**Statement of Objectives**

**Student Information System, Phase Three/Four**

**Information Technology and Communications Services**

**Naval Postgraduate School**

**1.0 Background/Introduction**

The Naval Postgraduate School (NPS) located in Monterey, California supports the U.S. Navy, other military branches, and foreign military services with postgraduate education for personnel. The Information Technology and Communication Services (ITACS) Department at NPS provides information technology (IT) support to the entire school. NPS has developed a Student Information System (SIS) for student registration and management known as “PYTHON.”

Located in Newport, Rhode Island, Navy War College (NWC) provides Professional Military Education and Joint Professional Military Education and helps the Chief of Naval Operations (CNO) define the future Navy, its missions and roles, support combat readiness, and strengthen maritime security cooperation. The Information Resource Department (IRD) is the NWC’s centralized provider of information technology services. The mission of the IRD is to provide day-to-day support of the NWC in IT, video and telecommunications support. NWC currently uses the “Empower SIS”, a commercial off-the-shelf (COTS) student information system.

The current SIS is a set of applications that function as a system for managing student admissions and enrollment, track completion of classes and thesis requirements, produce transcripts, manage course evaluations, provide workflow for student add, drop and validate course requests, and perform additional functions typically needed for academic administration of a university. The current NPS SIS is also used for a variety of functions that are not typical of a university SIS, such as Active Directory account lifecycle management (create accounts, disable accounts, delete accounts, expire accounts, expire passwords, enable accounts, unlock accounts, update Global Address List information in Active Directory from updates to user information in the SIS) for all NPS users, as well as thesis approval tracking, demand-based course offering, and demand-based class scheduling. The current user base includes approximately 1500 staff faculty and 2400 students.

NPS has a requirement to replace the current developmental SIS (PYTHON) with a commercial solution that is highly functional, customizable and supports continuous IT modernization as business needs evolve over time. The new SIS shall be a cloud-based Software-as-a-Service (SaaS)/Platform-as-a-Service (PaaS) solution that has readily available architecture designed for higher education institutions. The new SIS shall also provide out-of-the-box (OOTB) configurations, natively integrate with other systems using native connections such as APIs, feature dynamic reporting functionality and contain enhanced security parameters that safeguard student privacy and meet NPS cybersecurity requirements.

NWC has the same requirement but for replacing the Empower SIS

Here also state what has been done to SIS thus far with regards to Phase 1 and Phase 2.

**2.0 Scope**

The purpose of this Statement of Objectives (SOO) is to outline the requirements for Phase Three (Minimum Viable Product) and Phase Four (Go Live) of the Salesforce Government Cloud Plus Student Information System. The contractor shall provide all required development, testing, documentation, data migration and integration services. As such, the Contractor shall provide a Performance Work Statement that outlines how the work will be completed.

**3.0 Performance Objectives**

**3.1 Phase Three (Base CLIN)**

Continue development of Minimum Viable Product (MVP) out-of-the-box Salesforce functionality. Government Cloud Plus, DoD Impact Level (IL) 4 environment. Completion of this phase will indicate MVP that is ready to begin user training and testing.

**3.1.1 Development**

**3.1.1.1 Intelligent Degree Planning & Degree Planning Templates**

* Implement the out-of-the-box Intelligent Degree Planner, which enables students to visualize their paths to degree completion.

**3.1.1.2 Course Registration**

* Enable students to register for courses using a user-friendly drag-and-drop interface, streamlining the registration process.
* Implement validation rules to ensure that NPS and NWC students do not exceed credit limits or enroll in a course without completing prerequisite courses.

**3.1.1.3 Holds and Blocks**

**3.1.1.4 User Guides and Training for New Features**

* Develop comprehensive user guides and training materials for newly implemented features.

**3.1.2 MuleSoft Integration Discovery and Setup**

* Conduct integration discovery sessions to identify and understand integration requirements.
* Create MuleSoft architectural design documents.
* Establish connections to the MuleSoft infrastructure that HigherEchelon implemented for United States Naval Academy (USNA).
* Develop API governance documentation.

**3.1.3 SIS Authority to Operate (ATO)**

* Obtain ATO for NUS-SIS Salesforce Education Cloud Component
* Review NUS-SIS eMASS package ID#16045
* Establish & Identify a set of roles and responsibilities between the teams.
* Validate system information in eMASS is current and RMF Step 1 System Categorization is correct.
* DD2930 Privacy Impact Assessment (PIA) to be completed and routing for signature
* Ports, Protocols, and Services Management (PPSM) document uploaded to eMASS
* RMF Step 2 – Control Selection
  + Document applicable Security/Privacy controls (including all required overlays) implementation narrative for RMF Step 2.
  + Submit RMF Step 2 to SCA in eMASS for acceptance to move ATO package to RMF Step 3
* RMF Step 3 – Control Implementation
  + - Implement all applicable STIG/SRG technical configurations
    - Implement all applicable Security/Privacy control technical configurations
    - Collect implementation evidence artifacts and upload to eMASS
    - Develop NUS-SIS POA&M document.
* RMF Step 4 – Validation
* Submit eMASS package for PAO validation.
* Address and mitigate any post-validation findings.
* Prepare eMASS package for final submission
* RMF Step 5 – Authorization
* Submit eMASS package to Authorizing Official (AO) for authorization decision
* Authorizing Official issues ATO for NUS-SIS

**3.1.4**  **Data Migration/Data Quality**

* Collect program, faculty, and student data required for the first pilot.
* Map the collect program, faculty, and student data to Salesforce Education Cloud data model.

**3.1.5 Training**

* Personalized Training
* Define specific learning paths for each user group to ensure relevant and effective training.
* Develop tailored training materials and resources, including comprehensive user manuals.
* Facilitate interactive training sessions, providing hands-on experience and opportunities for questions and feedback.

**3.1.6 Salesforce Pilot**

* Pilot Program Strategy for Pilot #1
* Identify and select representative faculty, staff, and student groups to participate in the pilot program.
* Develop a comprehensive pilot program that outlines objectives, activities, and expected outcomes tailored for faculty, staff, and students.
* Provide training and orientation sessions for participants to ensure they understand the program’s goals, processes, and tools.
* Plan and migrate data into Salesforce in preparation for Pilot #1

**3.2 Phase Four (Option CLIN)**

Complete final development, integrations and testing for a full system Go Live. Completion of this phase will be a roll out to NPS and NWC users.

**3.2.1 Development**

**3.2.1.1 Agentforce**

* Implement Agentforce (AI) to enable the use of autonomous agents. These agents will provide personalized support to NPS and NWC candidates throughout the admission process. They will assist students by offering information and recommendations on key dates, such as drop deadlines, and guiding them on how to enroll in independent study courses, available 24/7. Additionally, Agentforce will generate student summaries for faculty and college staff, providing insights into each student’s journey.

**3.2.1.2 Continue Implementation of New Salesforce Education Cloud Features**

* Monitor and implement new features for Education Cloud as prioritized by NPS and NWC.
* Provide ongoing support and training on new functionalities as they become available.

**3.2.1.3 User Guides and Training**

* Develop comprehensive user guides and training materials for newly implemented features.

**3.2.2 MuleSoft Integration**

* Implement MuleSoft integrations for:
* Bursar/Tuition Tracking, unless it is determined that the app can be rebuilt in Salesforce (NPS)
* Agreements, unless it is determined that the app can be rebuilt in Salesforce (NPS)
* 25Live (NWC)
* Active Directory (NPS, NWC)
* Create integration design documents for each system
* Develop test plans and document results for each integration.
* Produce user guides for the functions of the integrated systems.

**3.2.3 Data Migration**

**3.2.3.1 Program, Faculty and Student Data Migration – Pilot #2**

* Collect data required for Pilot #2
* Map data to Salesforce Education Cloud
* Migrate mapped date into Salesforce

**3.2.3.2 Prepare Data for Agentforce**

* Prepare migrated data to endure compatibility Agentforce model.

**3.2.4 Agentforce Integration Authority to Operate (ATO)**

* FedRAMP authorization
* Submit NUS-SIS for re-authorization with Agenctforce integration

**3.2.5 Training**

* Define specific learning paths for each user group.
* Develop tailored training materials and resources.
* Facilitate interactive training sessions.

**3.2.6 Salesforce Pilot**

**3.2.6.1 Pilot Execution – Pilot #1**

* Implement mechanisms to collect feedback and data and analyze results.
* Conduct a success first pilot with faculty, staff and students.

**3.2.6.2 Pilot Program Strategy and Execution – Pilot #2**

* + Identify and select representative faculty, staff and student groups.
  + Develop a comprehensive pilot program.
  + Provide training and orientation sessions.
  + Implement mechanisms to collect feedback and data and analyze results.
  + Conduct a success first pilot with faculty, staff and students.

**4.0 Period of Performance**

Base CLIN (Phase Three): 4/1/25 – 9/30/25

Option CLIN (Phase Four): 10/1/25 – 3/31/26

**5.0 Place of Performance**

All work shall be performed remotely at the contractor’s place of business unless otherwise required by specific technical circumstances.

**6.0 Work Week and Hours of Operation**

The Contractor shall provide services during normal working hours excluding federal holidays. Normal working hours are 0800-1630 Pacific Standard Time Zone (PST), Monday through Friday, unless requirements dictate otherwise. Exceptions can be permitted by the COR upon request and at the COR’s discretion.

Following is a list of holidays observed by the Government.

Name of Holiday Time of Observance

New Year’s Day 1 January

Martin Luther King Jr. Day Third Monday in January

President's Day Third Monday in February

Memorial Day Last Monday in May

Juneteenth Independence Day 19 June

Independence Day 4 July

Labor Day First Monday in September

Columbus Day Second Monday in October

Veteran's Day 11 November

Thanksgiving Day Fourth Thursday in November

Christmas Day 25 December

If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be observed by the Contractor in accordance with the practice as observed by the assigned Government employees at the using activity.

**7.0 Security Requirements**

All Contractor Key Personnel must be U.S. citizens. The Contractor is responsible for ensuring personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01M, “Information Assurance Workforce Improvement Program”. The Contractor shall meet the applicable information assurance certification requirements, including:

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD8570.01--M; and (2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01--M.

Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions. Contractor personnel who do not have the appropriate and current certifications shall be denied access to DoD information systems for the purposes of performing information assurance or cybersecurity functions. This Position has been determined to require professional certification at the IAT Level II. The contractor shall provide evidence the personnel filling this position have a current COMPTia Security+ (or approved equivalent as determined by the approved IA baseline certification table (located at https://public.cyber.mil/cw/dcwf/ -OR- https://cool.osd.mil/usn/cswf/index.htm) and it shall be maintained for the entire period of performance at the cost of the Contractor.

The Contractor Personnel do not require access to classified information or material and do not require a security clearance for the tasks on this PWS. The contractor will follow the check in process through the Security Manager’s office.

Government POC (COR, ACOR or TPOC, etc.) shall make contact with the Facilities Security Officer or Security POC, prior to the arrival of the contractor, to coordinate various security requirements with the Requiring Activity’s Security Manager (RASM). Examples of such requirements include, but may not be limited to, the following: initiation of security background investigations, security in-processing, security briefings, coordinating applications for the Contractor Verification System, applying for a Common Access Card for the appropriate Government facility, access to Government IT systems and Security Out-Processing.

Prior to the arrival of the Contractor Personnel, the COR/TPOC must submit a Contractor Processing Check In form and ensure the Contractor coordinates all security and access requirements directly through the Requiring Activity’s Security Manager (RASM). The following security requirements are mandatory for all contracts and at all locations:

(1) Identify investigation requirements in accordance with SECNAV M-5510.30: DoN Personnel Security Program Manual and NAVSUPINST 5530.1E: Naval Supply Systems Command Security Manual. (All personnel working for the government require a favorably completed investigation.)

(2) Identify Information Assurance (IA) requirements, to include IA training requirements.

(3) Annually, and upon change, provide the RASM with an accurate roster of all contractor personnel working under this contract (to include task orders, modifications, etc.).

(4) In accordance with SECNAV M-5510.36: DoN Information Security Program Manual, all contracts requiring access to classified information or material shall include a valid DD Form 254 approved and endorsed by the RASM.

Government POC must contact security prior to on-boarding contractor:

* Provide security with contractor name, SSN, Date and Place of Birth. This information MUST be provided to the security manager office via phone (831) 656-2450.
* Contractor will be requested to provide U.S citizenship documentation, if contractor is local, he/she can bring citizenship documentation to the Security Manager’s office. Citizenship verification can be U.S. birth certificate, U.S. passport, or U.S. Naturalization Certificate. If unable to come in person, that information may be mailed. It must be original documentation, or a property notarized copy:

Security Manager Code 00M

Naval Postgraduate School

1411 Cunningham Rd, Rm B-13

Monterey CA, 93943-5015

Security shall:

* Verify a copy of the contract
* Verify performance work statement
* Verify the fully executed DD-254 (if classified requirement)
* Citizenship verified
* Check for existing background check or start background investigation
* Fingerprinting process can begin by making an appointment at NPS or convenient local installation to the contractor – Fingerprints must be done with Livescan. Hard copy fingerprints are not authorized.
* If CAC is required, confirm when issuance is ready, COR/TPOC will be notified
* If CAC is not required, COR/TPOC will be notified to contact NSAM/VCC to get a DBIDS card

**8.0 Data Rights**

It is the Government’s intent to retain unlimited rights to all software, documentation, and data first produced in performance of this contract.

**9.0 Privacy Act**

“Pursuant to Title 5 United States Code 552a(m)(l), the contractor and all employees of the contractor working under this contract are required to comply with the requirements of 5 U.S.C. 552a (“The Privacy Act of 1974”).”

**10.0 Identification of Contractor Employees**

In accordance with DFAR 211.106, there shall be a clear distinction between Government employees and service contractor employees. Service contractor employees shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel. Contractor personnel will be required to obtain and wear badges or other visible identification for meetings with Government personnel to provide a clear distinction between service contractor employees and Government personnel. In addition, contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

**11.0 Non-Personal Services**

Contractor employees performing services under this order will be controlled, directed, and supervised at all times by management personnel of the contractor. Contractor management shall insure employees properly comply with the performance work standards outlined in the SOW. Contractor employees shall perform their duties independent of, and without the supervision of, any Government official or other Defense Contractor. The tasks, duties, and responsibilities set forth in the task order may not be interpreted or implemented in any manner that results in any contractor employee creating or modifying Federal policy, obligating the appropriated funds of the United States Government, overseeing the work of Federal employees, or otherwise violating the prohibitions set forth in Parts 7.5 and 37.1 of the Federal Acquisition Regulation (FAR). The Government will control access to the facility and will perform the inspection and acceptance of the completed work.

**12.0 SUPTXT 204-9400 (3-19) CONTRACTOR UNCLASSIFIED ACCESS TO FEDERALLY CONTROLLED FACILITIES, SENSITIVE INFORMATION, INFORMATION TECHNOLOGY SYSTEMS OR PROTECTED HEALTH INFORMATION**

Executive Order 13467, Reforming Processes Related to Suitability for Government Employee, Fitness for Contractor Employees and Eligibility for Access to Classified National Security Information, Homeland Security Presidential Directive (HSPD)-12, requires government agencies to develop and implement Federal security standards for Federal employees and contractors. The 5 CFR 32 Part 157 in concert with DoD Manual 1000.13, Vol 1, implements the Federal Standards.

APPLICABILITY

This text applies to all DoD sponsored individuals who require CAC eligibility (or login and P/W if acceptable per contract) for: Physical access to DoD facilities or non-DoD facilities on behalf of DoD; Logical access to information systems (whether on site or remotely); or remote access to DoD networks that use only the CAC logon for user authentication, or access to sensitive and protected information. This applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

Each contractor employee providing services at a Navy command under this contract is required to obtain a DoD CAC. Additionally, depending on the level of computer/network access, the contract employee will require a successful investigation as detailed below.

Per HSPD-12 and implementing guidance, all contractor employees working at a federally controlled base, facility or activity under this clause will require a DoD CAC. When access to a base, facility or activity is required contractor employees shall in-process with the Command's Security Manager (CSM) upon arrival to the command and shall out-process prior to their departure at the completion of the individual's performance under the contract.

START-UP PERIOD

All contractor resource onboarding documents must be submitted via the prime contractor. The prime contractor shall make all necessary preparations to assume full responsibility for productive performance as of the performance start date.

Definition of "productive":

a. Visit Authorization Request (VAR)

b. Contractor Information Sheet (CIS)

c. FD-258 Fingerprint Card

d. Completed Electronic Investigation (EQIP)

e. All contractor resource(s) must have an active Joint Personnel Adjudication System (JPAS) profile

f. Common Access Card (CAC)

Note (1): Invoicing by the contractor will begin as of the commencement of the performance period of services and no reimbursement will be paid by the government for efforts expended during the start-up period.

Note (2): Foreign Nationals are not allowed access to the functional/system side of Enterprise Resource Planning (ERP).

ACCESS TO DOD INFORMATION TECHNOLOGY (IT) SYSTEM

In Accordance With (IAW) Secretary of the Navy (SECNAV) M-5510.30, contractor employees who require access to Department of the Navy (DoN) or DoD networks are categorized as IT-I, IT-II, or IT-III. The IT-II level, defined in detail in SECNAV M-5510.30, includes positions which require access to sensitive information. Sensitive information includes information protected under the Privacy Act, to include PHI. All contractor employees under this contract who require access to Privacy Act protected information are therefore categorized no lower than IT-II. IT Levels are determined by the requiring activity's Command Information System Security Manager (ISSM)/Information Assurance Manager (IAM).

Contractor employees requiring privileged or IT-I level access, (when specified by the terms of the contract) require a Single Scope Background Investigation (SSBI) or T5 or T5R equivalent investigation, which is a higher level investigation than the National Agency Check (NAC) with Law and Credit (NACLC)/T3/T3R described below. Due to the privileged system access, an investigation suitable for High Risk national security positions is required. Individuals who have access to system control, monitoring, or administration functions (e.g. system administrator, database administrator) require training and certification to Information Assurance (IA) Technical Level 1, and must be trained and certified on the Operating System (OS) or Computing Environment (CE) they are required to maintain.

Access to sensitive IT systems is contingent upon a favorably adjudicated background investigation. When access to IT systems is required for performance of the contractor employee's duties, such employees shall in-process with the Navy CSM, CSWF-PM, and ISSM/IAM manager upon arrival to the Navy command and shall out-process prior to

their departure at the completion of the individual's performance under the contract. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy IT resources. The decision to authorize access to a government IT system/network is inherently governmental. The contractor supervisor is not authorized to sign the SAAR-N; therefore, the government employee with knowledge of the system/network access required or the Technical Point of Contact (TPOC) shall sign the SAAR-N as the supervisor.

The SAAR-N shall be forwarded to the CSM at least thirty (30) days prior to the individual's start date. Failure to provide the required documentation at least thirty (30) days prior to the individual's start date may result in delaying the individual's start date.

When required to maintain access to required IT systems or networks, the contractor shall ensure that all employees requiring access complete annual Cyber Awareness training and annual Controlled Unclassified Information (CUI) training, and maintain a current requisite background investigation. The contractor's security representative shall contact the CSM for guidance when reinvestigations are required.

INTERIM ACCESS

The CSM may authorize issuance of a DoD CAC and interim access to a DoN or DoD unclassified computer/network upon a favorable review of the investigative questionnaire and advance favorable fingerprint results. When the results of the investigation are received and a favorable determination is not made, the contractor employee working on the contract under interim access will be denied access to the computer network and this denial will not relieve the contractor of his/her responsibility to perform.

DENIAL OR TERMINATION OF ACCESS

The potential consequences of any requirement under this clause including denial or termination of physical or system access in no way relieves the contractor from the requirement to execute performance under the contract within the timeframes specified in the contract. Contractors shall plan ahead in processing their employees and subcontractor employees. The contractor shall insert this clause in all subcontracts when the subcontractor is permitted to have unclassified access to a federally controlled facility, federally-controlled information system/network and/or to government information, meaning information not authorized for public release.

CONTRACTOR'S SECURITY REPRESENTATIVE

The contractor shall designate an employee to serve as the contractor's security representative. Within three (3) work days after contract award, the contractor shall provide to the requiring activity's Security Manager and the Contracting Officer, in writing, the name, title, address and phone number for the contractor's security representative. The contractor's security representative shall be the primary point of contact on any security matter. The contractor's security representative shall not be replaced or removed without prior notice to the Contracting Officer and CSM.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO NATIONAL SECURITY POSITIONS OR PERFORMING SENSITIVE DUTIES

Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Contractor employees under this contract are recognized as Non-Critical Sensitive [ADP/IT-II] positions when the contract scope of work require physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and PHI, provide support associated with fiduciary duties, or perform duties that have been identified as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLC or T3 or T3R equivalent investigation to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The investigation consists of a standard NAC and a FBI fingerprint check plus law enforcement checks and credit check. Each contractor employee filling a non-critical sensitive or IT-II position is required to complete:

* SF-86 Questionnaire for National Security Positions (or equivalent Office of Personnel Management (OPM) investigative product)
* Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission
* Original Signed Release Statements

Failure to provide the required documentation at least thirty (30) days prior to the individual's start date shall result in delaying the individual's start date. Background investigations shall be reinitiated as required to ensure investigations remain current (not older than ten (10) years) throughout the contract performance period. The contractor's security representative shall contact the CSM for guidance when reinvestigations are required.

Regardless of their duties or IT access requirements, ALL contractor employees shall in-process with the CSM upon arrival to the command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Employees requiring IT access shall also check-in and check-out with the Navy command's ISSM/IAM. Completion and approval of a SAAR-N form is required for all individuals accessing Navy IT resources. The SAAR-N shall be forwarded to the Navy CSM at least thirty (30) days prior to the individual's start date. Failure to provide the required documentation at least thirty (30) days prior to the individual's start date shall result in delaying the individual's start date.

The contractor shall ensure that each contract employee requiring access to IT systems or networks complete annual Cyber Awareness training and annual Controlled Unclassified Information (CUI) training, and maintain a current requisite background investigation. Contractor employees shall accurately complete the required investigative forms prior to submission to the CSM. The CSM will review the submitted documentation for completeness prior to submitting it to the OPM; Potential suitability or security issues identified may render the contractor employee ineligible for the assignment. An unfavorable determination is final (subject to SF-86 appeal procedures) and such a determination does not relieve the contractor from meeting any contractual obligation under the contract. The CSM will forward the required forms to OPM for processing. Once the investigation is complete, the results will be forwarded by OPM to the DoD Central Adjudication Facility (CAF) for a determination.

If the contractor employee already possesses a current favorably adjudicated investigation, the contractor shall submit a VAR via the JPAS or a hard copy VAR directly from the contractor's security representative. Although the contractor will take JPAS owning role over the contractor employee, the Navy command will take JPAS "Servicing" role over the contractor employee during the hiring process and for the duration of assignment under that contract. The contractor shall include the IT position category per SECNAV M-5510.30 for each employee designated on a VAR. The VAR requires annual renewal for the duration of the employee's performance under the contract.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO OR PERFORMING NON-SENSITIVE DUTIES

Contractor employee whose work is unclassified and non-sensitive (e.g., performing certain duties such as lawn maintenance, vendor services, etc...) and who require physical access to publicly accessible areas to perform those duties shall meet the following minimum requirements:

* Must be either a U.S. citizen or a U.S. permanent resident with a minimum of 3 years of legal residency in the U.S. (as required by the Deputy Secretary of Defense DTM 08-006 or its subsequent DoD Instruction (INST)) and
* Must have a favorably completed NACI or T1 investigation equivalent including a FBI fingerprint check prior to installation access.

To be considered for a favorable trustworthiness determination, the CSR must submit for all employees each of the following:

* SF-85 Questionnaire for Non-Sensitive Positions
* Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
* Original Signed Release Statements

The contractor shall ensure each individual employee has a current favorably completed NACI or T1 equivalent investigation or ensure successful FBI fingerprint results have been gained and investigation has been processed with OPM.

Failure to provide the required documentation at least thirty (30) days prior to the individual's start date may result in delaying the individual's start date.