exercise all efforts to organize and implement the program in accordance with the plans presented in the Contractor's proposal. All mobilization activities shall include, but not be limited to, assignment of a qualified Program Manager (PM), program planning, operating procedure familiarization, submitting personnel security nominations to DIA for clearance processing, personnel recruiting, assignment and deployment of personnel, and preparing for assumption of contract tasks.

45. Management and Supervision

45.1 Program Manager

The Program Manager (PM) shall commence work at the beginning of the mobilization phase of the contract and shall have full authority to represent the Contractor in all matters related to program operation, including, but not limited to, procedures, schedules, program status, security, logistics, reports, briefings, and administrative matters. The Contractor shall identify an alternate PM when the PM is unavailable. The Contractor's on-duty Supervisors shall be the initial Point of Contact (POC) when a PM is unavailable. While modification should be coordinated as far in advance as possible, the COR is authorized to unilaterally change the PM's schedule based on operational requirements.

45.2 PM and/or alternate PM, shall perform program management functions that include but not limited to:

- a. Respond to all exigent or problem situations as reported or referred by the CO or COR and coordinate appropriate follow-up actions.
- b. Monitor all Contract personnel of site security services to include coordinating and ensuring adequate staffing and effective allocation of resources.
- c. Advise and assist Site Supervisor and contract personnel.
- d. Participate in site visits, conduct random site quality control, and meet with site personnel to resolve issues.
- e. Report/document issues and actions taken to resolve.

45.3 Key Personnel

45.4 The Contractor shall provide key personnel meeting the following qualifications.

- a. All Key Personnel are required to have the following minimum qualifications:

Labor Category	Minimum Qualifications
Program Manager	Possess the necessary demonstrated working knowledge and of personnel, Government project management and deliverable / report compliance. In addition, the Program Manager is required to be a Certified Program Management Professional (PMP) and or have a minimum of three (3) years of on-site experience managing Government Access Control Support Services. (Resume required)
Alternate PM	Qualified Key Personnel with at least a minimum of three (3) years U.S. of Government Access Specialist or Supervisor experience. This candidate can be a designated Supervisor or senior staff member (Resume required).
Supervisor/Access Control Specialists	Qualified Key Personnel with at least a minimum of three (3) years of experience as a U.S. Government Access Specialist or Supervisor managing day-to-day post personnel activities,

	requirements, procedures, and short-notice personnel replacement execution.
--	---

- a. The Contractor shall provide (1) PM, (1) Alternate PM, and (8 posts) Supervisor/Access Control Specialists.
- b. The PM/Alternate PM must be an employee of the prime contractor.
- c. The PM shall be assigned and working on-site from date of contract award.
- d. The PM shall interface with the COR to facilitate performance of SOW requirements, and coordination of all reports and deliverables. The PM shall normally be based at DIA HQ and shall have full authority to represent their company on all matters related to program operations, including, but not limited to, program status, security, logistics, reports, briefings, and administrative matters.
- e. The Alternate PM shall be on-site in the event of PM absence.
- f. Supervisor/Access Control Specialists shall manage day-to-day post personnel activities, requirements and procedures, inspection of uniforms, provide direction for on-the-job training, and ensure Access Control Specialists adhere to all applicable regulations, orders, policies, and procedures.
- g. Supervisors/Access Control Specialists shall be assigned and working on-site from date of contract award.

46. Substitution

- a. During the first ninety (90) days of performance, the Contractor shall make no substitutions of key personnel unless the substitution is necessitated by illness, death, or termination of employment. After the initial 90-day period, the Contractor shall submit substitution requests to the Contracting Officer and COR at least 15 days prior to making any permanent substitution.
- b. The Contractor shall provide a detailed explanation of the circumstances necessitating changing the PM or alternate PM, complete resumes for proposed substitutes, and any additional information requested by the Contracting Officer. All proposed substitutes are required to have qualifications that are equivalent to or exceed the qualifications of those of the person they are replacing.
- c. The Contractor shall notify the Contracting Officer of any changes to Key Personnel taking place after proposal submission, and prior to contract award.

Employee Orientation

The Contractor shall ensure contract personnel are adequately familiar with their assigned duties. The Contractor shall orient all newly assigned Access Control Specialists (ACS). The Contractor shall ensure that all ACS Contractors are kept up to date on regulatory and/or procedural changes.

48. Personnel Requirements

48.1 The Contractor shall only assign to this program new employees who are eligible and maintain the required security clearance, health and physical requirements, and skills and abilities for their assigned post. All Contractor personnel, within each labor category, must meet the following requirements:

- a. Possess binocular vision correctable to 20/20 and close vision correctable to Saiger No. 4 type test for both eyes, be free of color blindness, and have normal fields of vision and depth perception
- b. Be in good health without conditions which would interfere with duty performance.
- c. Have normal hearing or correctable to normal levels with hearing aids.
- d. The ability to read and understand regulations, detailed written orders, policies, and training instructions.
- e. The ability to make independent decisions in a quick and decisive manner using good judgement.
- f. The ability to maintain effective working relations with supervisors, coworkers, and Sponsor's employees.
- g. The ability to represent the organization in a professional, customer-oriented manner and effectively communicate in-person and over Information Technology systems, the telephone, and radio.

48.2 The Contractor shall conduct yearly drug screening of bodily fluids as required for all contract employees. A certification for each person attesting to final results, pass/fail, of this examination shall be furnished to the COR initially with their DIA Security Nomination package and annually thereafter.

49. Service Certification

The Contractor shall maintain records that are legible attesting to the services performed for each month of the contract. The certification shall identify the location, name of the person assigned, time started, time finished, and total hours of service performed. The COR, or an authorized representative, shall review the certification, reconcile any discrepancies with the Contractor, and approve the document, as appropriate. The certification will provide the basis for substantiation of service performed and will be used in connection with invoice approval.

50. Safety

The Contractor shall ensure all reasonable measures are taken to perform in a safe manner. The Contractor shall immediately notify the Contract Management Staff and COR of any accidents occurring on United States Government controlled property, or damage to third party property. Notification shall be followed up by written reports, as required by the Sponsor' Safety Office and COR.

51. Logistic Support

50.1 General

- a. Parking is available at the Sponsor's locations. Limited public transportation services are available.
- b. The Contractor is NOT authorized at any time during the Period of Performance of this contract to utilize government-owned vehicles.
- c. The Sponsor may provide site-specified support, including electrical and mechanical equipment, such as access control systems, computer systems, communications equipment, and official-use-only telephone service.
- d. The Sponsor shall provide written post operating procedures/orders, instructions, and administrative forms.

The Sponsor shall provide other equipment and supplies necessary for duty performance.

52. Property Control and Accountability

All Government Furnished Property (GFP) under this contract shall remain the property of DIA. The Contractor shall maintain an accounting of all such property that has come into its possession under this contract. Any GFP that is lost or damaged through improper use or negligence by the Contractor's employees shall be repaired or replaced by the Contractor at no cost to DIA. The Contractor is required to immediately report to the COR or designated ACOR, the malfunction, loss, or damage of Sponsor-provided equipment.

53. Inspection and Acceptance:

The COR will inspect and accept all deliverables and provide written evidence of acceptances to the appropriate Finance and Accounting Office.

54. Reporting Requirements

All information and data related to this contract that the contractor gathers or obtains shall be both protected from unauthorized release and considered property of the government. The Contracting Officer is the sole authorized official to release verbally or in writing, any data, the draft deliverables, the final deliverables, or any other written or printed materials pertaining to this contract. Contractor shall provide monthly status reports to include delivered products, metrics, burn rate, risks, mitigations, vacancies and future actions.

55. Personnel Standards

All personnel shall adhere to common positive and proactive standards of conduct normally found in successful private business and the DoD. Contractor management is responsible for quickly resolving all issues with regards to contractor employees, especially as it relates to programmatic performance. The Contractor will maintain continuity and expertise to ensure tasks are met and delivered on time. The Contractor shall ensure all contractor employees conduct themselves professionally and show proper tact and diplomacy while under DIA contract.

56. Surge Capability:

57. Security Investigations – SEC4

57.1 Description

Skilled, experienced, and professional Personnel Security Specialists (Screening Interviewers and a Lead Screening Interviewer) to support the Personnel Security Division and Investigations Division. Duties will include: 1) the review of SEC developed SEAD 4 adjudicative relevant information in SEC systems of record, relevant security forms, or through the continuous vetting/continuous evaluation system process; 2) conducting security screening interviews to assess and validate the trustworthiness of DIA and designated DoD affiliated personnel in response to SEAD 4 adjudicative guidelines; and 3.

58. Deliverables

Timely submission of deliverables is essential to successful completion of this requirement.

Schedules for deliverables are specified on table below.

Table 1 Contract Deliverables:

CDRL	SOW Reference	Description	Frequency	Format	Submit to
CDRL 001	9.1	Picture ID Cards/Site Access Records Report	Monthly NLT 10 th of the month	Microsoft Excel/Encrypted	Contracting Officer Representative (COR), Designee, Authorizing Office (AO)
CDRL 002	9.2	Inspection/Observation Reports	Monthly NLT 10 th of the month	Microsoft Excel/Encrypted	Contracting Officer Representative (COR), Designee, Authorizing Office (AO)
CDRL 003	9.3	Security Incidents Reports	Monthly NLT 10 th of the month	Microsoft Excel/Encrypted	Contracting Officer Representative (COR), Designee, Authorizing Office (AO)
CDRL 004	9.4	Financial Status Report- Monthly	Monthly NLT 10 th of the month	Microsoft Excel/Encrypted	Contracting Officer Representative (COR), Designee, Authorizing Office (AO)
CDRL 005	9.5	Contractor Activity Report (CAR)- Monthly	Monthly NLT 10 th of the month	Microsoft Excel/Encrypted	Contracting Officer Representative (COR), Designee, Authorizing Office (AO)

UNCLASSIFIED



UNCLASSIFIED