**FILL IN OF CONTRACT CLAUSES**

Certain solicitation clauses have been uploaded with the solicitation which is to be completed by the Offeror, saved and submitted as File 3. These clauses are contained in this document.

All areas marked as TBD in these clauses are to be filled in by the Offeror, this information shall than be utilized to complete these specific areas prior to contract award.

**B.1 SERVICES BEING ACQUIRED – TECHNICAL SECURITY, COMMUNICATIONS SECURITY, CYBER, ANAYLSIS and SECURITY ADMINISTRATION**

1. The Contractor shall furnish all personnel, equipment, material, supplies, and services (except as may be expressly set forth in this contract as furnished by the Government) and otherwise do all things necessary for, or incident to, the performance of the items of work as specified in the Performance Work Statement (PWS) set forth in Part III, Section J, Attachment A for the **(TERM)** specified in Part I, Section F. This contract is a hybrid blend of cost-plus-award-fee (CPAF) and firm-fixed price (FFP) contract line item numbers (CLINs). The contract provides Classification Support Services as described in the PWS.
2. For the Cost-Plus-Award-Fee (CPAF) CLINs, the level of effort specified for the base period is the present level of effort **estimated** for the performance of work set forth in Part III, Section J, Attachment A, PWS. However, changes in programmatic requirements may cause a substantial increase or decrease in the number of Direct Productive Labor Hours (DPLH) identified for the Contract Line Item Numbers (CLIN) listed in Part I, Section B. This contract is to be available for the Government to obtain services for the contract period **(TERM),** even if the level of effort and/or the estimated cost as originally specified is insufficient. The estimated level of effort, as may be approved by the Contracting Officer in accordance with this contract, is inclusive of all effort for the prime, subcontractor(s), consultant(s), or other such entities that provide labor under this contract. The estimated DPLH is identified below for each CLIN. The Total Estimated Cost identified below is inclusive of all items (e.g. labor, supplies, materials, subcontracts, etc.)
3. For the Firm-Fixed Price CLINs, the fixed price shall encompass completion of all work specified in Part III, Section J, Attachment A, PWS.
4. All work under this contract shall be performed under the general guidance and direction of the DOE Contracting Officer’s Representative (COR) whose responsibilities are set forth in the clause Technical Direction in Part I, Section H. Such guidance and direction shall not; however, effect any change in the Contract Schedule, PWS, or other provisions of this contract. Such changes shall only be made by the expressed written direction of the Contracting Officer.
5. The PWS set forth in Part III, Section J, Attachment A, defines the scope of work specific for each CLIN listed below.

**CLIN 1 – TSP Support Services (Cost Reimbursement)**

This CLIN provides support services and qualified personnel for all programs within the TSP. Technical security personnel provide support for the implementation and administration of the DOE TSP in accordance with DOE Order 470.6, relevant National Security Agency implementations, Committee on National Security Policies, Director of National Intelligence Policies and Directorate Central Intelligence Agency Directives (DCIDs) and various Executive order and legislations. Each of these support services are further described in the Performance Work Statement (PWS).

|  |
| --- |
| **Base Period (Effective date through 12 months)** |
|  **Item Number** |  **Description (Cost-Plus-Award-Fee)** |  **Estimate** |  |  **Total Est Cost/Fee** |
| CLIN 1 | Technical Support Services  |  |  |
| Total Estimated Cost |  TBD |  |
| Estimated DPLH |  TBD |  |
| Maximum Award Fee Pool |  TBD |  |
| Total Estimated Cost Plus Maximum Award Fee |  |  TBD |
|  |  |  |  |
|  |  |  |  |
| **Option Period I (month 13 through month 24)** |
|  **Item Number** |  **Description (Cost-Plus-Award-Fee)** |  **Estimate** |  |  **Total Est Cost/Fee** |
| CLIN 1 | Technical Support Services  |  |  |
| Total Estimated Cost |  TBD |  |  |
| Estimated DPLH |  TBD |  |
| Maximum Award Fee Pool |  TBD |  |
| Total Estimated Cost Plus Maximum Award Fee |  |  TBD |
|  |  |  |  |
|  |  |  |  |
| **Option Period II (month 25 through month 36)** |
|  **Item Number** |  **Description (Cost-Plus-Award-Fee)** |  **Estimate** |  |  **Total Est Cost/Fee** |
| CLIN 1 | Technical Support Services |  |  |
| Total Estimated Cost |  TBD |  |  |
| Estimated DPLH |  TBD |  |
| Maximum Award Fee Pool |  TBD |  |
| Total Estimated Cost Plus Maximum Award Fee |  |  TBD |
|  |  |  |  |
| **Option Period III (month 37 through month 48)** |
|  **Item Number** |  **Description (Cost-Plus-Award-Fee)** |  **Estimate** |  |  **Total Est Cost/Fee** |
| CLIN 1 | Technical Support Services |  |  |
| Total Estimated Cost |  TBD |  |
| Estimated DPLH |  TBD |  |
| Maximum Award Fee Pool |  TBD |  |
| Total Estimated Cost Plus Maximum Award Fee |  |  TBD |

|  |
| --- |
| **Option Period IV (month 49 through month 60)** |
|  **Item Number** |  **Description (Cost-Plus-Award-Fee)** |  **Estimate** |  |  **Total Est Cost/Fee** |
| CLIN 1 | Technical Support Services |  |  |
| Total Estimated Cost |  TBD |  |
| Estimated DPLH |  TBD |  |
| Maximum Award Fee Pool |  TBD |  |
| Total Estimated Cost Plus Maximum Award Fee |  |  TBD |
|  |  |  |  |

**CLIN 2 – Contract Administration and General Administrative Support Services (Firm-Fixed Price).**

This CLIN supports the contract administration and general administrative support services necessary to perform the support services of this contract.

|  |
| --- |
| **Base Period (Effective date through 12 months)** |
| **Item Number** | **Description (Firm-Fixed-Price)** |  | **Total Price** |
| CLIN 2 | Contract Administration, General Administrative Support |  |  TBD |

|  |
| --- |
| **Option Period I (month 13 through month 24)** |
| **Item Number** | **Description (Firm-Fixed-Price)** |  | **Total Price** |
| CLIN 2 | Contract Administration, General Administrative Support |  |  TBD |

|  |
| --- |
| **Option Period II (month 25 through month 36)** |
| **Item Number** | **Description (Firm-Fixed-Price)** |  | **Total Price** |
| CLIN 2 | Contract Administration, General Administrative Support |  |  TBD |

|  |
| --- |
| **Option Period III (month 37 through month 48)** |
| **Item Number** | **Description (Firm-Fixed-Price)** |  | **Total Price** |
| CLIN 2 | Contract Administration, General Administrative Support |  |  TBD |

|  |
| --- |
| **Option Period IV (month 49 through month 60)** |
| **Item Number** | **Description (Firm-Fixed-Price)** |  | **Total Price** |
| CLIN 2 | Contract Administration, General Administrative Support |  |  TBD |

**CLIN 3 – TRANSITION (Firm-Fixed Price)**

The Contractor shall perform all transition activities to begin performance of this contract, consistent with this contract. Transition activities are defined as any effort that is necessary to transition the work from the incumbent Contractor in a manner that (1) assures that all work for which the Contractor is responsible under the contract is continued without disruption; (2) provides for an orderly transfer of resources, responsibilities, and accountability from the incumbent Contractor; and (3) allows the Contractor to perform the work in an efficient, effective, and safe manner. Specific transition activities will be identified; however, anticipated transition activities include, but are not limited to, assuming operational control of staffing, orienting, and training Key Personnel and other than Key Personnel, etc. Transition shall commence upon contract award and continue through the effective date of the contract which will coincide with the date the Contractor assumed full responsibility for contract operational performance.

|  |
| --- |
|  |
| **Item Number** | **Description (Firm-Fixed-Price)** |  | **Total Price** |
| CLIN 3 | Transition |  |  TBD |

**H.5 KEY PERSONNEL/PROGRAM MANAGER & sENIor tECHNICAL sECURITY sPECIALIST**

1. Introduction

The key personnel, which include the Program Manager and Senior Technical Security Specialist (STSS), specified below, are considered to be critical to the success of all work being performed under this award. This Clause provides specific requirements, in addition to the requirements of the clause in Section I entitled, “952.215-70 Key Personnel.” Any changes to these personnel require prior DOE Contracting Officer’s written approval.

1. Key Personnel Team Requirements

The Contracting Officer and designated Contracting Officer’s Representative(s) shall have direct access to the Key Personnel. In addition to the definition contained in the Section I Clause entitled, “DEAR 952.215-70, Key Personnel,” Key Person(s) are considered managerial personnel.

In addition, the Program Manager is the most senior resident manager. This individual is responsible for the planning, implementation, management, performance, and supervision of the contract. The Program Manager shall receive and execute, on behalf of the Contractor, such technical directions as the DOE Contracting Officer’s Representative may issue within the terms and conditions of the contract.

1. Definitions

For the purposes of this clause, Changes to Key Personnel is defined as: (i) any changes to the position assignment of a current Key Person under the contract, except for a person who acts for short periods of time, in the place of a Key Person during his or her absence, the total time of which shall not exceed 30 working days during any given year; (ii) utilizing the services of a new substitute Key Person for assignment to the contract; or (iii) assigning a current Key Person for work outside the Contract.

1. Contract Award Fee Reductions for Changes to Key Personnel
2. Notwithstanding approval by the Contracting Officer, anytime the Program Manager (the initial Program Manager or any accepted substitution approved by the Contracting Officer) is changed for any reason after being placed in the position, the total Available Award Fee Pool (sum of all individual CLIN award fee pools), may be reduced, for the fee period in which the change occurs, by $75,000 for each and every occurrence of a change to the Program Manager.
3. Notwithstanding approval by the Contracting Officer, anytime a Key Person other than the Program Manager (any initial Key Person or any accepted substitution approved by the Contracting Officer) is changed for any reason after being placed in the position, the total Available Award Fee Pool (sum of all individual CLIN award fee pools), may be reduced, for the fee period in which the change occurs, by $25,000 for each and every occurrence of a change to the Key Person.
4. The Contractor may request, in writing, that the Contracting Officer consider waiving all or part of a reduction in the available award fee pool. Such written request shall include the factual basis for the request. The Contracting Officer shall have unilateral discretion to make the determination to waive or not waive all or part of a reduction in the available award fee pool.
5. Key Personnel for this Contract

The Key Personnel that have been approved for this contract are identified below. Any changes to these personnel require prior DOE Contracting Officer’s written approval.

Name Position/Title

[TBD] Program Manager (PM)

[TBD] Senior Technical Security Specialist (STSS)

The Contractor shall notify the Contracting Officer not less than thirty (30) calendar days prior to the diversion or substitution of key personnel and shall submit a written justification (including qualifications of proposed substitutions) to permit evaluation. The proposed changes will be approved in writing at the sole discretion of the Contracting Officer.

1. Contract Award Fee Reductions for Key Personnel Commitments

Unless a written waiver is approved in advance, by the CO, should any key personnel be removed, replaced, or diverted by the Contractor prior to fulfillment of the commitment letter received for that specific key personnel, the total Available Award Fee Pool (sum of all individual CLIN award fee pools), may be reduced, for the fee period in which the change occurs, by $30,000 for each and every failure to fulfill commitment. The reduction referred in this paragraph is in addition to the specific position reduction stated in paragraph D, above.

**H.10 LIMITATION OF INDIRECT COST (COST REIMBURSEMENT)**

Notwithstanding any other clause(s) of this contract, the Government shall not reimburse the Contractor for any site specific on-site, off-site, and G&A indirect costs in excess of the indirect expense dollars derived for each of the Contractor’s fiscal years by the application of the following individual indirect cost ceiling rates to the appropriate base outlined below. The indirect cost ceiling rates are based on a [TBD - *percentage of overall rate or percentage of growth for individual or groups of cost elements*] basis. All indirect costs in excess of said limit(s) shall be borne by the Contractor.

* + - * 1. Percentage of Overall Rate

|  |  |
| --- | --- |
| Entity[TBD] | Indirect Cost Ceiling Rate(s) per Contractor’s Fiscal Year (1) (Years 1-5) |
| Indirect Cost | Base of Application | FY[TBD] | FY[TBD] | FY[TBD] | FY[TBD] | FY[TBD] | FY[TBD] |
| DOE Site Specific On-Site Overhead | $[TBD] | [TBD]% | [TBD]% | [TBD]% | [TBD]% | [TBD]% | [TBD]% |
| Off-Site Overhead (Contractor’s site) | $[TBD] | [TBD]% | [TBD]% | [TBD]% | [TBD]% | [TBD]% | [TBD]% |
| G&A | $[TBD] | [TBD]% | [TBD]% | [TBD]% | [TBD]% | [TBD]% | [TBD]% |

*(1) For Contractor’s FY beginning [TBD] and ending [TBD].*

Or

* + - * 1. Percentage of Growth for Individual or Group of Cost Elements

|  |  |  |
| --- | --- | --- |
|  | Entity[TBD] | Indirect Cost Ceiling Rate(s) per Contractor’s Fiscal Year (1) (Years 1-5) |
| Indirect Cost | Cost Element | FY[TBD ] | FY[TBD] | FY[TBD] | FY[TBD] | FY[TBD] | FY[TBD] |
| DOE Site Specific On-Site Overhead | [TBD] | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed |
| Off-Site Overhead (Contractor’s site) | [TBD] | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed |
| G&A | [TBD] | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed | [TBD]% of growth allowed |

*(1) For Contractor’s FY beginning [TBD] and ending [TBD].*

The indirect cost limitations set forth above include provisions for all known increases that will take place during the term of this contract resulting from statute, court decisions and/or written ruling or regulation by the Internal Revenue Service (IRS) or any other taxing authority. However, in the event that during the term of this contract, any other statute, court decision and/or written ruling or regulation affects the Contractor’s indirect costs, the indirect cost limitations will be adjusted to the extent the Contracting Officer determines the increase or decrease, if any, said statute, court decision and/or ruling or regulation impacts the Contractor’s indirect costs.

This clause shall be flowed down to all subcontracts issued under a cost reimbursement basis. The indirect rate ceilings contained in this clause shall be negotiated prior to the placement of any cost-reimbursement subcontracts not previously authorized in Part I, Section, H, “Prior Approval Requirements for Placement of Subcontracts and/or Consultants.” The prime Contractor is responsible for negotiating the indirect rate ceilings and ensuring a copy is contained in the subcontract approval package submitted to the Government. However, if the subcontractor is concerned with the prime Contractor having access to company proprietary information, with permission from the prime Contractor, the required information can be submitted directly to the Government for negotiation. In this instance, the prime Contractor will forward an e-mail to the Contract Specialist stating their intention/agreement for the Government to negotiate the indirect rate ceilings. Upon completion, the Government will maintain the agreed upon rate ceilings and provide the prime Contractor with a written notification that negotiations with the subcontractor have been completed.

**J.C ATTACHMENT C TECHNICAL SECURITY POSITION (TSP) QUALIFICATIONS**

NOTE: If accepted, the labor category and minimum position qualifications proposed will be incorporated (and/or replace) the below listing.

**TECHNICAL SECURITY POSITION (TSP) QUALIFICATIONS**

All personnel are required to possess an active Department of Energy (DOE) “Q” access authorization in order to perform under this contract. An active Top Secret clearance from Other Government Agencies, such as Department of Defense (DoD) based upon a single scope background investigation is typically acceptable for clearance reciprocity if the background investigation is less than five (5) years old. It is required that specified personnel have access to Sensitive Compartmented Information (SCI).

**KEY PERSONNEL**

**PROJECT MANAGER (1 FTE – KEY)**

***Job Summary*:**

The Project Manager serves as the principal point of contact to the Department of Energy (DOE) Federal Representative in support of specific or general requirements, daily project management, personnel, financial, training, and programmatic requirements associated with the DOE TSP. These programs include Technical Surveillance Countermeasures (TSCM), Communications Security (COMSEC), Secure Telecommunications, Protected Distribution Systems (PDS), Wireless Security (WiSec) and TEMPEST. Managing areas include (but not limited to) policy review, operations planning, reports, personnel, equipment and supporting the DOE Federal Technical Security employees. The candidate must possess advanced level proficiency with Excel skills required; and intermediate level proficiency with MS Word. Ability to effectively interact with personnel at all levels in a dynamic work environment is required. The candidate must be able to work independently and in a team environment and possess excellent written and oral communication skills. The Project Manager must maintain proper clearances and DOE/National training/certification requirements.

***Functional Responsibility*:**

Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor personnel, and communicating policies, purposes, and goals of the organization to subordinates. The Project Manager shall be responsible for the overall contract performance, milestones, reporting and budget.

***Minimum Position Requirements*:**

Undergraduate degree in Business Administration, Management, Finance or other relevant discipline is desired, but not required. A minimum of 10 years related specialized management/supervisory experience with Technical Security and/or Counterintelligence (CI) programs combined. Relevant Technical Security certifications are required, (ex., include but are not limited to: Federal TSCM, TEMPEST and/ CI certifications). Must have a thorough understanding of the systems identified in the scope of work and specialized experience in related project work required. Two years of direct Government contracting experience at task/project management/supervisory level is required; experience in protecting national security information in either the Government or private sector; basic knowledge/familiarity with contract administration desired.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**SENIOR TECHNICAL SECURITY SPECIALIST (1 FTE KEY)**

***Job Summary*:**

Applicable knowledge, effective employment and utilizing state-of-the-art technical equipment, in support of the DOE TSP. The Senior Technical Security Specialist (STSS) will be responsible for conducting Technical Surveillance Countermeasures (TSCM), WiSec, PDS and TEMPEST services, inspections, in-conference security monitoring services, pre-construction support, to include other services as directed by the Department of Energy (DOE), in accordance with DOE and National Policies, Procedures and applicable laws. The STSS will be responsible for all other aspects related to participation and operation of a TSP as outlined. The STSS will also be responsible for maintaining proper clearances and DOE/National training/certification requirements. Must maintain appropriate security clearances and accesses.

The STSS that is designated as Key will be required to act as back-up to the Project Manager.

***Functional Responsibility*:**

Serve as the technical subject matter expert providing support and education to personnel on matters of technical security policy, procedures, and regulations. The candidate must possess a thorough knowledge of specialized equipment operations to include effective countermeasures employment. Provide technical security services to ensure the security of DOE information. Develop and present technical security related training to personnel in a formal classroom and in a field setting. Provide technical security support services as directed by DOE for a comprehensive TSP designed to protect facilities, employees and assets. Assist in developing and reviewing technical security designs for the agency's facilities. Provide input/review of proposed policies. Apply technical procedures in conducting needs surveys for preventing unauthorized access to, and possible disclosure of, classified and sensitive information. The candidate must have the ability to effectively relate technical requirements/issues to non-technical personnel. Must have the ability to communicate effectively to large or small groups on technical and non-technical issues related to the TSP. Effectively work in a team environment, as a team lead or team member. Provide clear and concise reports for each service conducted to identify cost effective strategies and effective security protection measures in accordance with DOE and National Policy and Protection Strategies. Provide support services on national and international developments in commercial, state- of-the-art, security technology through briefings and educational Materials. Physical and psychological capabilities are required which allow him/her to perform activities during sustained periods of intense concentration, working with electrical hazards, under adverse weather conditions, in confined and restricted areas. The ability to climb and work at heights; lift and carry heavy loads of at least 70 pounds; ability to distinguish colors and read codes on electronic components is required. Knowledge of, but not limited to, various types of communication and internet technology (IT) systems, physical security devices and methods, intelligence and counterintelligence methods, physical security, Operational Security, methods of radio frequency modulations coupled with a comprehensive appreciation of practices and techniques employed in espionage are essential position elements. Will be required to maintain/acquire certifications as mission necessities. Must be able to obtain and maintain DOE/National certification within the time limitations depicted in DOE policy.

***Minimum Position Requirements*:**

Undergraduate degree in an information technology, electronics, business, security or a related discipline is desired. Technical Security and Counterintelligence (CI) programs are required, to include, but not limited to, Federal TSCM, TEMPEST and/ CI certifications). Graduation/Certification from a National Level Federal TSCM School is required. The candidate must have previous federal government training and current (within the last year) operational experience in/with a National Level TSCM/TS program. A combination of training and current operational experience of at least 15 years is required. Must possess/obtain all required security clearances to perform a technical security-related activity.

At least one year of management/supervisory responsibility required.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**SENIOR TECHNICAL SECURITY SPECIALIST (10 FTEs NON-KEY)**

Job Summary:

Applicable knowledge, effective employment and utilizing state-of-the-art technical equipment, in support of the DOE TSP. The Senior Technical Security Specialist (STSS) will be responsible for conducting Technical Surveillance Countermeasures (TSCM), WiSec, PDS and TEMPEST services, inspections, in-conference security monitoring services, pre-construction support, to include other services as directed by the Department of Energy (DOE), in accordance with DOE and National Policies, Procedures and applicable laws. The STSS will be responsible for all other aspects related to participation and operation of a TSP as outlined. The STSS will also be responsible for maintaining proper clearances and DOE/National training/certification requirements. Must maintain appropriate security clearances and accesses.

The STSS that is designated as Key will be required to act as back-up to the Project Manager.

Functional Responsibility:

Serve as the technical subject matter expert providing support and education to personnel on matters of technical security policy, procedures, and regulations. The candidate must possess a thorough knowledge of specialized equipment operations to include effective countermeasures employment. Provide technical security services to ensure the security of DOE information. Develop and present technical security related training to personnel in a formal classroom and in a field setting. Provide technical security support services as directed by DOE for a comprehensive TSP designed to protect facilities, employees and assets. Assist in developing and reviewing technical security designs for the agency's facilities. Provide input/review of proposed policies. Apply technical procedures in conducting needs surveys for preventing unauthorized access to, and possible disclosure of, classified and sensitive information. The candidate must have the ability to effectively relate technical requirements/issues to non-technical personnel. Must have the ability to communicate effectively to large or small groups on technical and non-technical issues related to the TSP. Effectively work in a team environment, as a team lead or team member. Provide clear and concise reports for each service conducted to identify cost effective strategies and effective security protection measures in accordance with DOE and National Policy and Protection Strategies. Provide support services on national and international developments in commercial, state- of-the-art, security technology through briefings and educational Materials. Physical and psychological capabilities are required which allow him/her to perform activities during sustained periods of intense concentration, working with electrical hazards, under adverse weather conditions, in confined and restricted areas. The ability to climb and work at heights; lift and carry heavy loads of at least 70 pounds; ability to distinguish colors and read codes on electronic components is required. Knowledge of, but not limited to, various types of communication and internet technology (IT) systems, physical security devices and methods, intelligence and counterintelligence methods, physical security, Operational Security, methods of radio frequency modulations coupled with a comprehensive appreciation of practices and techniques employed in espionage are essential position elements. Will be required to maintain/acquire certifications as mission necessities. Must be able to obtain and maintain DOE/National certification within the time limitations depicted in DOE policy.

**Minimum Position Requirements:**

Undergraduate degree in an information technology, electronics, business, security or a related discipline is desired. Technical Security and Counterintelligence (CI) programs are required, to include, but not limited to, Federal TSCM, TEMPEST and/ CI certifications). Graduation/Certification from a National Level Federal TSCM School is required. The candidate must have previous federal government training and current (within the last year) operational experience in/with a National Level TSCM/TS program. A combination of training and current operational experience of at least 15 years is required. Must possess/obtain all required security clearances to perform a technical security-related activity.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**MID-LEVEL TECHNICAL SECURITY SPECIALIST (1 FTE, non-key)**

***Job Summary*:**

Applicable knowledge, effective employment and utilization of state-of-the-art technical equipment, in support of the DOE TSP. The Mid-Level Technical Security Specialist (MTSS) will be responsible for conducting Technical Surveillance Countermeasures (TSCM), WiSec, PDS and TEMPEST services, inspections, in-conference security monitoring services, pre-construction advice, to include other services and provide assistance as directed by the Department of Energy (DOE), in accordance with DOE and National Policies, Procedures and applicable laws. The MTSS will be responsible for all other aspects related to participation and operation of a TSP as outlined. The MTSS will also be responsible for maintaining proper clearances and DOE/National training/certification requirements. Must maintain appropriate security clearances and accesses.

***Functional Responsibility*:**

Serve as the technical subject matter expert providing support and provide recommendations of technical security policy, procedures, and regulations. The candidate must possess a thorough knowledge of specialized equipment operations to include effective countermeasures employment; provide technical security services to ensure the security of DOE information; develop and present technical security related training to personnel in a formal classroom and in a field setting; and, provide technical security support services as directed by DOE for a comprehensive TSP designed to protect facilities, employees and assets. The candidate must assist in developing and reviewing technical security designs for the agency's facilities; provide input/review of proposed policies; and, apply technical procedures in conducting needs surveys for preventing unauthorized access to, and possible disclosure of, classified and sensitive information. The candidate must have the ability to effectively relate technical requirements/issues to non-technical personnel; must have the ability to communicate effectively to large or small groups on technical and non-technical issues related to the TSP; and, effectively work in a team environment, as a team lead or team member. The candidate must provide clear and concise reports for each service conducted to identify cost effective strategies and security effect protection measures in accordance with DOE and National Policy and Protection Strategies. Must provide support services and recommendations on national and international developments in commercial, state- of-the-art, security technology through briefings and educational materials. Physical and psychological capabilities are required which allow him/her to perform activities during sustained periods of intense concentration, working with electrical hazards, under adverse weather conditions, in confined and restricted areas. The ability to climb and work at heights; lift and carry heavy loads of at least 70 pounds; ability to distinguish colors and read codes on electronic components is required. Knowledge of, but not limited to, various types of communication and internet technology (IT) systems, physical security devices and methods, intelligence and counterintelligence methods, physical security, Operational Security, methods of radio frequency modulations coupled with a comprehensive appreciation of practices and techniques employed in espionage are essential position elements. Will be required to maintain/acquire certifications as mission necessities. Must be able to obtain and maintain DOE/National certification within the time limitations depicted in DOE policy.

***Minimum Position Requirements*:**

Undergraduate degree in an information technology, electronics, business, security or a related discipline is desirable. Extensive Technical Security and Counterintelligence (CI) programs are required, (Ex. Federal TSCM, TEMPEST and/ CI certifications). Graduation/Certification from a National Level Federal TSCM School is required. The candidate must have previous federal government training and current (within the last year) operational experience in/with a National Level TSCM/TS program. A combination of training and current operational experience of at least 10 years is required. Must possess/obtain all required security clearances to perform a TS related taskings.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**JUNIOR TECHNICAL SECURITY SPECIALIST (1 FTE, non-key)**

***Job Summary*:**

Applicable knowledge, effective employment and utilizing state-of-the-art technical equipment, in support of the DOE TSP. The Junior Technical Security Specialist (JTSS) will be responsible for conducting Technical Surveillance Countermeasures (TSCM), WiSec, PDS and TEMPEST services, inspections, in-conference security monitoring services, pre-construction advice, to include other services and provide assistance as directed by the Department of Energy (DOE), in accordance with DOE and National Policies, Procedures and applicable laws. The JTSS will be responsible for all other aspects related to participation and operation of a TSP as outlined and directed by the DOE Office of Technical Security Director and/or relevant Federal Program/Operations Manager. The JTSS will also be responsible for maintaining proper clearances and DOE/National training/certification requirements. Must maintain appropriate security clearances and accesses. One FTE may be located at the Albuquerque, NM site.

***Functional Responsibility*:**

Serve as the technical subject matter expert to provide support and recommendations of technical security policy, procedures, and regulations. The candidate must possess a thorough knowledge of specialized equipment operations to include effective countermeasures employment; provide technical security services to ensure the security of DOE information; develop and present technical security related training to personnel in a formal classroom and in a field setting; and, provide technical security support services as directed by DOE for a comprehensive technical security program designed to protect facilities, employees and assets. The candidate must assist in developing and reviewing technical security designs for the agency's facilities; provide input/review of proposed policies; and, apply technical procedures in conducting needs surveys for preventing unauthorized access to, and possible disclosure of, classified and sensitive information. The candidate must have the ability to effectively relate technical requirements/issues to non-technical personnel; must have the ability to communicate effectively to large or small groups on technical and non-technical issues related to the TSP; effectively work in a team environment, as a team lead or team member. Provide clear and concise reports for each service conducted to identify cost effective strategies and security effect protection measures in accordance with DOE and National Policy and Protection Strategies. Provide support services and recommendations on national and international developments in commercial, state- of-the-art, security technology through briefings and educational materials. Physical and psychological capabilities are required which allow him/her to Perform activities during sustained periods of intense concentration, working with electrical hazards, under adverse weather conditions, in confined and restricted areas. The ability to climb and work at heights; lift and carry heavy loads of at least 70 pounds; ability to distinguish colors and read codes on electronic components is required. Knowledge of, but limited to, various types of communication and internet technology (IT) systems, physical security devices and methods, intelligence and counterintelligence methods, physical security, Operational Security, methods of radio frequency modulations coupled with a comprehensive appreciation of practices and techniques employed in espionage are essential position elements.

***Minimum Education*:**

Undergraduate degree in an information technology, electronics, business, security or a related discipline is desirable. Extensive Technical Security and Counterintelligence (CI) programs are required, (Ex. Federal TSCM, TEMPEST and/ CI certifications). Graduation/Certification from a National Level Federal TSCM School will be required. The candidate must have previous federal government training and current (within the last year) operational experience in/with a National Level TSCM/TS program. A combination of training and current operational experience of at least 5 years is required. Must be able to obtain and maintain DOE/National certification within the time limitations depicted in DOE policy. Must possess/obtain all required security clearances to perform a TS related taskings.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**TECHNICAL SECURITY TRAINEE (1 FTE, non-key, beginning in Option Year 2)**

***Job Summary***:

Prepare for DOE and National TSCM and TEMPEST Certification through formal training, self-study and on the job training. The candidate must apply applicable knowledge, effective employment and utilization of state-of-the-art technical equipment, in support of the DOE TSP. The Trainee will be responsible for conducting TSCM services, inspections, in-conference security monitoring services, pre-construction advice, to include other services and provide assistance as directed by the Department of Energy (DOE), in accordance with DOE and National Policies, Procedures and applicable laws. Must maintain proper clearances and achieve DOE/National training/certification requirements. The candidate must receive recommendation through an interview process of senior DOE TSCM technicians and approval from DOE Office of Technical Security for placement into this position. Trainee must meet all DOE and National Training pre-requisites, interviews and processes to be admitted into the TSP. Must pass all applicable National Training requirement as specified in DOE Orders for TSCM and Applicable technical security programs.

***Functional Responsibility*.**

Gain knowledge of specialized equipment operations to include effective countermeasures employment to provide TS services to ensure the security of DOE information for National and DOE TSP certifications and performance requirements as a Technical Security Specialist Trainee (TSST). Through formal training and on-the-job (OTJ), the trainee will learn to provide technical security support services for a comprehensive TSP designed to protect facilities, employees and assets. Assist in developing and reviewing technical security designs for the agency's facilities. Provide input/review of proposed policies. Apply technical procedures in conducting needs surveys for preventing unauthorized access to, and possible disclosure of, classified and sensitive information. The candidate must possess the ability to effectively relate technical requirements/issues to non-technical personnel. Must have the ability to communicate effectively to large or small groups on technical and non-technical issues related to the TSP. Effectively work in a team environment, as a team lead or team member. Provide a clear and concise reports for each service conducted to identify cost effective strategies and security effect protection measures in accordance with DOE Policy and Protection Strategies. Provide research services and advising office personnel on national and international developments in commercial, state-of-the-art, security technology through briefings and educational materials.

The candidate must have the physical and psychological capabilities which allow him/her to perform activities during sustained periods of intense concentration, working with electrical hazards, under adverse weather conditions, in confined and restricted areas. The ability to climb and work at heights; lift and carry heavy loads of at least 70 pounds; ability to distinguish colors and read codes on electronic components is required. Will gain and become proficient in, but limited to, various types of communication systems, physical security devices and methods, intelligence and counterintelligence methods, physical security, Operational Security, methods of radio frequency modulations coupled with a comprehensive appreciation of practices and techniques employed in espionage are essential position elements.

***Minimum Education*:**

Undergraduate degree in an information technology, electronics, electronics, telecommunications, computer technology, security or a related discipline is desirable. Five (5) years of demonstrated current experience in information technology, electronics, electronics, telecommunications, computer technology, security or a related discipline is required. Counterintelligence/Investigate experience is very desirable. Must possess and maintain necessary security clearances to perform a technical security related tasking and training.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**LOGISTICIAN/EQUIPMENT MANAGER (1 FTE, non-key)**

***Job Summary*:**

Will maintain and control a system of records relative to purchasing and logistics for all equipment and contracting activities. Will present the service of vendors and assist in evaluation of the quality of items purchased. Will complete all necessary documentation and activities in the procurement, maintenance, certification and destruction of technical security equipment in accordance with DOE and manufacturer’s requirements. Complete required documentation for equipment requests, maintenance, certification logs and updates. Maintain in-house equipment inventory. Coordinate all phases to maintain TSP equipment and transfers/loans of equipment within DOE and with other Government Agencies. Must maintain appropriate clearance levels. The candidate must be proficient with various software programs to include all Microsoft Office programs. The candidate must possess sufficient computer and word processor skills to accomplish basic inventory and records keeping entries.

***Functional Responsibility*:**

Process purchase and maintenance requests and related documentation of materials and services in support of the TSP. Obtain competitive pricing on equipment and services. Maintain equipment and associated records and control the fixed asset inventory. Perform inventory control, property management and maintain approximately 1,000-line items of supplies and equipment.

***Minimum Education*:**

Undergraduate degree is desirable. Three (3) years of related finance, budget, equipment logistics, office management or procurement experience required.

 **(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**SENIOR COMSEC AUDITOR (3 FTEs, non-key)**

***Job Summary*:**

The Senior COMSEC Auditor will plan and conduct COMSEC audits and COMSEC training for the protection of COMSEC materials and items. The candidate must have expertise and working knowledge of COMSEC and COR operations and requirements. Must be able to maintain COMSEC databases and interactions with NSA. Will provide analytical, problem solving, and communication skills to deal with senior level field oversight.

***Functional Responsibility*:**

Plan, coordinate and conduct COMSEC audits and inventories in accordance with DOE and National Policies for the protection for COMSEC materials, classified and CCI equipment for DOE. Prepare audit reports, review various COMSEC requests, conduct inquiries into COMSEC incidents, prepare and conduct COMSEC training and briefings. Will conduct day-to-day Central Office of Records activities. Coordination with the National Office of Record as required. Required to travel to field sites to conduct audits and training. Maintain electronic databases and records files. Required to assist in COMSEC Key transfers to field sites and training certifications as necessary. Maybe required to perform duties as COMSEC account manager.

***Minimum Education*:**

Bachelor's degree is desired, but not necessary. Ten (10) years of combined experience conducting COMESEC audits and/or Central Office of Record Operations (COR) for the protection of Type 1 encryption key, Controlled Cryptographic Items (CCI), supporting COMSEC accounts and other associated equipment in accordance with National Security Agency (NSA) policies and requirements and Committee on National Security Systems (CNSS) and is required.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**COMSEC AUDITOR (1 FTE, non-key)**

***Job Summary*:**

The COMSEC Auditor will provide support in conducting COMSEC audits and COMSEC training for the protection of COMSEC materials and items. The candidate must have expertise and working knowledge of COMSEC and COR operations and requirements. Must be able to maintain COMSEC databases and interactions with NSA. Provide analytical, problem solving, and communication skills to deal with senior level field oversight.

***Functional Responsibility*:**

Plan, coordinate and conduct COMSEC audits and inventories in accordance with DOE and National Policies for the protection for COMSEC materials, classified and CCI equipment for DOE. Prepare audit reports, review various COMSEC requests, conduct inquiries into COMSEC incidents, prepare and conduct COMSEC training and briefings. Will conduct day-to-day Central Office of Records activities. Coordination with the National Office of Record as required. Required to travel to field sites to conduct audits and training. Maintain electronic databases and records files. Required to assist in COMSEC Key transfers to field sites and training certifications as necessary.

***Minimum Education*:**

Bachelor's degree is desired, but not necessary. Five (5) years of combined experience conducting COMESEC audits and/or Central Office of Record Operations for the protection of Type 1 encryption key, Controlled Cryptographic Items (CCI), supporting COMEC accounts and other associated equipment in accordance with Committee on National Security Systems (CNSS) and National Security Agency (NSA) policies and requirements or as COMSEC custodian is required.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**SENIOR TELECOMMUNICATIONS SPECIALIST (3 FTEs, non-key)**

***Job Summary*:**

The Senior Telecommunications Specialist will demonstrate analytical, problem solving, and communication skills in working with technical, functional, and management personnel. The candidate must have experience working with Communications Security (COMSEC) type 1 KEY and associated equipment. Will conduct secure telecommunication equipment (STE) installation, repair, upgrades, trouble shooting and destruction of Controlled Cryptographic Items (CCI). Will utilize National Security Agency approved Key Management Systems and associated equipment. As required by the contract, must possess appropriate level clearance (Q and TS clearance and SCI eligible).

***Functional Responsibility*:**

Responsible for the day-to-day management, administration, maintenance, security, installation and support secure telecommunications equipment for DOE HQ responsibilities and COMSEC Key Management System. Interface/integrate with the local classified and unclassified wide area network telecommunications operations on all matters involving secure telecommunications compatibility and connectivity. Detect, diagnose, report and analyze and resolve problems associated with hardware, applications software in support of classified telecommunications equipment and cryptographic items. Assist in COMSEC audits/inspections/inventories and training as required. Keep abreast of new equipment and Key Management requirements and operations. Protect operations and equipment in accordance with DOE and National Policy requirements. One FTE maybe be located at the Albuquerque, NM site.

***Minimum Education*:**

Bachelor’s degree in a relevant technical discipline is desired, but not a requirement. A combination of eight (8) years of relevant industry experience in Type I Key management and secure telecommunications/COMSEC equipment and/or Federal Government experience with relevant certifications is required.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**TELECOMMUNICATIONS SPECIALIST (1 FTE, non-key)**

***Job Summary*:**

The Telecommunications Specialist will demonstrate analytical, problem solving, and communication skills in working with technical, functional, and management personnel. Must have experience working with Communications Security (COMSEC) type 1 KEY and associated equipment. Must have working knowledge in secure telecommunication equipment (STE) installation, repair, upgrades, trouble shooting and destruction of Controlled Cryptographic Items (CCI). Must have experience utilizing National Security Agency approved Key Management Systems and associated equipment.

***Functional Responsibility*:**

Responsible for the day-to-day management, administration, maintenance, security, installation and support secure telecommunications equipment for DOE HQ responsibilities and COMSEC Key Management System. Interface/integrate with the local classified and unclassified wide area network telecommunications operations on all matters involving secure telecommunications compatibility and connectivity. Detect, diagnose, report and analyze and resolve problems associated with hardware, applications software in support of classified telecommunications equipment and cryptographic items. Assist in COMSEC audits/inspections/inventories and training as required. Protect operations and equipment in accordance with DOE and National Policy requirements.

***Minimum Education*:**

Bachelor’s degree in a relevant technical discipline is desired, but not a requirement. A combination of four (4) years of specialized experience in Type 1 Key management and secure telecommunications/COMSEC equipment and/or Federal Government experience with relevant certifications are required.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**TECHNICAL SECURITY ANALYST/RESEARCHER (1 FTE, non-key)**

***Job Summary*:**

Provide research and analysis service in accordance with or directly related to the scope of work. Provide briefings, on analysis results, to members of management, the professional staff, and to the customer. Exercise independent judgment and initiative in solving problems and performing complex technical efforts in specialty area by conducting research and analysis and provide professional national level assessments of technical security issues. Conduct research and analyze data to establish trends, identify threats, vulnerabilities, and potential areas of interest for technical security programs. Support TSP by utilizing specialized software provided for data mining and link analysis. Establish a fundamental understanding of DOE and TSP operations to include policies and procedures, and data sources available for analysis. Demonstrate fundamental understanding of investigative and intelligence processes to include the intelligence cycle. Proactively develop intelligence to provide support in accomplishing TSP objectives and mission.

Excellent verbal and written communication skills. Proficient in Microsoft Windows OS and Microsoft Suite. Demonstrated ability to work in a fast-paced environment and meet deadlines. Strong problem-solving skills with an interest and ability to conduct analysis and report on findings.

The candidate must demonstrate the ability to work independently in providing consulting, research and analytical products (Classified and Unclassified) on specialized projects that are professional in nature. The ability to plan and manage an activity with committed objectives, schedules, and costs.

***Functional Responsibility:***

Conduct research and analyze data to establish trends, identify threats, vulnerabilities, and potential areas of interest for TSP programs. Provide TSP support by utilizing specialized software provided for data mining and link analysis. Establish a fundamental understanding of DOE and TSP operations to include policies and procedures, and data sources available for analysis. Demonstrate fundamental understanding of investigative and intelligence processes to include the intelligence cycle. Proactively develop intelligence to assist in accomplishing TSP objectives and mission. Submit detailed reports to DOE regarding research and intelligence findings.

Other functions are to provide, within the specialty area, plan and initiate studies for original or advanced areas of customer problems and determines the techniques or methods involved that will accomplish the objectives. Develop and analyze analytical data, techniques and methodology for the solution of highly complex problems. Review reports and other products intended for release to the customers to ensure that technical merit and style of presentation reflect the highest quality. Analyze problem studies and problem history and prepare technical and managerial reports, including feasibility and desirability of extensions or modifications to the problem, program or system. Generally, provide knowledge and problem-solving abilities that are integral to the project in a specialty area of study.

***Minimum Education:***

A college degree is not required, but the applicant must have seven (7) years of experience in a specific field related to the scope of work. Requires thorough knowledge of the principles and concepts of National Level Analytical and Research Products. Must meet and maintain appropriate clearances and Special Access Program (SAP) and Sensitive Compartmental Information (SCI) eligibility.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**CYBER/NETWORK SECURITY SPECIALIST LEVEL 1 (1 FTE, non-key)**

***Job Summary*:**

The primary function of Cyber/Network Security Specialist will be to support TSP operations and teams during the conduct of and Technical Security investigations, inquiries, inspections and reviews. Must be familiar with security policy/manuals and the appropriate DOE, Committee on National Security Systems (CNSS), Intelligence Community (IC) and other guiding policy documents. Must have the ability to work in a dynamic environment and effectively interact with numerous DOE, military/civilian personnel and industry partners. Working knowledge of Microsoft Office (Word, PowerPoint, and Excel). Possess a high degree of originality, creativity, initiative requiring minimal supervision.

Willingness to travel within the organizational geographic Area of Responsibility (AOR)

Must be able to lift up to 50 lbs.

May be required to obtain additional skills and/or certifications related to cyber/digital/network analysis.

***Functional Responsibility:***

Safeguards network against unauthorized infiltration, modification, destruction or disclosure. Conduct network traffic analysis for anomalies.

Research, evaluate, test, and recommend new security software or devices.

Provides recommendations on information assurance engineering standards, implementation dependencies, changing information assurance related technologies.

Prepares evaluation reports. Recommends remedial action.

Perform risk assessments and make recommendations to customers.

Advise government program managers on security testing methodologies and processes.

Periodically review system security to accommodate changes to policy or technology.

Coordinate Automated Information System (AIS) security inspections, tests, and reviews as part of TSP operations and surveys.

Develop policies and procedures for responding to security incidents, and for investigating and reporting security violations and incidents.

Ensure proper protection or corrective measures have been taken when an incident or vulnerability has been discovered within a system

Evaluate threats and vulnerabilities to ascertain whether additional safeguards are needed.

Assess changes in the system, its environment, and operational needs that could affect create technical security vulnerabilities.

Provide support services for Conduct periodic testing of the security posture of the AIS.

Provide expert research and analysis in support of expanding programs and area of responsibility

***Minimum Education/General Experience:***

Documented experience analyzing and synthesizing information with other relevant data sources, providing guidance and mentor-ship to others in cyber threat analysis and operations, evaluating, interpreting, and integrating all sources of information, and fusing computer network attack analyses with counterintelligence and law enforcement investigations.

Bachelor's degree in the IT or Computer Security field with two (2) years of experience; or associate degree in the Information Technology or Computer Security field with three (3) years of experience; or five (5) years of experience with Local Area Networks, Wide Area Networks, and workstations. Must be certified Information Assurance Technician (IAT) Level 1 IAW DoD Directive 8570.01-M. Must meet and maintain Special Access Program (SAP) and Sensitive Compartmental Information (SCI) eligibility. Must have Global Industrial Cyber Security Certification (GICSP) and GIAC Security Essentials (GSE) Certification.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**CYBER/NETWORK SECURITY SPECIALIST LEVEL 2 (1 FTE, non-key)**

***Job Summary*:**

The primary function of Cyber/Network Security Specialist will be to support and augment TSP operations and teams during the conduct of and Technical Security investigations, inquiries, inspections and reviews. Must be familiar with security policy/manuals and the appropriate DOE, CNSS, IC and other guiding policy documents. Must have the ability to work in a dynamic environment and effectively interact with numerous DOE, military/civilian personnel and industry partners. Working knowledge of Microsoft Office (Word, PowerPoint, and Excel). Possess a high degree of originality, creativity, initiative requiring minimal supervision.

Willingness to travel within the organizational geographic Area of Responsibility (AOR)

Must be able to lift up to 50 lbs.

Maybe required to obtain additional skills and/or certifications related to cyber/digital/network analysis.

***Functional Responsibility:***

Safeguards network against unauthorized infiltration, modification, destruction or disclosure. Conduct network traffic analysis for anomalies. Research, evaluate, test, and recommend new security software or devices. Provides recommendations on information assurance engineering standards, implementation dependencies, changing information assurance related technologies.

Perform risk assessments and make recommendations to customers.

Provide recommendations to Government program managers on security testing methodologies and processes.

Periodically review system security to accommodate changes to policy or technology.

Coordinate AIS security inspections, tests, and reviews as part of TSP operations and surveys.

Develop policies and procedures for responding to security incidents, and for investigating and reporting security violations and incidents. Prepares evaluation reports. Recommends remedial action.

Ensure proper protection or corrective measures have been taken when an incident or vulnerability has been discovered within a system.

Evaluate threats and vulnerabilities to ascertain whether additional safeguards are needed.

Assess changes in the system, its environment, and operational needs that could affect create technical security vulnerabilities. Conduct periodic testing of the security posture of the AIS.

Provide expert research and analysis in support of expanding programs and area of responsibility.

***Minimum Education/General Experience:***

Documented experience analyzing and synthesizing information with other relevant data sources, providing guidance and mentor-ship to others in cyber threat analysis and operations, evaluating, interpreting, and integrating all sources of information, and fusing computer network attack analyses with counterintelligence and law enforcement investigations.

Bachelor's degree in the Information Technology or Computer Security field with two (2) years of experience; or associate degree in the Information Technology or Computer Security field with three (3) years of experience; or five (5) years of experience with Local Area Networks, Wide Area Networks, and workstations. Must meet and maintain Special Access Program (SAP) and Sensitive Compartmental Information (SCI) eligibility. Must have Global Industrial Cyber Security Certification (GICSP) and GIAC Security Essentials (GSE) Certification. Must be certified Information Assurance Technician (IAT) Level 2 IAW DoD Directive 8570.01-M.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**Digital Forensic Specialist (1 FTE, non-key)**

***Job Summary*:**

The Digital Forensics Analyst performs a variety of highly technical analyses and procedures dealing with the collection, processing, preservation, analysis, and presentation of computer-related evidence, and is responsible for disseminating and reporting cyber-related activities, conducting vulnerability analyses and risk management of computer systems and recovering information from computers and data storage devices. Computer forensic analysts use forensic tools and investigative methods to find specific electronic data, including Internet use history, word processing documents, images and other files. This expert is not only proficient in the latest forensic, response, and reverse engineering skills, but is astute in the latest exploit methodologies.

***Functional Responsibility:***

Will be required to recover information from computers and data storage devices, often working alongside technical security Technicians, Security, Counterintelligence and law enforcement officers helping to solve security issue or find electronic evidence.

May be required to recover data like documents, photos and e-mails from computer hard drives and other data storage devices, such as zip and flash drives that have been deleted, damaged or otherwise manipulated. Examine computers find evidence of illegal activity. Use expertise in a corporate setting to protect computers from infiltration, determine how a computer was broken into or recover lost files.

Utilize use forensic tools and investigative methods to find specific electronic data, including Internet use history, word processing documents, images and other files, hunt for files and information that may have been hidden, deleted or lost. Assist officials, analyze data, and evaluate its relevance to the service request. Transfer the evidence into a format that can be used for legal purposes.

Provide network security services for customer to protect against and identify outside threats. The Forensic Specialist will perform a full spectrum forensic analysis across multiple types of computer and network devices, Windows/Linux hosts, mobile devices, virtual machines, software and hardware. The candidate is expected to stay up-to-date with industry forensics best practices, industry accepted forensic methodologies, in addition to being responsible for the overall quality control of forensic investigations and related case reporting.

***Minimum Education/General Experience:***

A bachelor's degree in cyber/digital forensics, computer engineering, computer science, or other closely related IT discipline. Equivalent work of eight (8) years' of demonstrated experience may be considered on a case by case basis. Demonstrated experience using EnCase and Open Source methods and tools to perform Computer Forensic investigations. Minimum 5 years' of progressively responsible experience performing forensic investigations, malware reverse engineering, cyber security incident response, with a minimum of 3 years of experience specifically conducting cyber forensic investigations. Must meet and maintain Special Access Program (SAP) and Sensitive Compartmental Information (SCI) eligibility.

Must be certified Information Assurance Technician (IAT) Level 1 IAW DoD Directive 8570.01-M within 12 months of hiring.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**TECHNICAL SECURITY ADMINISTRATIVE SPECIALIST (1 FTE, non-key)**

***Job Summary*:**

Provide executive level technical security and administrative support to the DOE Office of Technical Security. The candidate must possess knowledge of the DOE general administration, basic DOE physical and technical security requirements. The candidate must be familiar with utilization of classified databases and networks for research and creating Intelligence Information Reports (IIR). Provide coordination support for all technical security members. Efficient with computer applications, be able to track and complete multiple tasks, maintain various administrative reports and databases, proper handle classified information and review technical and executive reports for administrate correctness. Provide general administrative support and other-directed tasks to the DOE TSP staff. Detailed oriented and proficient with Microsoft Office products.

***Functional Responsibility*:**

Provide administrative support for DOE Office of Technical Security. As requested, provides Executive Level status reports, briefing presentations and special projects support. Use work breakdown structures to track project activities. Assist in preparing charts, tables, graphs, and diagrams to assist in tracking and reporting program activities.

Coordinate and maintain office equipment, property/equipment inventories, and office vehicles as assigned by the DOE. Possess basic knowledge and/or experience in security disciplines, such as; Physical, Technical, Information, Computer Security, OPSEC, etc.

***Minimum Education*:**

Undergraduate degree is desired. A combination of a minimum of 5 years of related work experience and training is required. Work experience includes technical and physical security related areas, office management, executive administrative support, suspense tracking, review of executive level correspondence, database administration, financial and project status tracking and reporting, monthly reports, maintaining operating procedures, electronic database operations management, administrative and correspondence processing procedures, and understanding of procedures required for processing actions for review/ approval and release.

**(Minimum Position Requirement TBD, must meet above RFP minimum)**

(TBD)

**K.2 FAR 52.204-8 ANNUAL REPRESENTATIONS AND CERTIFICATIONS. (OCT 2018)**

(a)

(1) The North American Industry classification System (NAICS) code for this acquisition is 561621.

(2) The small business size standard is $20,500,000.00.

(3) The small business size standard for a concern which submits an offer in its own name, other than on a construction or service contract, but which proposes to furnish a product which it did not itself manufacture, is 500 employees.

(b)

(1) If the provision at 52.204-7, System for Award Management, is included in this solicitation, paragraph (d) of this provision applies.

(2) If the provision at 52.204-7, System for Award Management, is not included in this solicitation, and the Offeror has an active registration in the System for Award Management (SAM), the Offeror may choose to use paragraph (d) of this provision instead of completing the corresponding individual representations and certifications in the solicitation. The Offeror shall indicate which option applies by checking one of the following boxes:

[TBD\_] (i) Paragraph (d) applies.

[TBD\_] (ii) Paragraph (d) does not apply and the offeror has completed the individual representations and certifications in the solicitation.

(c)

(1) The following representations or certifications in SAM are applicable to this solicitation as indicated:

(i) 52.203-2, Certificate of Independent Price Determination. This provision applies to solicitations when a firm-fixed-price contract or fixed-price contract with economic price adjustment is contemplated, unless—

(A) The acquisition is to be made under the simplified acquisition procedures in Part 13;

(B) The solicitation is a request for technical proposals under two-step sealed bidding procedures; or

(C) The solicitation is for utility services for which rates are set by law or regulation.

(ii) 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions. This provision applies to solicitations expected to exceed $150,000.

(iii) 52.203-18, Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements—Representation. This provision applies to all solicitations.

(iv) 52.204-3, Taxpayer Identification. This provision applies to solicitations that do not include the provision at 52.204-7, System for Award Management.

(v) 52.204-5, Women-Owned Business (Other Than Small Business). This provision applies to solicitations that—

(A) Are not set aside for small business concerns;

(B) Exceed the simplified acquisition threshold; and

(C) Are for contracts that will be performed in the United States or its outlying areas.

(vi) 52.209-2, Prohibition on Contracting with Inverted Domestic Corporations—Representation.

(vii) 52.209-5; Certification Regarding Responsibility Matters. This provision applies to solicitations where the contract value is expected to exceed the simplified acquisition threshold.

(viii) 52.209-11, Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law. This provision applies to all solicitations.

(ix) 52.214-14, Place of Performance--Sealed Bidding. This provision applies to invitations for bids except those in which the place of performance is specified by the Government.

(x) 52.215-6, Place of Performance. This provision applies to solicitations unless the place of performance is specified by the Government.

(xi) 52.219-1, Small Business Program Representations (Basic & Alternate I). This provision applies to solicitations when the contract will be performed in the United States or its outlying areas.

(A) The basic provision applies when the solicitations are issued by other than DoD, NASA, and the Coast Guard.

(B) The provision with its Alternate I applies to solicitations issued by DoD, NASA, or the Coast Guard.

(xii) 52.219-2, Equal Low Bids. This provision applies to solicitations when contracting by sealed bidding and the contract will be performed in the United States or its outlying areas.

(xiii) 52.222-22, Previous Contracts and Compliance Reports. This provision applies to solicitations that include the clause at 52.222-26, Equal Opportunity.

(xiv) 52.222-25, Affirmative Action Compliance. This provision applies to solicitations, other than those for construction, when the solicitation includes the clause at 52.222-26, Equal Opportunity.

(xv) 52.222-38, Compliance with Veterans' Employment Reporting Requirements. This provision applies to solicitations when it is anticipated the contract award will exceed the simplified acquisition threshold and the contract is not for acquisition of commercial items.

(xvi) 52.223-1, Biobased Product Certification. This provision applies to solicitations that require the delivery or specify the use of USDA-designated items; or include the clause at 52.223-2, Affirmative Procurement of Biobased Products Under Service and Construction Contracts.

(xvii) 52.223-4, Recovered Material Certification. This provision applies to solicitations that are for, or specify the use of, EPA- designated items.

(xviii) 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals—Representation. This provision applies to solicitations that include the clause at 52.204-7.

(xix) 52.225-2, Buy American Certificate. This provision applies to solicitations containing the clause at 52.225-1.

(xx) 52.225-4, Buy American--Free Trade Agreements--Israeli Trade Act Certificate. (Basic, Alternates I, II, and III.) This provision applies to solicitations containing the clause at 52.225- 3.

(A) If the acquisition value is less than $25,000, the basic provision applies.

(B) If the acquisition value is $25,000 or more but is less than $50,000, the provision with its Alternate I applies.

(C) If the acquisition value is $50,000 or more but is less than $80,317, the provision with its Alternate II applies.

(D) If the acquisition value is $80,317 or more but is less than $100,000, the provision with its Alternate III applies.

(xxi) 52.225-6, Trade Agreements Certificate. This provision applies to solicitations containing the clause at 52.225-5.

(xxii) 52.225-20, Prohibition on Conducting Restricted Business Operations in Sudan--Certification. This provision applies to all solicitations.

(xxiii) 52.225-25, Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran—Representation and Certification. This provision applies to all solicitations.

(xxiv) 52.226-2, Historically Black College or University and Minority Institution Representation. This provision applies to solicitations for research, studies, supplies, or services of the type normally acquired from higher educational institutions.

(2) The following representations or certifications are applicable as indicated by the Contracting Officer:

[Contracting Officer check as appropriate.]

\_\_\_ (i) 52.204-17, Ownership or Control of Offeror.

\_\_\_ (ii) 52.204-20, Predecessor of Offeror.

\_\_\_ (iii) 52.222-18, Certification Regarding Knowledge of Child Labor for Listed End Products.

\_\_\_ (iv) 52.222-48, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Certification.

\_\_\_ (v) 52.222-52 Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Certification.

\_\_\_ (vi) 52.223-9, with its Alternate I, Estimate of Percentage of Recovered Material Content for EPA-Designated Products (Alternate I only).

\_\_\_ (vii) 52.227-6, Royalty Information.

\_\_\_ (A) Basic.

\_\_\_ (B) Alternate I.

\_\_\_ (viii) 52.227-15, Representation of Limited Rights Data and Restricted Computer Software.

(d) The Offeror has completed the annual representations and certifications electronically in SAM accessed through [https://www.sam.gov](https://www.sam.gov/). After reviewing the SAM information, the Offeror verifies by submission of the offer that the representations and certifications currently posted electronically that apply to this solicitation as indicated in paragraph (c) of this provision have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201); except for the changes identified below [offeror to insert changes, identifying change by clause number, title, date]. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

|  |  |  |  |
| --- | --- | --- | --- |
| FAR Clause | Title | Date | Change |
|    |    |    |    |
|    |    |    |    |

Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted on SAM.