

SAFEGUARDS & SECURITY PROGRAMS SUPPORT SERVICES

STATEMENT OF WORK

1.0 OBJECTIVE

The objective of this contract is to provide diverse technical safeguards and security support services required to assist the Security Support Department (SSD) and Office of Secure Transportation (OST) in the implementation of safeguards and security programs for the Department of Energy (DOE), National Nuclear Security Administration (NNSA), NNSA Service Center, and to OST facilities located at Kirtland Air Force Base, Albuquerque, New Mexico.

2.0 BACKGROUND

The NNSA mission includes being a responsible steward of the Nation's nuclear weapons. DOE/NNSA is a vital contributor to reducing the global nuclear danger through its national security, nuclear safety, nonproliferation activities, and nuclear materials stabilization by supporting a safe, secure, reliable stockpile, and the safe dismantlement and disposal of excess nuclear weapons.

The multi-disciplined NNSA Service Center safeguards and security programs are the first line of defense against the insider threat and are designed to protect our most vital national assets. These programs directly support weapons and national security objectives through an integrated nuclear weapon technology infrastructure and core competencies that ensure (a) safety, security, and reliability of the enduring stockpile, (b) the safe and secure dismantlement of nuclear weapons, (c) safe and secure staging of nuclear components and materials awaiting permanent disposition, (d) proper classification and controlled information guidance is provided to the NNSA, (e) only trustworthy individuals receive/maintain a DOE access authorization to classified materials, information, and facilities, and (f) protection of government property and personnel located at the NNSA Service Center Complex and other NNSA facilities located on Kirtland Air Force Base at Albuquerque, New Mexico, as required.

SSD is responsible for the management, implementation, and oversight of diverse DOE and NNSA safeguards and security programs at (a) NNSA Site Offices, (b) NNSA Service Center, (c) NNSA headquarters/project offices and other activities co-located at the Service Center, and (d) DOE and NNSA contractors and their subcontractors. SSD is currently organized into three divisions: the Personnel Security Division (PSD), the Security Programs Division (SPD), and the Classification and Controlled Information Division (CCID). The responsibilities include coordination, development, implementation, and programmatic oversight of DOE and NNSA safeguards and security policy, including but not limited to: the Personnel Security Program, Safeguards and Security Programs, Protective Force Services, and the Classification and Controlled Information Program. SSD serves as the primary point of contact for federal, state, and private agencies on matters concerning safeguards and security programs under NNSA Service Center cognizance.

OST is responsible for the transportation, security and safeguarding of nuclear explosives, devices and Category I special nuclear material, and other material vital to the national security.

3.0 SCOPE

The work supports office and technical requirements necessary for the successful accomplishment of SSD program responsibilities, as well as protective force operations support to the NNSA Service Center and OST facilities in Albuquerque, New Mexico. The preponderance of work is performed at the NNSA Service Center and Site Support Offices/facilities. Travel is required to NNSA Site Offices, and to DOE and NNSA sites/facilities when necessary to perform assignments associated with safeguards and security responsibilities.

At time of contract award and subsequent performance, the contractor shall furnish qualified and skilled personnel, equipment, supplies, services, materials, and training necessary to provide the required technical support services to perform work as described herein, except what is expressly cited in the contract as being furnished by the government. Formal DOE/NNSA training opportunities for the technical requirements described in paragraph 4.0 are limited. Technical guidance is available at all

times, however, the contractor is responsible for training contractor employees and shall ensure that all contractor employees are sufficiently qualified to performed the technical requirements and functions as described in the Technical Requirements and in the Minimum Personnel Qualifications Requirements.

The contractor shall provide primary SSD security services between the hours of 7:30 a.m. and 5:00 p.m. Monday through Friday, with the exception of Protective Force Services which shall be provided on a 24-hour, 7-days a week basis ("24X7"), 365 days a year to both SSD and OST.

Work Environment: Except as noted elsewhere in this SOW and for Protective Force operations, work is largely sedentary. Workspace is limited in an "open" office environment subject to constant noise and distraction. Protective Force operations include fixed post and outdoor roving foot patrols in all types of weather.

4.0 TECHNICAL REQUIREMENTS

The Program Manager is responsible for overall program management, serves as a single point of contact to the NNSA Service Center, and represents the contractor in dealing with senior NNSA Service Center management; manages resources, costs, and conflicts; provides overall direction to contractor personnel; provides reports identified in the Reporting Requirements Checklist, and ensures the quality and timeliness of deliverables and completed assignments. The contractor shall provide technical support with expertise in, but not limited to, the following areas:

4.1 Personnel Security Program

The contractor shall provide technical support expertise for the implementation of the DOE Personnel Security Program to include, but not limited to, clearance processing, adjudication of investigative reports or other security related information, management and administration of Human Reliability and Special Access Programs, and the Administrative Review process. Clearance and adjudicative actions shall be completed in accordance with Executive Orders, U.S. Code of Federal Regulations, and DOE Headquarters, NNSA and NNSA Service Center orders, policies, directives, and regulations. The contractor uses experience in applying procedures, policies, and/or precedents; determines when further information is required; contacts appropriate source to obtain information and maintains a range of personal contacts within and outside the NNSA, NNSA Service Center, and the Personnel Security Division, being tactful and articulate; performs routine statistical data analysis related to clearance and adjudicative actions and expenditures. DOE/NNSA technical guidance is available at all times, however, the contractor should work independently with reviews conducted by DOE/NNSA oversight to ensure assignments and deliverables are completed against stated objectives and assignments. The contractor makes recommendations only; final decisions regarding access authorizations are made by DOE.

4.1.1 Adjudication

Provide expertise, to include training of contractor personnel security specialists, in the review and analysis of investigative reports in order to be able to correctly identify and evaluate derogatory and mitigating information; provide adjudicative deliverables as described in Section 5.0. of this SOW to include, but not limited to, prepare case evaluations and recommend appropriate security action(s); prepare letters of interrogatory, reports, or other security related documents, as appropriate; conduct in-depth personnel security interviews in accordance with DOE policies and procedures; prepare interview summaries and recommend appropriate security action; prepare correspondence related to any subsequent security action, such as psychiatric evaluations, clearance suspensions, administrative reviews; testify before a Hearing Officer during Administrative Review hearings when deemed appropriate by the Director, Personnel Security Division.

4.1.2 Clearance Management

Provide expertise, to include training of contractor clearance management contractor staff, in document control to prepare/process, route/transmit, and control personnel security documents and files, and provide clearance management deliverables as described in Section 5.0. of this SOW to include, but not limited to, the following: review clearance packages for initial clearances and reinvestigations to ensure information is complete and consistent with procedures, policies and/or precedents; transmit the reviewed

clearance packages to investigative agency. Clearance packages must be processed, completed, and transmitted in accordance with DOE and Office of Personnel Management (OPM) requirements. Documents include clearance request forms, security questionnaires; fingerprint charts, foreign residence and foreign interest questionnaires, and any other documents provided in support of the clearance action.

4.1.3 Personnel Security Related Deliverables

The personnel security program work involves numerous and varied personnel security access authorization adjudicative and processing activities, as well as investigating and analyzing the background of approximately 40,000 clearance holders/applicants, including approximately 5000 human reliability program incumbents. The population of clearance holders is anticipated to increase to approximately 55,000-60,000 incumbents by the end of CY 2004.

The backgrounds of applicants for DOE access authorizations, and incumbents with DOE access authorizations, may involve alcohol abuse/dependency, drugs, sex perversion, unreliable and untrustworthy behavior, mental/emotional instability, etc. Recommendations made and actions taken by the contractor in these matters determine whether an individual receives (or keeps) his/her clearance. For many individuals this determines whether they maintain their jobs.

Timeliness is of the essence. The contractor will provide the expertise to ensure the timely and effective administration and completion of the numerous adjudicative, clearance management, and processing activities, actions, and products. These deliverables and activities and their associated timeframes include, but are not limited to, those identified in the Table of Personnel Security Deliverables in 5.0. of the SOW. DOE reserves the right to add, delete, or modify deliverables and timeframes as necessary to ensure that the personnel security program is managed and executed in accordance with applicable laws, statutes, codes, and DOE/NNSA Orders, guidelines, directives, and policies.

4.1.4 Security Related Documents

Provide expertise to review for completeness and process other security-related documents, such as requests for clearance extensions, transfers, reinstatements, terminations, spouse/cohabitant data documents, incident reports, requests for personnel security files or information therein, and any other requests related to a personnel security action; process microfilm/microfiche into hard copy reports; access credit report system and produce credit reports; query OPM data base for investigation status.

4.1.5 Duplication of Security Records

Provide expertise for the duplication of security records, including personnel security files, to support various security initiatives, such as Administrative Review, psychiatric evaluations, and special program clearances.

4.1.6 Correspondence

Provide expertise to prepare draft and final correspondence, including forms, letters, and memorandums, related to security activities. Documents are available on templates and are to be completed in accordance with requirements cited in DOE correspondence manuals and the specific form instructions.

4.1.7 Mail Station

Provide expertise to maintain an SSD mail station adequate to: a) receive, time/date stamp, and distribute incoming mail; b) prepare outgoing correspondence for mailing by ensuring appropriate signatures and attachments, date stamp, copy as required, and distribute as appropriate for internal/external delivery; c) package mail, including classified mail and personnel security files, in accordance with DOE and NNSA regulations, Administrative Review procedures, Privacy Act and classified mail procedures, as appropriate.

4.1.8 Records Management

Provide expertise to operate the personnel security vault by maintaining the control and accountability for the NNSA Service Center active and terminated personnel security files, to include classified and unclassified files or documents; operate the personnel security bar code system to ensure efficient file tracking and retrieval; facilitate the DOE personnel security file destruction program for NNSA and the

NNSA Service Center; recommend changes to records management procedures to facilitate personnel security operations; and maintain personnel security files in strict accordance with DOE/NNSA Orders, guidelines, directives, and policies.

4.1.9 Data Entry

Provide expertise to maintain the DOE and NNSA Service Center personnel security databases as they pertain to clearance history and/or activity at the NNSA Service Center. DOE/NNSA technical guidance is available at all times and should be acquired when unusual questions arise related to changes to be made to a clearance history. Only authorized personnel shall perform deletion of a clearance record. The data entry includes, but is not limited to, the following activities: create and update data base records of personnel security actions using the personnel security data base residing on a mainframe at DOE Headquarters; create and update database records of personnel security actions using the NNSA Service Center data base designed to provide an audit trail for clearance actions and a tracking system for file location; ensure information is complete and consistent with procedures, policies, and/or precedents; determine when further information is required to reflect an accurate history; reconcile the DOE Headquarters personnel security data against the NNSA Service Center data and Site Office data as requested; reconcile the DOE Human Resources employment records against access authorization activity as requested.

4.1.10 Information Management

Provide expertise to administer and maintain the DOE and NNSA Service Center personnel security databases as they relate to personnel security access authorizations assigned to the NNSA Service Center; create and update database records as required to ensure accurate clearance activity for each access authorization holder and applicant; extract data necessary to prepare statistical, management, survey/inspection, reconciliation, and ad hoc reports; extract data necessary to prepare briefing materials; administer and maintain an automated reinvestigation system adequate to track the reinvestigation process of clearance holders due for reinvestigation, such as to identify individuals due for reinvestigation, requests for and receipt of clearance paperwork, and submission to the investigative agency; administer and maintain a clearance action tracking system sufficient to identify specific clearance activities and time lines of clearance requests, such as to accurately and timely identify the nature of clearance requests received, status, and completion of personnel security clearance and adjudication activities and actions.

4.1.11 Budget Reporting

Provide expertise to maintain a budget reporting system adequate to account for the expenditure of security investigation funds; travel funds; prepare monthly expenditure reports to DOE and NNSA Headquarters, NNSA Service Center Financial Services, and NNSA sites/facilities; prepare ad hoc reports as requested.

4.1.12. Work Environment: Work is largely sedentary. Workspace is limited in an “open” office environment subject to constant noise and distraction. Continuous heavy workload with deadlines causes stress and may necessitate overtime. During the conduct of interviews and delivering of suspensions or administrative review correspondence and documents, the contractor many times encounters unwilling, hostile, and/or emotional subjects. Work involves frequent travel for training, the conduct of personnel security interviews, surveys, testifying at administrative hearings, and so forth.

4.2 Safeguards and Security Programs

The contractor shall provide technical support expertise for review, development, implementation, evaluation, and inspection of all safeguards and security programs in Section 4.0 of the SOW, including but not limited to, Program Management, Program Planning and Administration; Personnel Development and Training; Facility Clearance and Registration Activities; Foreign Ownership, Control, or Influence (FOCI); Unclassified Visits and Assignments by Foreign Nationals; Security Plans; Security Education Briefings and Awareness; Surveys and Self-Assessments; Resolution of Findings; Incident Reporting and Management . DOE/NNSA technical guidance is available at all times; however, the contractor should work independently with reviews conducted by DOE/NNSA to ensure assignments and deliverables are

completed against stated objectives and assignments. The contractor makes recommendations only; final decisions are made by DOE/NNSA.

4.2.1 Foreign Ownership, Control, or Influence Program

The contractor shall provide technical support expertise, to include training, for the implementation of the Foreign Ownership, Control, or Influence (FOCI) Program. The contractor shall review companies for FOCI. The contractor screens, reviews, and evaluates documents including those that contain substantial foreign interests, and makes recommendation regarding the company's FOCI. Assures completeness of documentation identifies and analyzes foreign interests and mitigating information, prepares detailed written analysis of all available information, and makes written determination or recommendations for further action. The contractor must be able to conduct in-depth interviews with presidents and attorneys of large corporations, and provide guidance or input regarding the company's FOCI. The contractor provides guidance and training to the M&O contractors, and other as required, regarding FOCI

4.2.2 Facility Clearances and Registration of Safeguards and Security Activities

The contractor shall provide technical expertise, to include training, for the registration of facility clearances. The contractor ensures that all requirements of the facility clearance have been met; to include, but not limited to, a thorough and complete site security plan, satisfactory survey(s), FOCI, and justifying activity. The contractor must have a thorough knowledge of the Safeguards and Security Information Management System, and register, update and maintain facilities (FDAR's), and activities (CSCS's) as necessary.

4.2.3 Resolution of Findings

The contractor shall assist with the resolution of findings. Conducts root cause analysis of findings, and develops corrective action plans and milestones as appropriate. Assures that milestones are met and that corrective measures are taken to ensure the closure and validation of findings. Ensures that corrective actions are entered in the SSIMS or other tracking system as appropriate.

4.2.4 Security Education Briefings and Awareness

The contractor provides expertise and support to the Security Education Coordinator. The contractor prepares and conducts briefings as necessary.

4.2.5 Security Badges and Visitor Control

The contractor provides expertise, to include training, for badging and visitor control for the NNSA/SC site, to include the implementation of program changes.

4.2.6 Survey and Self-Assessment Support

The contractor shall provide subject matter experts for the review, evaluation, and inspection/survey of various possessing, non-possessing, or property protection facilities, as directed. The contractor shall provide expertise to conduct all elements of a safeguards and security survey. To include, but not limited to, planning meetings; review of safeguards and security plans, review of site vulnerability analyses; review of previous inspection/surveys reports; review of applicable DOE orders and manuals; the development implementation of performance tests, conduct of threat evaluation and validation; preparation of inspection plans; conduct of thorough survey to include sampling and interviews with appropriate officials; and preparation of a comprehensive report in accordance with established format.

4.2.7 Planning Assistance

Provide expertise in security-related management activities, such as emergency operation and limited scope performance tests for all topical areas.

4.2.8 Review Safeguards and Security Documents

Provide expertise in the review, evaluation, and validation of safeguards and security plans, reports, studies, evaluations, and analyses.

4.2.9 Vulnerability Assessment and Risk Analysis

Provide expertise in the development and validation of the methods used in assessing vulnerabilities; the operation of vulnerability assessment codes; and the preparation of risk analyses as required.

4.2.10 Technical Security Support

Provide specialized technical expertise with computer security, TSCM, TEMPEST, Protected Transmission Systems, intrusion detection, access control, and physical security; review technical security projects and documentation to include costs estimates, prints, specifications, methods, schedules and milestones; review completed projects; develop recommendations regarding suitability based upon applied standards.

4.2.11 Safeguards and Security Program Review

Provide expertise in program reviews to include: DOE orders; Vulnerability Assessments; SSSP's and Site Security Plans; Conception Design Plans for Construction Projects; Alarm Testing and Maintenance Plans; Sensitive Compartmented Information Facility Plans; Protective Force Annual Training Plans; Training Approval Plans; Classified Computer Security Plans; TEMPEST Plans; Protected Transmission System Plans; Telecommunications Plans; Secure Video teleconferencing Plans; TSCM Plans; Foreign Visit and Assignment Plans; Corrective Action Plans; Self-Assessment Plans; develop recommendations for suitability based upon applied standards and prepare reports.

4.2.12 Information Management

Provide expertise in the development, implementation, and maintenance of all intra-and inter-office information management systems to include project tracking, action tracking, accountability and control of classified matter, facility clearance and registration of activities, classified mailing address verification to include support for data and file entry. Provide expertise and support to the information security program including, but not limited to, the Classified Matter Protection and Control program, Classified and Controlled Information; Special Access Programs and Intelligence Information; Classified Automated Information Systems Security; Unclassified Automated Information Systems Security; Technical Surveillance Countermeasures (TSCM); Operations Security (OPSEC); Protected Transmission Systems; Communications Security (COMSEC).

4.2.13 General Technical Assistance

Provide expertise in the development of presentations and documents related to safeguards and security programs, including technical writing and security programs.

4.2.14 Safeguards and Security Special Security Projects

Provide expertise with special projects related to safeguards and security programs.

4.2.15 Correspondence

Provide expertise to prepare draft and final correspondence, including forms, letters, and memorandums, related to security activities. Documents are available on templates, and are to be completed in accordance with requirements cited in DOE/NNSA and NNSA Service Center correspondence manuals and the specific form instructions.

4.2.16 Records Management

Provide expertise to maintain and operate a filing system by maintaining the control and accountability for documents, to include classified and unclassified files; ensure efficient file tracking and retrieval; facilitate the destruction program in accordance with established Records Inventory Disposal Schedules.

4.2.17 Incidents of Security Concern

Provide incidents of security concern program support by performing inquiries and completing required documentation in accordance with NNSA Orders, Directives, and guidelines.

4.3 Protective Force Services

The contractor shall provide expertise in the operation of an unarmed guard service for the protection of all property and personnel located at the NNSA Service Center complex and its adjacent facilities located on Kirtland Air Force Base (KAFB), New Mexico, and to OST facilities located on KAFB, New Mexico.

The services include fixed post and foot patrols, 24-hours a day, 365 days a year. The service includes continuous site video surveillance and response. Inclement weather or other reasons for closure of the base or the AL complex does not affect the protective services provided by the contractor; otherwise, the NNSA Service Center complex is governed by tenant regulations of KAFB. The Protective Force is responsible for guard services and not law enforcement services; the KAFB Security Police will provide law enforcement services. The contractor shall assist, as appropriate, law enforcement personnel to facilitate resolution and to protect government property. The contractor retains the prime responsibility for NNSA Service Center and OST site security irrespective of incident responder. Auxiliary services shall be provided at the request of the government, e.g., providing additional personnel in special situations. Protective Force Officers will be attired in a recognizable, professional, and uniformed manner, subject to DOE/NNSA approval; and deal courteously with the public and personnel of DOE, NNSA, and its contractors. The Protective Force will be required to demonstrate knowledge and proficiency through periodic limited scope performance tests. The Protective Force shall perform assigned work in accordance with DOE and NNSA orders/manuals and/or internal procedures, policies, and directives. DOE and NNSA technical guidance is available at all times; however, the contractor should work independently with reviews conducted by DOE and NNSA oversight to ensure assignments are completed against stated objectives. The contractor makes recommendations only; the DOE/NNSA make final decisions.

4.3.1 Access Control

Provide expertise in the control of access to ensure entry into the NNSA Service Center complex is limited to individuals possessing appropriate credentials. Scrutiny of credentials must be sufficient to reasonably verify the identity and clearance level of the bearer. Access is controlled at all personnel and vehicle entry points. Prompt and courteous service is expected when dealing with personnel and the public; courteous but firm service is expected when conducting security responsibilities. Provide expertise on the upkeep and operations of the installed or newly installed access control systems with recommendation for enhancements, repairs and upgrades.

4.3.2 Emergency Responder Access

Provide expertise for the access of emergency personnel and/or vehicles from other entities responding to assist with an emergency at the NNSA Service Center complex/site; maintain access log; escort responders, if possible.

4.3.3 Issue and Accountability for Temporary Badges

Provide expertise to issue access badges to cleared and un-cleared visitors during NNSA Service Center non- operational hours; verify visitors against pre-approval list generated by the Access Control Office; establish identity of visitor through photographic identification; issue appropriate badge and confiscate badge at conclusion of visit; maintain log.

4.3.4 Alarm Systems

Provide expertise to monitor intrusion alarm systems using output and input screens as well as graphics displays; initiate emergency response procedures; maintain lists of vault custodians; maintain log of alarm activity; complete written incident reports as appropriate; verify identity of personnel performing maintenance and/or modifications to alarm systems; verify repair of alarm problem. Provide expertise on the upkeep and operations of the installed or newly installed alarm systems with the recommendation for enhancements, repairs, and upgrades. Provide and support testing of alarm system components and overall integrated effectiveness.

4.3.5 Detection/Assessment

Provide expertise in the recognition of suspicious activity, unusual events, and/or criminal activity; identification of breaks in fence lines; cognizance of office areas, vaults and safes; cognizance of security infractions; preparation of infraction reports or other security incident reports. The Protective Force Supervisor shall be notified as soon as practicable, and the incident annotated in the daily shift report.

4.3.6 Roving Patrols

Provide expertise in roving coverage of the NNSA Service Center complex and OST facilities to detect and/or mitigate potential security and safety risks; e.g., unlocked exterior doors outside the security area, indications of unauthorized entry, unauthorized individuals in motor vehicles within the security area, fire hazards within buildings as well as weeds and trash along fence lines, inappropriate objects along fence lines, and breaks in fence lines, as well as problems with outriggers and barbed wire.

4.3.7 Inspections

Provide expertise to conduct inspections, to include K-9 inspections and random searches; accompany KAFB Security Police on K-9 inspections; make appropriate notifications upon discovery of drugs, explosives, or other prohibited devices; document search results; conduct random searches of vehicles, personnel, and/or hand-carried items to deter or detect the unauthorized introduction of prohibited items or the removal of government property and/or classified documents; initiate inspections; verbal challenges must be courteous but firm.

4.3.8 Classified Storage

Provide expertise for the storage of classified packages on a temporary basis during non-operational hours; provide signed receipts for accountability; store in approved safe; adhere to safe access and locking procedures.

4.3.9 Flag Protocol

Provide expertise in the protocol of the display of the national flag.

4.3.10 Key, Combination, and Lock Control

Provide expertise in the accountability, inventory, and storage of security master keys and classified safe combinations; control opened perimeter gate padlocks; initiate compensatory measures for lost or stolen keys or padlocks; appropriate notification of emergency access to vaults, repositories, and compromise of combinations.

4.4 Classification and Controlled Information Program

The contractor shall provide technical support expertise for review, development, implementation, evaluation, and inspection of classification and controlled information programs in 4.0. These programs primarily concern Restricted Data (RD), Formerly Restricted Data (FRD), National Security Information (NSI) and Unclassified Controlled Nuclear Information (UCNI). DOE/NNSA technical guidance is available at all times; however, the contractor should work independently with reviews conducted by DOE/NNSA oversight to ensure assignments are completed against stated objectives and assignments. Frequent interaction and cooperative work with NNSA Federal staff is standard. The contractor makes recommendations only; final decisions are made by DOE/NNSA.

4.4.1 Guidance Development

Assist the Classification and Controlled Information Division (CCID) and the Office of Information Classification and Control Policy - Technical Guidance (SO-122) in their guidance development efforts. Provide expert technical support including representative membership in classification guide working groups. Review and comment on proposed changes to DOE/NNSA classification guides.

4.4.2 Training

Provide instruction, to include preparation of procedures and course development, for training of personnel in classification policies in such structured venues as Derivative Classifier courses.

4.4.3 Document Review

Work with CCID Federal staff in regularly complex document review for classification determination. Supply historical classification perspective for document determinations involving intricate weapon complex projects.

4.4.4 Litigation

As necessary, be prepared to present expert testimony to civil or criminal judicial proceedings regarding RD, FRD, NSI, and UCNI. Assist CCID staff in responding to attorney requests for classification guidance and document review.

4.4.5 Surveys and Oversight Processes

Participate in security surveys and classification oversight processes of the NNSA. Bring unique insight (attained via over 15 years of classification experience) of weapon complex operations and programs to the oversight and survey responsibilities of CCID.

4.4.6 Policy and Procedures

Maintain knowledge of classification and controlled information policy. As required, assist CCID Federal Staff to develop policy and procedures for the NNSA classification community and nuclear weapon complex. Understand the requirements of other agency and foreign government information programs.

4.4.7 Classified Matter Marking

Maintain proper knowledge of the marking of classified matter. This includes recognition and use of DOE/NNSA classified and sensitive matter markings, recognition and procedural requirements of other agency and foreign government markings, and restrictive caveats.

5.0 Deliverables

Deliverables include, but are not limited to, those items listed in the Tables of Deliverables below for the Personnel Security Division, Classification and Controlled Information Division, and the Security Programs Division, as well as technical reports, manuals, handbooks, cost management reports, as identified on DOE Form 1332.1, Reporting Requirements Checklist; or as designated in the scope of work outlined in Sections 3.0 and 4.0.

TABLE OF DELIVERABLES - PERSONNEL SECURITY DIVISION	
DELIVERABLE	TIMEFRAME/STANDARD
Adjudication (4.1.1)	
Written "Case Evaluation Summary" (CES) for investigations for applicants for a DOE access authorization that are determined to contain no derogatory information or security concerns as defined in 10 CFR 710, Subpart A.	Processed and adjudicated <u>no later than</u> 7 workdays from receipt in Personnel Security Division (PSD). NOTE: All CES's referred to in this Table of Deliverables will be prepared to acceptable contemporary professional business standards, be technically correct, and conform to DOE/NNSA and PSD, Service Center, personnel security program standards in style and content.
Written "Case Evaluation Summary" (CES) for reinvestigations for individuals with a DOE access authorization, and investigations for applicants for a DOE access authorization, that are determined to contain derogatory information or security concerns as defined in 10 CFR 710.	Processed and an adjudicative recommendation made <u>no later than</u> 30 workdays from receipt in PSD.
Review and make adjudicative recommendations (prepare a CES) on requests for reinstatements of DOE access authorizations in those cases without a background investigation.	Review completed within 3 workdays of receipt by contractor personnel security specialist (PSS)
Review and make adjudicative recommendations (prepare a CES) on requests for reinstatements of DOE access authorizations in those cases with a background investigation.	7 workdays from receipt by PSS, if no derogatory information identified in the background investigation. 30 workdays from receipt by PSS, if derogatory information identified in the background investigation
Conduct personnel security interviews (PSI) on applicants for a DOE access authorization and	PSI scheduled within 30 workdays of receipt of the background investigation and conducted as soon

TABLE OF DELIVERABLES - PERSONNEL SECURITY DIVISION	
DELIVERABLE	TIMEFRAME/STANDARD
incumbents with a DOE access authorization as approved by the DOE. PSI includes preparation of a CES, and completion of all associated adjudicative actions and activities necessary to make a complete and correct recommendation regarding the individual's eligibility for a DOE access authorization or continued eligibility for a DOE access authorization.	as possible after approved by DOE, but no later than within 90 workdays of receipt of the background investigation in PSD. Conduct of the PSI includes travel as necessary to the Site Office closest to the applicant or incumbent to conduct the interview and all necessary coordination with the Site Office to conduct the PSI. All PSI's will be conducted in strict accordance with applicable laws and DOE Orders, policy, and guidance. Contractor must be trained and qualified to conduct PSI, and approved by the DOE.
Conduct PSI on reinvestigations that contain substantial or serious derogatory information, and represent a high risk security concern, as determined by DOE. PSI includes preparation of a CES, and completion of all associated adjudicative actions and activities necessary to make a complete and correct recommendation regarding the individual's eligibility for a DOE access authorization or continued eligibility for a DOE access authorization.	Conducted within 10 workdays from DOE approval. Conduct of the PSI includes travel as necessary to the Site Office closest to the applicant or incumbent to conduct the interview and all necessary coordination with the Site Office to conduct the PSI. All PSI's will be conducted in strict accordance with applicable laws and DOE Orders, policy, and guidance. Contractor must be trained and qualified to conduct PSI, and approved by the DOE.
Conduct PSI on individuals who possess a DOE access authorization and who test positive for illegal drugs or substances, or who test positive for alcohol. PSI includes preparation of a CES, and completion of all associated adjudicative actions and activities necessary to make a complete and correct recommendation regarding the individual's eligibility for a DOE access authorization or continued eligibility for a DOE access authorization.	Conducted within 2 workdays from receipt of notification of a positive drug test if no travel involved. Conducted within 2 days if travel involved, if possible, but no later than 10 workdays from receipt of notification of a positive drug test. Conduct of the PSI includes travel as necessary to the Site Office closest to the applicant or incumbent to conduct the interview and all necessary coordination with the Site Office to conduct the PSI. All PSI's will be conducted in strict accordance with applicable laws and DOE Orders, policy, and guidance. Contractor must be trained and qualified to conduct PSI, and approved by the DOE.
Conduct PSI on individuals who possess a DOE access authorization and who are determined by the DOE to be potential candidates for the DOE EAPRO Program. PSI includes preparation of a CES, and completion of all associated adjudicative actions and activities necessary to make a complete and correct recommendation regarding the individual's eligibility for a DOE access authorization or continued eligibility for a DOE access authorization.	Conducted within 2 workdays of eligibility determination if no travel involved. Conducted as soon as possible if travel involved, but not more than 10 days from eligibility determination. Conduct of the PSI includes travel as necessary to the Site Office closest to the applicant or incumbent to conduct the interview and all necessary coordination with the Site Office to conduct the PSI. All PSI's will be conducted in strict accordance with applicable laws and DOE Orders, policy, and guidance. Contractor must be trained and qualified to conduct PSI, and approved by the DOE.
Conduct PSI's as requested by other DOE Operations Offices, including DOE Headquarters. PSI includes preparation of a CES, and completion of all associated adjudicative actions and activities necessary to make a complete and correct recommendation regarding the individual's eligibility	Conducted within 30 workdays of receipt in PSD. Conduct of the PSI includes travel as necessary to the Site Office closest to the applicant or incumbent to conduct the interview and all necessary coordination with the Site Office to conduct the PSI. All PSI's will be conducted in strict accordance with

TABLE OF DELIVERABLES - PERSONNEL SECURITY DIVISION	
DELIVERABLE	TIMEFRAME/STANDARD
for a DOE access authorization or continued eligibility for a DOE access authorization.	applicable laws and DOE Orders, policy, and guidance. Contractor must be trained and qualified to conduct PSI, and approved by the DOE.
Written CES of PSI	Within 2 workdays of conduct of PSI.
Preparation of Letter of Interrogatory (LOI)	Within 3 workdays of DOE concurrence of LOI.
Adjudicate LOI response and prepare CES.	Within 7 workdays of receipt of LOI response.
Adjudicate Psychiatric Reviews/Examinations/Analysis and prepare CES.	Within 4 workdays of receipt in PSD Branch
Prepare CES recommending Administrative Review (AR) and prepare the "Statement of Charges" (SOC)	Within 10 workdays of DOE concurrence. The SOC will be prepared in strict accordance with DOE standards, clearly and concisely describe the DOE's security concerns in the case, must be of the highest quality in format, style, content, and legally sufficient to present the DOE's case before a Hearing Officer. The contractor will be required to assist the DOE legal counsel and the Hearing Officer as required, and be prepared to testify in the Hearing.
Analyze Incident Reports (Excluding Positive Drug Test) and prepare the CES recommending the appropriate action(s).	Within 7 workdays of receipt in PSD Branch
Complete other actions as required by the DOE to ensure that a fully informed and correct adjudicative determination is made on an individual's eligibility for a DOE access authorization or continued eligibility for a DOE access authorization. These actions include, but are not limited to obtaining additional financial information, medical records, law enforcement records, court records, etc., and routinely require a completed CES for each action completed.	Follow-up required by the contractor personnel security specialists at least every two weeks from date the request is submitted. In cases involving substantial derogatory information that could result in AR, the contractor will follow-up on a weekly basis. The personnel security file (PSF) will be documented as appropriate to reflect that follow-up action is occurring as required.
Complete security reviews as appropriate for the Personnel Security Assurance Program (PSAP)/Human Reliability Programs (HRP) and prepare CES, if required.	Within 2 workdays of receipt, unless otherwise directed by DOE.
Clearance Management and Processing (4.1.2)	
Process Applicant case to the investigative agency	Within 10 workdays of receipt of a complete and approved clearance package from the requestor.
Process Reinvestigation case to the investigative agency	Within 5 workdays of receipt of a complete and approved clearance package from the requestor.
Process Investigation Reports	Within 2 workdays of receipt, complete data base entries, and process investigation reports and PSF to the appropriate PSD branch.
Process Clearance Reinstate Requests	Within 5 workdays of receipt, complete data base entries, process the PSF, and investigation reports, if appropriate, to the appropriate PSD branch.
Process Requests for Clearance Extensions and Transfers	Within 5 workdays of receipt.
Process requests for clearance downgrades.	Within 8 hours of receipt.
Process clearance continuations	Within 8 hours of receipt from the PSD Branch
Process Grant of clearance for applicants	Daily upon receipt from the PSD Branch.
Produce/Disseminate Daily Access Report	Daily.
Process discontinuance of investigation	Within 8 hours of receipt of request.

TABLE OF DELIVERABLES - PERSONNEL SECURITY DIVISION	
DELIVERABLE	TIMEFRAME/STANDARD
/reinvestigation	
Process clearance cancellations	Within 2 workdays of receipt of request.
Process clearance terminations	Within two workdays, however, CPCI will be updated the day the termination statement is received.
Process Incident Reports	Immediately upon receipt send the Incident Report and PSF to the appropriate PSD Branch Chief or Team Leader.
Process Fingerprint retakes	Within 8 hours of receipt of request.
Process Data Report on Spouse	Within 5 workdays of receipt.
Process Reciprocity Requests	Verify with other government agency within 5 workdays, and process any investigative reports and PSF to the appropriate PSD branch.
Process queries to investigative agencies on status of pending investigations	Daily, as required.
Process PIPS queries	Daily, as required
Process requests for File (PSF) transfers	Within 8 hours of request, mail via 405.
Process requests to combine files	Within 8 hours of request.
Prepare additional PSF volumes.	Within 2 workdays of request.
Duplication of PSF's and Destruction of duplicates	Daily, as required.
Process submission of name changes	Within 5 workdays of receipt
Process mail	Daily, as required. Administrative Review correspondence, responses to Congressional Inquiries, and all requests for overnight express mail (FedEx, USPS, etc.) will be processed immediately upon receipt.
Provide DOE clearance numbers	As requested.
Process facility code inquiries	As requested.
Data entry into PSD and DOE databases	As requested and required by PSD/DOE policies.
Mail Station (4.1.7)	
Maintain mail station with all required accountability.	Mail is due to addressees within 2 hours of receipt in mailroom. Mail will be sent out according to the Service Center schedule.

TABLE OF DELIVERABLES -- SECURITY PROGRAMS DIVISION	
DELIVERABLE	TIMEFRAME/STANDARD
Foreign Ownership, Control, or Influence Program (FOCI) (4.2.1)	
Provide a FOCI determination or request for additional information.	Within 30 calendar days.
Facility Clearances and Registration of Safeguards and Security Activities (4.2.2)	
Take Action to register facility Clearance.	Within 10 working days.
Resolution of Findings (4.2.3)	
As required.	As required.
Security Education Briefings and Awareness (4.2.4)	
As required.	As required.
Security Badges and Visitor Control (4.2.5)	
As required.	As required.
Survey and Self Assessment Support (4.2.6)	
Provide comprehensive knowledge of security discipline being reviewed.	Standard will be the ability to assess the implementation of a security discipline, and to determine a site's

TABLE OF DELIVERABLES -- SECURITY PROGRAMS DIVISION	
DELIVERABLE	TIMEFRAME/STANDARD
	capability for protecting information/assets.
Develop inspection plan for security discipline to be reviewed.	Due upon call from Team Leader. All background documentation must be reviewed no later than 10 days prior to the start of a survey.
Prepare draft report of survey conducted.	Survey report, after-action and lessons-learned reports are due to Team Leader prior to leaving the site surveyed. Report must be concise, accurate, and prepared in correct format.
Planning Assistance (4.2.7)	
Participate in management activities.	Due upon assignment.
Review Safeguards and Security Documents (4.2.8)	
Evaluate the review of safeguards and security documents.	Present (written or oral) results of evaluation. Due within one week of assignment.
Vulnerability Assessment and Risk Analysis (4.2.9)	
Provide VA and RA support as required by Service Center Support agreements with NNSA Sites Offices and HQ.	Due as requested or in accordance with the service support agreement.
Technical Security Support (4.2.10)	
Provide Technical Security support in the area of security systems.	Comprehensive knowledge of security system operations and administration. Daily, as required
Provide general support to TSCMOM, ISOM/DAA, PTSAA, and TEMPEST Program Manager.	Comprehensive knowledge of the technical security disciplines and their inter-relationships. Due upon assignment.
Safeguards and Security Program Review (4.2.11)	
Provide analysis (written or oral) of plans noted in the Statement of Work to the appropriate Federal oversight person.	Comprehensive knowledge of the security discipline described in the plan reviewed. Due upon assignment.
Information Management (4.2.12)	
Develop/maintain data base(s) that will track activities noted in the Statement of Work.	Due upon assignment.
General Technical Assistance (4.2.13)	
Develop/update viewgraphs, slide-show presentations, information papers.	Due upon assignment.
Safeguards and Security Special Security Projects (4.2.14)	
As assigned	Due upon assignment.
Correspondence (4.2.15)	
Develop clear, concise correspondence.	Due upon assignment.
Records Management (4.2.16)	
Establish/maintain a file system to enable access to all official Division records.	Due upon assignment.
Incidents of Security Concern (4.2.17)	
Receive notification of suspected incidents of security concerns. Prepare incident reports. Conduct inquiry. Prepare written security incident notification reports. Submit monthly reconciliation reports. Submit status of on going inquiry reports.	Categorize in accordance with DOE N473.1 within 1-8 hours. Daily as required in accordance with applicable DOE requirements/guidance.
Access Control (4.3.1)	
Control Limited Area entry and exit. Visually inspect badges.	Daily.
Emergency Responder Access (4.3.2)	
Facilitate and escort emergency response	As required.

TABLE OF DELIVERABLES -- SECURITY PROGRAMS DIVISION	
DELIVERABLE	TIMEFRAME/STANDARD
personnel and vehicles within the Limited Area.	
Issue and Account for Temporary Badges (4.3.3)	
Issue permanent and temporary badges to NNSA, DOE and DOE contractor personnel.	Daily, as required
Alarm Systems (4.3.4)	
Provide security system expertise as required by Service Center Support agreements with NNSA Sites Offices and HQ to support alarm system design, development, and implementation.	Standard will be the ability to assess/advise and report capability of system to protect security assets.
Monitor security systems. Identify, assess and respond to alarms. Monitor fire alarm system.	Daily, as required.
Detection/Assessment (4.3.5)	
FST provides Detection/Assessment as required by Service Center Support agreements with NNSA Sites Offices and HQ alarm system design, development, implementation, and assessment.	Per DOE Order Requirements and Service Center Agreements. Contractor Protective Force and technical support personnel support the Service Center.
Monitor alarm systems. Identify and respond to alarms. Monitor Fire alarm system.	Daily, as required.
Roving Patrols (4.3.6)	
Conduct interior and exterior patrols of NNSA Service Center facilities.	Daily
Inspections (4.3.7)	
Conduct inspection of hand-carried items. Conduct search/inspection of vehicles entering and exiting the Limited Area.	Daily, as required.
Classified Storage (4.3.8)	
Monitor combination storage and control. Ensure annual inventories are conducted on all accountable classified matter.	Daily, as required. Annually.
Flag Protocol (4.3.9)	
Perform the raising and lowering of the flag, per flag protocol.	Daily.
Key, Combination, and Lock Control (4.3.10)	
Annually, conduct the security key and lock inventory. Monitor the issuance of Security keys	Annually. Daily, as required.

TABLE OF DELIVERABLES -- CLASSIFICATION AND CONTROLLED INFORMATION DIVISION	
DELIVERABLE	TIMEFRAME/STANDARD
Guidance Development (4.4.1)	
Written comments on draft classification and UCNi guides. Written analysis and final documentation of declassification proposals and position papers.	Timeframe for delivery of finished product will be established by the Manager, CCID at the time of assignment and will be based on the scope and complexity of work. NOTE: All documentation referred to in this Table of Deliverables will be prepared to acceptable contemporary professional business standards, be technically correct, and conform to DOE/NNSA, Service Center, CCID, and classification program standards in style and content.
Training (4.4.2)	

TABLE OF DELIVERABLES -- CLASSIFICATION AND CONTROLLED INFORMATION DIVISION	
DELIVERABLE	TIMEFRAME/STANDARD
Prepare policy and technical written and/or computer-based curriculum for the purpose of training derivative classifiers and UCNI reviewing officials.	Timeframe for delivery of finished product will be established by the Manager, CCID at the time of assignment and will be based on the scope and complexity of work. The final training product will be in the form of class handouts and formal presentations.
Prepare final examinations and practical exercises for derivative classifiers and UCNI reviewing officials.	Timeframe for delivery of finished product will be established by the Manager, CCID at the time of assignment and will be based on the scope and complexity of work. Examinations and practical exercises will be of sufficient scope as to reinforce training and allow the student to demonstrate proficiency to the appointing authority that classification authority should be granted.
Teach policy and technical classes and proctor and grade examinations pertaining to classification and controlled information.	Classes must be succinct and delivered within the timeframe specified in the class agenda. Instructor must be well versed in all aspects of the curriculum to the extent that most student questions can be answered accurately and examples gained through experience can be provided.
Document Review (4.4.3)	
Provide formal classification determinations of any documents containing DOE equity and/or provide consultation and advice to clients needing assistance in reviewing documents. Documents may be in form of written text, photographs, film, data, or any other means of conveyance.	Timeframe for delivery of finished product will be established by the Manager, CCID at the time of assignment and will be based on the scope and complexity of work. The minimum standard for all reviews is identification of classification level, category, classification guide, and declassification instructions. When needed, some documents require portion marking or bracketing. Consultations normally require a written analysis.

6.0 Applicable Documents

The work performed supports requirements derived from the following federal laws, codes, and DOE orders, manuals, and regulations:

Executive Orders (EO)(Includes all applicable amendments):

- E.O. 10450 – Security Requirements For Government Employees
- E.O. 10865 – Safeguarding Classified Information Within Industry
- E.O. 12333 – United States Intelligence Activities
- E.O. 12564 – Drug-Free Federal Workplace;
- E.O. 12829 – National Industrial Security Program
- E.O. 12968 – Access to Classified Information
- E.O. 12958 – Classified National Security Information

Code of Federal Regulations:

- Title 5, Code of Federal Regulations (CFR):
 - Part 732 – National Security Positions
 - Part 736 – Personnel Investigations

- Title 10, Code of Federal Regulations (CFR):
 - Part 707 – Workplace Substance Abuse Programs
 - Part 709 – Polygraph Examination Regulation

Part 710 (Subparts A and B) – Criteria and Procedures for Determining Eligibility for Access to Classified matter or Special Nuclear Material
Part 711 – Personnel Assurance Program
Part 712 (Proposed Final Rule) – Human Reliability (When published in the Federal Register, this final rule revokes 10 CFR Part 710, Subpart B, and 10 CFR Part 711)
Part 725 – Permits for Access to Restricted Data
Part 1008 – Records Maintained on Individuals (Privacy Act)
Part 1016 – Safeguarding of Restricted Data
Part 1017 – Identification and Protection of Unclassified Controlled Nuclear Information
Part 1045 – Nuclear Classification and Declassification

Title 48 Code of Federal Regulations (CFR):
Part 970.2201 – Basic Labor Policies

United States Code (USC)(Includes all applicable amendments):
Title 5 USC, 552a – Privacy Act of 1974 (Public Law 93579)
Title 21 USC, 802 – Controlled Substances Act of 1970
Title 42 USC, et. seq. – Atomic Energy Act of 1954

Director of Central Intelligence Directive (DCID) No. 6/4 – Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information

Department of Defense – National Industrial Security Program Operating Manual (DoD 5220.22-M) and Supplement

DOE Notices/Orders/Manuals:

DOE N 142.1 Unclassified Visits and Foreign Assignments (DOE N 251.47, dated 08/14/02, extends this directive until 05/14/03)
DOE O 200.1 – Information Management Program
DOE O 232.1A – Occurrence Reporting and Processing of Operations Information
DOE O 452.4A – Security and Control of Nuclear Explosives and Nuclear Weapons
DOE O 461.1 – Packaging and Transfer or Transportation of Materials of National Security Interest
DOE O 470.1 Chg 1 – Safeguards and Security Program (DOE N 251.47, dated 08/14/02, extends this directive until 05/14/03)(Will be replaced by DOE O 470.1A presently in draft)
DOE O 471.1A – Identification and Protection of Unclassified Controlled Nuclear Information
DOE M 471.1-1 Chg1 – Identification and Protection of Unclassified Controlled Nuclear Information Manual
DOE O 471.2A – Information Security Program (DOE N 251.47, dated 08/14/02, extends this directive until 05/14/03)(Will be replaced by DOE 471.2B presently in draft)
DOE M 471.2-1C – Classified Matter Protection And Control Manual
DOE M 472.1-1B – Personnel Security Program Manual
DOE O 472.1C – Personnel Security Activities
DOE M 475.1-1A – Identifying Classified Information
DOE O 481.1B – Work For Others (Non-Department of Energy Funded Work)
DOE O 1450.4 – Consensual Listening-in to or Recording Telephone/Radio Conversations
DOE O 5610.13 – Joint Department of Energy/Department of Defense Nuclear Weapon System Safety, Security, and Control Activities
DOE O 5639.8A – Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities
DOE O 5660.1B – Management of Nuclear Materials
DOE O 5670.1A – Management and Control of Foreign Intelligence
DOE O 5670.3 – Counterintelligence Program