Attachment 1
Contract No. HR0011-12-C-0024

April 8, 2011

STATEMENT OF WORK

CONTRACTOR SUPPORT SERVICES FOR THE

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA),

SUPPORT SERVICES OFFICE (SSO),

SECURITY AND INTELLIGENCE DIRECTORATE (SID)

TABLE OF CONTENTS

SECTION 1 - DESCRIPTION OF SERVICES

1.0 OBJECTIVE: The objective of the Security Support Services Contract is to provide the Defense Advanced Research Projects Agency (DARPA) Support Services Office's (SSO), Security and Intelligence Directorate (SID) with a professional capability to augment the government staff and to execute the inherently non-governmental functions central to SID's responsibilities in preserving and enhancing National Security objectives through active and integrated security operations, processes, mechanisms and management. This support must provide multi-disciplinary security execution across the life of a program; including analytical/program protection support, flexibility and responsiveness to dynamic DARPA technology protection challenges. The government requires full-time support in a number of security disciplines. Individuals supporting these tasks may be required to perform a combination of the functions described in this Statement of Work (SOW). These security services are required for programs at all protection levels (unclassified, collaterally classified, Sensitive Compartmented Information (SCI), and Special Access Programs (SAP)).

1.1 DARPA's mission is to maintain the technological superiority of the U.S. military and prevent technological surprise from harming our national security by sponsoring revolutionary, high payoff research. DARPA's mission is also to create technological surprise for our adversaries. This implies one imperative – radical innovation for national security. DARPA's business philosophy is to bring in expert, entrepreneurial program managers (PM) for the technical programs, empower them, protect them from red tape, and quickly make decisions about starting, continuing or stopping research projects. The DARPA technical staff organization is dynamic and changes as the projected requirements of the Department of Defense, the state-of-the-art of technology development, and adversarial threats to the United States evolve.

1.2 SSO's mission is to provide a knowledgeable, lean, and adaptable staff exemplifying world-class customer service in support of the DARPA mission; supplying the tools, facilities, expertise, administrative services, and secure environment that enables the technical and administrative offices to perform their jobs more quickly, with greater ease and economy.

1.3. SID's mission is to develop, manage and implement programs that facilitate the secure and successful accomplishment of DARPA' s mission, while protecting DARPA technical and administrative personnel, information, property, and ensuring business continuity. SID supports this mission by planning, executing, and directing multi-disciplined security, emergency management, and international cooperation at DARPA. SID also formulates and implements security policy and procedures at DARPA and represents DARPA on security matters with external organizations.

1.4 SID's objectives are to provide world-class service to each of our customers; to establish credible Agency policy and procedures; to be responsive to technical program needs in a timely manner; to represent DARPA's interests in National Security Forums; and above all, to protect our people and information. SID's challenge is to accomplish the mission and objectives while enabling the DARPA business philosophy. The SID requires a contractor that will provide a high-quality professional security staff that believes in teamwork and customer service and that will partner with SID to accomplish these objectives using initiative, innovativeness, and cost consciousness. In fulfilling this responsibility, SID requires a support services contractor experienced in developing, implementing and maintaining programs that facilitate the secure and successful accomplishment of its mission while protecting DARPA personnel, information, property, and maintaining business continuity consistent with DARPA's Mission, Public Law, National Policy, and Department of Defense Directives and Regulations. Just as the DARPA technical offices (Figure 1) dynamically change to meet the Agency's obligation to providing world-class technology vision and leadership, the SID organization must remain flexible to provide seamless security support to the technical offices and their industry and academia researchers and capability builders. The SID organization chart in Figure 2, on the following page, reflects the current structure to support the Agency's needs.

1.5 Paramount to SID's support to the DARPA vision and mission is the concept that in every security related action or document approved by the DARPA staff, the action is accomplished, or the document approved, on behalf of the DARPA Director. Therefore, the contractor will ensure that the contents and formats (including spelling and grammar) fully comply with DoD, governmental, and accepted English standards. The contractor staff in support of SID is expected to fully comply with this concept.

2.0 General and specific tasks for all positions on this contract are provided in Section 2.

2.1 Deliverables which may require the efforts of multiple positions are identified in Section 3.

2.2 Executive Orders, United State Code, Department of State, Director National Intelligence, Defense Intelligence Agency and Eos, other Agency Instructions, Directives, Memos, Guides, Forms, etc are applicable to the duties and tasks articulated in this Statement of Work and are provided on page 46. Current and updated versions shall be used in lieu of outdated copies.

2.3 Common Acronyms and Abbreviations associated with the duties and tasks are provided on page 50.

2.4 The Director, SID, from time-to-time task-organizes government staff with contractor support to address issues that arise which are either outside the responsibility of individual SID offices, or which encompass the responsibilities of multiple ones. These tasks whether assigned to a single individual or to a group take the form of a Special Project, Study, Assessment or Analysis, (either government only, or mixed government/contractor) and normally require extensive knowledge of security disciplines and an understanding of DARPA missions, functions, and organization and may be of a time-sensitive nature.

3.0 On the following page, Figure 1 shows the basic organization of DARPA and the relationship of the SSO and the SID to the Technical Offices (all other administrative and support offices have been left out for brevity). Figure 2 shows the basic functional organization of SID.

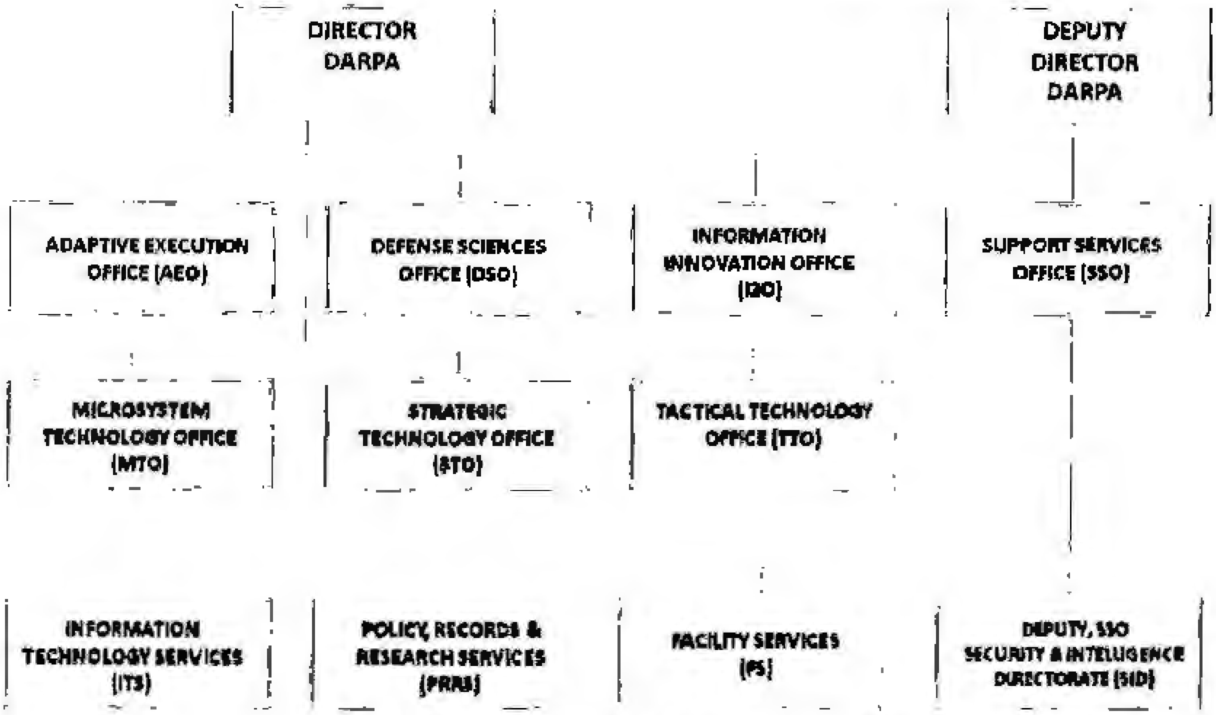
DIRECTOR
DARPA
DEPUTY
DIRECTOR
DARPA
ADAPTIVE EXECUTION OFFICE (AEO)
DEFENSE SCIENCES OFFICE (DSO)
INFORMATION INNOVATION OFFICE (I2O)
SUPPORT SERVICES OFFICE (SSO)
MICROSYSTEM TECHNOLOGY OFFICE (MTO)
STRATEGIC TECHNOLOGY OFFICE (STO)
TACTICAL TECHNOLOGY OFFICE (TTO)
INFORMATION TECHNOLOGY SERVICES (ITS)
POLICY, RECORDS & RESEARCH SERVICES (PRRS)
FACILITY SERVICES (FS)
DEPUTY, SSO
SECURITY & INTELLIGENCE DIRECTORATE (SID)

Figure 1. BASIC DARPA ORGANIZATION

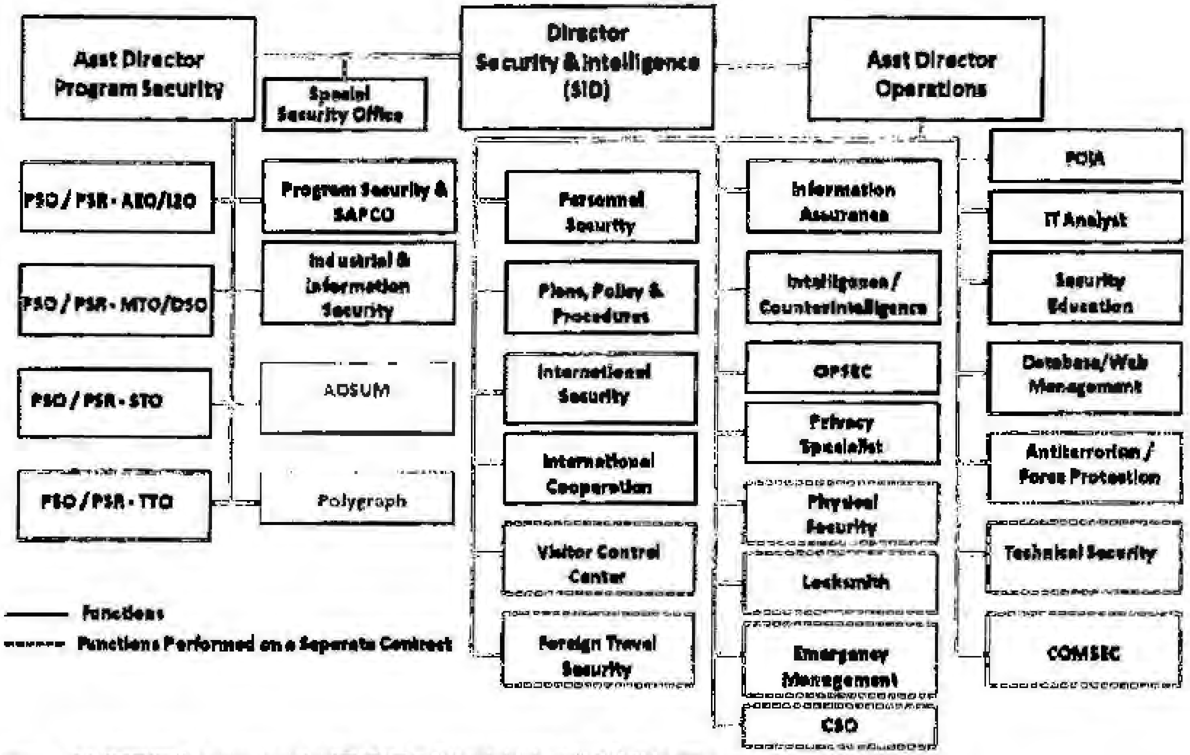

Figure 2. SECURITY & INTELLIGENCE DIRECTORATE ORGANIZATION

SECTION 2 - SECURITY POSITION DESCRIPTION/REQUIREMENTS

OVERVIEW: Each position on this contract requires the ability to work independently, with little to no supervision. Flexibility and adaptability to change and innovation are imperative in supporting DARPA. Each position requires these intangibles as well as demonstrated technical competence. The DARPA mission model is based upon a consistently changing and evolving leadership and PM base. Each position has its core functional requirements listed. However, in addition to the position-specific requirements, all positions on this contract will be required and expected to incorporate the following base-line professional business functions in their specific job descriptions:

a) Attend meetings (either out-of-area or locally) and create meeting summaries or trip reports;

b) Prepare and submit Meeting Minutes on an as-required basis;

c) Prepare/present briefings, incorporating graphics (if appropriate) for/to SID and DARPA leaders;

d) Prepare various, numerous, security forms associated with their duties;

e) Assist in entry control and perform escort duties for visitors;

f) Answer telephones and other modes of administrative communications in the performance of duties;

g) Perform self-inspections; identify security discrepancies, and report security incidents;

h) Perform, or support, security inspections; identify security discrepancies; prepare reports;

i) Perform courier duties within the continental United States (CONUS);

j) Perform user-level security administrator and information security responsibilities, as required and in compliance with US Codes, Executive Orders, DoD, and DARPA policy in addition to their core duties;

k) Perform objective reviews on all documentation encountered during performance of duties;

l) Update security databases (e.g., SIMS, SILVERADO, CAST, JPAS, suspense tracking, personnel files, facility, etc), as required, in the performance of assigned duties;

m) In conjunction with other contract Subject Matter Experts (SME) perform QC reviews of all documentation provided to SID staff. These QC reviews will encompass technical content, spelling/grammar, and delivery format (including required reference/back-up materials) to ensure the highest professional standards are applied;

n) Possess and demonstrate excellent written and oral communication skills.

Security professionals assigned to positions under the SOW are expected perform the tasks germane to their assignments. There are detailed descriptions of the positions associated with the services required under each job description. In addition to those specific tasks each of the security professionals performing under the contract, within their area of responsibility, are expected to apply the policies, guidance, and instructions appropriate to their programs, and in concert with the stakeholders involved, to:

1) Identify their duty to protect. This includes: (1) identifying and/or assisting in the identification of information and/or assets requiring protection, (2) identifying, interpreting, and analyzing protection requirements critical to protecting the identified information and/or assets, (3) specifying laws, standards, regulations, policies, and requirements that govern the identification and protection of the information and/or assets, and (4) determining how those laws, standards, regulations, policies, and requirements need to be applied to identify information and/or assets requiring protection.

2) Review, respond, and solve security-related concerns, issues, and problems that fall within one's area of responsibility and provide stakeholders the technical assistance and guidance they need to effectively perform their security roles and responsibilities.

3) Specify and provide direction on the laws, standards, regulations, policies, and requirements that:

    a) Identify roles and responsibilities associated with the classification decision process (original and derivative). Determine security practitioner's roles and responsibilities in the classification decision process and enact actions, under one's own area of responsibility, that facilitate the effective execution of the classification decision process.

    b) Are applicable to security clearance processes (e.g., personnel security clearance, facility security clearance), and determine how those laws, standards, regulations, policies, and requirements need to be applied in one's area of responsibility and enact actions that result in the accurate determination of an entity's eligibility for a security clearance.

    c) Call for the application of risk assessment processes and determine how those laws, standards, regulations, policies, and requirements need to be applied in one's area of responsibility and enact actions that result in the systematic identification, characterization, and evaluation of risks.

    d) Are applicable to the application of countermeasures to manage risks to identified information and/or assets requiring protection. Identify potential countermeasures that can be applied to reduce identified vulnerabilities and enact actions that result in the systematic evaluation of costs and benefits associated with each identified countermeasure. Prioritize countermeasures to support risk management decisions, and support the implementation and/or implement specified and/or selected countermeasures to manage risks to identified information and/or assets requiring protection.

e) Are applicable to the development, implementation, and evaluation of security awareness, education, and training programs. Determine how those laws, standards, regulations, policies, and requirements need to be applied in one's area of responsibility and enact actions that result in the execution of effective security awareness, training, and education requirements.

f) Are applicable to the detection, identification, and handling of security incidents. Determine how those laws, standards, regulations, policies, and requirements need to be applied in one's area of responsibility and enact actions that facilitate the effective handling of security incidents.

g) Are applicable to the need to evaluate security program effectiveness. Determine how those laws, standards, regulations, policies, and requirements need to be applied in one's area of responsibility, to enact actions that facilitate the comprehensive and targeted evaluation of a program's effectiveness (including the identification, characterization, and communication of lessons-learned) and identify, coordinate, and execute program modifications and improvements based on evaluation results.

h) Are applicable to the development and generation of plans for protecting information and/or assets. Determine how those laws, standards, regulations, policies, and requirements need to be applied in one's area of responsibility and enact actions, based on the application of sound risk management planning, that result in the development, documentation, and coordination of plans for protecting information and/or assets.

4) Appropriately identify, coordinate, and/or manage resources necessary to successfully pursue security mission and/or roles and responsibilities.

1. <u>PROGRAM MANAGEMENT TEAM:</u>

DARPA requires a lean management structure that employs qualified personnel and allows the personnel to perform their duties without unnecessary supervision or filtering. The contractor will provide a construct that retains and incentivizes new and existing employees given the nature of the competitive market which exists in the national capital region. DARPA is a dynamic work environment and Management will need to respond rapidly and with directed purpose. The contractor on-site management team will be empowered to make responsive employee hiring, counseling and removal decisions, as well as sub-contract and consultant actions. The on-site management team will have the full authority to commit the company to all operational functions in support of the contract and to represent and act for, and in the name of, the company in all contract matters relative to the execution of this contract. While there are descriptions and qualifications of the positions associated with the services required on this contract detailed within the RFP, for clarity the company's management team is responsible for the overall execution of all contract requirements. In addition the government has not mandated the management and supervisory structure of the proposed contract organization. The contractor should propose the necessary management team; to include supervisors/leads that it envisions are necessary to execute the requirements.

2. PROGRAM SECURITY REPRESENTATIVES:

Program security representative (PSR) support provides life-cycle development and protection for research, development, test & evaluation/science & technology (RDT&E/S&T) programs at DARPA. PSRs provide embedded support to the various DARPA Technical Offices. The PSR's take direction from government PSO's and utilizing their omnibus security discipline expertise provide services to program managers. Physical security expertise and the associated responsibilities are inherent in the PSR tool-kit in assuring appropriate security infrastructure and practices are incorporated at DARPA program performer locations.

2.1 The Contractor shall provide program security support with personnel referred to as PSRs to work closely with government Program Security Officers (PSO). The security scope of the programs to be worked on by the PSR will range from Unclassified through TOP SECRET and include SAP and SCI compartments. The PSR is embedded into one or more DARPA Technology Offices. The primary functions of the PSR shall be to provide security augmentation support to the PSOs and the DARPA technical office PMs and program SETA staff in determining, interpreting, and applying security requirements applicable to assigned technical office programs. PSRs are expected to be familiar with DARPA policies and procedures as well as the programs to which they are assigned. The PSR shall use initiative, innovation, and risk management techniques to apply program security requirements in such a manner that the programs can be executed in a cost-effective, schedule compliant manner, with minimum risk to information, personnel, and business continuity. The PSR shall apply their security background knowledge to aid the PSO, PM and SETAs in identifying and managing risks associated with the programs. The PSR's duties will include, but are not limited to: working with the DARPA SID Program Security Office (SAPCO for SAPs) to establish security compartments, as required, develop security classification guides (SCG); write and coordinate Department of Defense Contract Security Classification Specification's (DD Form 254); and, in cooperation with DARPA program performer security staffs: the selection, interpretation, and implementation of information, industrial, physical, and personnel security concepts applicable to the DARPA programs; recommend the adoption of appropriate OPSEC measures, information technology concepts/configurations, International Traffic in Arms Regulation (ITAR), and Export Administration Regulations (EAR) procedures. PSRs are expected to support multiple programs, if required. When incidents occur, conduct containment actions and develop a recovery strategy and procedures to prevent recurrence.

2.2 In order to be able to understand the challenges and effectively interface with the PMs, their SETAs, admin staff, and performer staffs, PSRs are required to have or to develop rudimentary background knowledge of the technologies and proposed applications involved in the programs for which they will provide informed security support and recommendations.

2.3 Typical duties of a PSR include, but are not limited to:

1) Using their knowledge of the various security disciplines (e.g. physical, information, personnel) determine, apply, and monitor appropriate security

requirements and tasks relative to the specific technology programs to be protected; prepare and present suggestions for improvement;

2) Research and recommend/develop long and short range security strategies and tactics for new or established programs, or changes in program direction;

3) Develop DD 254's, ensure security requirements are spelled out clearly on the initial contracts and required security documentation is provided to the contractor;

4) Establish and sustain personnel access actions, to include personnel Tier reviews, document control, and other database maintenance, applicable to the specific areas (collateral, SCI, or SAP);

5) Apply a working knowledge of Executive Order 12968 and 13526;

6) In cooperation with other SID offices, assist in the investigations/inquiries of security violations and Practices Dangerous to Security (PDS) conducted in accordance with DoD 5105.21-M-1;

7) Assist in determining program access requirements/process personnel for access;

8) Indoctrinate newly assigned personnel and de-brief departing personnel;

9) Support the creation, processing, coordination, and approval of physical security and Automated Information Systems (AIS) accreditations, as well as entering such information and including individuals, programs, contracts and performers, if required, into appropriate information security management systems, i.e.,

   a. DARPA ISMS;
   b. JPAS;
   c. CASTS;
   d. SCATTERED CASTLES; and,
   e. SILVERADO.

10) Provide program courier services, as required;

11) Plan, coordinate, and manage security support for test activities, including equipment/material/personnel transportation;

12) Develop, write, review, coordinate, and execute security documentation, i.e.,

   a) SCGs; provide guidance and assistance for all security levels, including collateral, SAP and SCI;
   b) Program Protection Plans;
   c) Public Affairs / Perception Management Plans;
   d) Exposure Contingency Plans;
   e) System accreditation plans;
   f) Test Security Plans;
   g) System Security Plans;
   h) Detailed trip & meeting reports;
   i) Technology Transfer and Program Transition Plans;
   j) Standard Operating Procedures;
   k) Memorandums of Agreement and Understanding;
   l) Transportation Plans;
   m) OCONUS Deployment Plans;
   n) Managed Access Plans;
   o) Treaty Compliance Plans;

p) Dismantle, Disposition & Demilitarization Plans;

q) Determine Security Architecture

13) Plan, coordinate, provide, and manage security support for meetings;

14) Actively support Agency Program Security Reviews and Self-Inspection Programs;

15) Manage security incident investigations and reporting;

16) Develop and support intelligence requests to obtain state-of-the-world, rest-of-the-world, or state-of-the-art technology/capability status;

17) Perform OPSEC analysis and provide other OPSEC support, to include identification of critical program information (CPI), collecting and analyzing threat data, developing, and coordinating program OPSEC plans;

18) Participate in program close-outs reviews at program sites;

19) Prepare plans and provide on-site security for transportation of equipment and systems for program tests;

20) Travel to, and attend/conduct, briefings and plans for system/facility security changes;

21) Coordinate AIS testing with the Designated Approval Authorities, to include certification and accreditation requirements; and,

22) Attend program reviews, i.e., preliminary design reviews (PDR), critical design reviews (CDR), and integrated product team (IPT) reviews, to ensure changes to system baselines don't negatively affect security and initiate actions to add mitigation where necessary.

23) Provide the proper protection for privacy information.

3. SECURITY ASSISTANTS:

Security Assistants perform a vital administrative security support function by providing direct access control to secure areas; ensuring consistent and efficient processing and distribution of security-related documentation; the maintenance and monitoring of calendar schedules; monitoring suspense items; conducting document quality reviews; scheduling presentation of special taskings; accepting deliveries of classified and unclassified materials (reports, presentations, etc); and, the management and administration of the SID-related portion of the Defense Travel Service database. SID has embedded Security Assistants in key positions throughout the Directorate.

3.1 The contractor shall provide administrative support across all functional areas to assure the maintenance of records and files, the preparation and distribution of mail, correspondence, reports, and other documents, and the maintenance of a suspense date file. These efforts include the development, review, analysis, and preparation of ad hoc reports, spreadsheets, charts, graphs, and narratives.

3.2 The contractor shall perform the following duties related to security assistance:

1) Plan, conduct, analyze, evaluate, and report security issues;
2) Generate and maintain databases that reflect receipt, storage, inventory and disposition of information; to include data entry, updates, and generation of reports;
3) Conduct audits/inventories to ensure proper control and/or accountability;
4) Assist in the inspection, inventory, logging, storage, and internal distribution of information received;
5) Maintain and document personnel security programs, to include databases for all collateral, SAP, and SCI personnel;
6) Review and analyze requests for information;
7) Assist in the preparation and execution of security directives and security guides;
8) Assist in reviewing customer security regulations and procedures and determine methods of implementation;
9) Participate in security reviews, security incident investigations and preliminary inquiries, and surveys, as required;
10) Assist with implementing the Security Education Awareness training program;
11) Develop security education bulletins, directives, security plans, procedures and controls as required;
12) Prepare and protect security files, records and other information;
13) Perform entry, exit, visit processing, and escorting;
14) Conduct end-of-day security checks and performing other security administrative functions as requested; and,
15) Conduct indoctrination and debriefings, as required.

3.3 The contractor shall perform the following duties related to general administration:

1) Serves as the principal point of contact for the Director SID, Assistant Director Operations, and Assistant Director Program Security;
2) Provide day-to-day access control management of supported facilities;
3) Maintain supported facilities and conference rooms;
4) Assist customers in completing meeting checklist forms;
5) Complete and file, in and/out processing checklists on all personnel;
6) Coordinate with other security offices, organizations, and personnel in support of mission requirements;
7) Coordination of conferences and meetings at local and other supported facilities;
8) Perform files management functions for office to which assigned;
9) Perform calendar management functions for assigned offices;
10) The contractor shall perform the following duties related to documents and media:

a) Manage and update Document Control Center (DCC) procedures, and conduct DCC training

b) Handle incoming and outgoing faxes, and document scanning for faxing

c) Prepare packages & documentation for transmission via appropriate channels.

d) Pick-up and deliver selected items to local US Postal Service (USPS)

e) Receive and account for all USPS registered and Express mail

f) Maintain document control/accountability databases

g) Maintain magnetic and optical media, and perform annual inventories and reconciliation

h) Virus check media

i) Document and perform proper disposal of documents and magnetic media

j) Perform document archiving

k) Internal distribution of all office material

l) Update magnetic media used to backup all systems

m) Conduct secure Electronic Data Transfer service (EDTS) operations

n) Perform copying and other document/media reproduction

o) Perform self-inspections, identify security discrepancies, and report security incidents

11) Assist DARPA staff in completing personnel security related documents and ensuring that personnel are notified in advance when they are due for reinvestigation, and;

12) Provide the proper protection for privacy information.

13) Plan, support, and accomplish office automation support work using multiple automated programs and software;

14) Develop and/or maintain administrative methods and procedures for an office;

15) Schedule and track the calendar for appointments, meetings and travel, to include use of the Defense Travel Service System (DTS);

16) Maintain and follow-up on suspense records for correspondence or action items;

17) Prepare a wide variety of recurring and nonrecurring correspondence, reports and other documents;

18) Apply knowledge of management principles, organizational theory, and techniques of analysis and evaluation in order to conduct studies of automated clerical work processes;

19) Establish, update, and develop inclusive administrative office procedures and methods;

20) Gathering information, verify facts, and assemble background materials, reference material, and reports for executive level officials for meetings and conferences;

21) Proof reading, QC, DoD and DARPA Format compliance, task tracking and disposition;

22) Establish and manage workflow staffing process;

23) Assist with new employee processing and indoctrinations to the respective SID offices;

24) Support the coordination of executive correspondence/products to resolve issues/obtain concurrences for planned actions; receive guidance on choosing appropriate courses of policy/programmatic or administrative actions; and,

25) Make recommendations for the best use of present resources and assist with planning for future resource needs, estimating both short and long-range personnel, budgetary, space, and equipment needs, and implements new resources.

4. SECURITY ASSISTANTS (SA) IN THE SPECIAL SECURITY OFFICE (SSO)

The function of the DARPA SSO is to provide a reliable and secure means to receive and disseminate Sensitive Compartmented Information (SCI) to authorized recipients. The SSO has overall security responsibility of all SCI Facilities (SCIFs) and Temporary Secure Work Areas (TSWA) within DARPA. The SSO assists DARPA Technical Offices in the development, implementation, document marking, safeguarding, procedures for use, and the exercise of classification and declassification issues for SCI involved in DARPA programs.

4.1 Contractor SA in the SSO shall perform the following functions in supporting the DARPA SSO:

1) Maintain applicable SCI directives, regulations, manuals, and guidelines to adequately discharge SSO duties and responsibilities;

2) Maintain listings of available SCI electrical and hard copy products;

3) Validate product request requirements, and ensure dissemination to authorized users;

4) Conduct SCI security briefings, indoctrinations, and debriefings;

5) Interface with SCI telecommunications centers, Automated Data Processing (ADP) facilities, computer centers, and similar offices to ensure SCI security;

6) Working with the SID Security Education, Training, and Awareness Office, develop and provide input for, and assist in conducting, a continuing SCI security education training and awareness program to ensure that all SCI-indoctrinated individuals are kept apprised of the requirements and guidelines for protecting SCI;

7) Ensure appropriate accreditation documentation is available for each SCIF and communications/automated information systems under DARPA's security cognizance;

8) Produce, review, and manage emergency plans for DARPA SCIFs, ensuring that these plans are in concert with Agency emergency planning actions;

9) In coordination with SID Intelligence/Counterintelligence Office, constantly evaluate SCI risks associated with DARPA facilities and programs and recommend appropriate countermeasures to mitigate them;

10) Create SOPs for DARPA SSO operations and review and provide recommendations, as appropriate, for DARPA program-specific SOPs involving the use or transport of SCI materials;

11) In cooperation with other SID offices, assist in the investigations/inquiries of security violations and Practices Dangerous to Security (PDS) conducted in accordance with DoD 5105.21-M-1;

5. SECURITY ASSISTANTS PERFORMING PERSONNEL SECURITY TIER II ADJUDICATOR DUTIES

5.1 The contractor shall perform TIER II SAP Access Eligibility Determination reviews, in accordance with DoD 5220.22-M-Supp 1, JFAN 6/4, and relevant DARPA/Service MOAs, to support DARPA's SAPs.

5.2 The following are functional duty areas for the DARPA TIER II Reviewer:

1) Develop, review, and update as required: TIER 1 and TIER II office policies and procedures;

2) Determine, or initiate the process for determining, a candidate's access eligibility;

3) Perform TIER I and TIER II SAP access eligibility determinations;

4) Input, as appropriate, TIER I & II access eligibility determination results into relevant database(s) ;

5) Review and process requests for interim SCI eligibility;

6) Monitor and track personnel security actions until complete;

7) Respond within two (2) working days to incoming eligibility determination requests and reports;

8) Review, and remain current, on the personnel security standards appropriate to the classification level of the programs for which access is being requested;

9) Prepare request for waiver and/or exception documentation and initiate staffing for approval;

10) Coordinate access approval or denial process with appropriate access approval authority;

11) Prepare documentation, as required to notify appropriate personnel of access approval or denial and staff or DARPA approval;

12) Conduct indoctrination briefings and processing of relevant documentation (e.g., SAP indoctrination agreement, nondisclosure agreements, polygraph agreement);

13) Update program access lists or roster in appropriate database(s) following indoctrination;

14) Coordinate the DARPA Polygraph schedule with the DARPA Polygrapher; and,

15) Provide advice to the DARPA SAPCO relating to the access eligibility review process and guidelines regarding TIER III issues, including the procedures to be followed in the appeal processes.

16) Provide the proper protection for privacy information.

6. PERSONNEL SECURITY SPECIALIST

SID manages a comprehensive personnel security program. This program includes efficiently and effectively processing DARPA employees for security clearances and access to both facilities and information. The program encompasses the collection and protection of personal history data, the review of that data to ensure its completeness, and the support and coordination for initial, periodic reinvestigations, special investigations, continued eligibility reviews, and adjudications by other agencies. The DARPA Personnel Security program ensures that all personnel meet the standards mandated by DoD Regulation 5200.2 to obtain and maintain a personnel security clearance and, if appropriate, accesses to SAP and SCI programs. The contractor shall support the DARPA SID in initiating appropriate investigative and administrative actions needed to ensure that DARPA and selected contractor personnel are efficiently and effectively processed for their security clearances and appropriate compartmented accesses.

6.1 The contractor shall perform the following tasks related to Personnel Security:

1) The collection and protection of personal history and privacy data; the determination, in conjunction with other DARPA entities, of position sensitivity levels;

2) Reviewing an individual's background information prior to final adjudication submission. This includes determining:

    a. The suitability of personnel for clearances and processing personnel for personnel security clearances by the collection of personal history data;

    b. The review of the information collected, the coordination of appropriate background investigations with appropriate agencies and the maintenance of personnel security files;

    c. The review of completed case files and Personnel Security Questionnaires (PSQ's);

3) Update appropriate personnel database(s), handle phone inquiries, and protect the dissemination of adverse information reports;

4) Compose, analyze, edit, QC , transmit, and track security requests; input data into appropriate personnel database(s);

5) Research and verify data in security databases for DARPA staff;

6) Conduct liaison with Central Adjudication Facilities, DoD, and Intelligence Community (IC) agencies to coordinate clearance issues;

7) Update account authorizations for the appropriate personnel database(s);

8) Provide personnel security guidance to PSRs and other individuals in the DARPA technical offices who have personnel security responsibilities, including DARPA performer organizations having questions relating to DARPA's involvement in providing personnel security support for Agency efforts;

9) Assist in training new SID and DARPA personnel on procedures involving personnel security issues; and,

10) Review security documents, draft, and initiate staffing of waiver request documentation to appropriate security authorities.

7. INFORMATION ASSURANCE SPECIALIST

IA encompasses, but is not limited to, the entire spectrum of Network Administration, Certification and Accreditation, Network Defense, and Enterprise establishment, management, and oversight. The DARPA systems to be protected include systems that process and store information from the unclassified (including controlled unclassified information) up to the Top Secret level, including SCI and SAP compartments operating on IT systems with protection levels 1-5. The contractor shall review and perform the IA tasks necessary to ensure that the existing DARPA IA program meets National and DoD Information Assurance standards and continues to protect and defend DARPA information and information systems by ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of the systems. The contractor shall provide for restoration of information systems by incorporating protection, detection, recognition, and reaction capabilities. The DARPA systems to be protected include systems that process and store information at the unclassified, collateral, SCI and SAP levels.

7.1 Information Assurance personnel duties shall include, but are not limited to the following:

1) Certification and Accreditation Activities in accordance with DoD Instruction 8510.01, DCID 6/3, and NISPOM Chapter 8.

2) Analysis of Threats and Vulnerabilities and Risk Mitigation and Acceptance;

3) Examination of computer and associated equipment;

4) Reviewing and recommending changes or amplification of policy, procedures, and strategy development;

5) Ensuring that system security requirements are addressed during all phases of DARPA program life cycles (concept development, Request for Information (RFI), Request for Proposal (RFP) or Broad Agency Announcement (BAA), Proposal, Selection, Award, Closeout, Transition, etc.). This includes coordinating all technical security issues outside of area of expertise or responsibility with appropriate SMCs SME;

6) Monitor, as necessary, activities of DARPA and selected performer automated IS, providing advice and assistance, as required;

7) Develop and review Automated Information System Security Plan and/or System Security Authorization Agreement (SSAA);

8) Evaluate IA products and provide written recommendations as to their usefulness and/or adoption for the DARPA IA mission;

9) Develop and implement Red Team Plans and activities, as directed;

10) Develop, implement and evaluate, as directed, DARPA information system security program policy incorporating special emphasis on integration of existing SAP network infrastructures;

11) Establish, schedule, and perform network security analysis for DARPA systems; these activities shall be based on established certification and accreditation processes; advise DARPA SID on IT certification and accreditation issues revealed;

12) Perform IA risk assessments and provide recommendations to SID;

13) Advise DARPA PMs and their SETA staffs on security testing methodologies and processes;

14) Evaluate certification documentation and provide written recommendations for accreditation to government PMs;

15) Periodically review system security to accommodate changes to policy or technology;

16) Evaluate IT vulnerabilities to assess whether additional safeguards are prudent; ensure that certification, as appropriate, is accomplished for each information system;

17) Develop and maintain formal, written, Information Systems Security Program Standard Operating Procedures (SOP);

18) Ensure that all appropriate SOPs are readily available to DARPA performers assigned to IA tasks;

19) Ensure that all Information System Security Officers (ISSO), network administrators, and other Automated Information Security (AIS) personnel, to include DARPA performers performing these functions, receive the necessary, and required, technical and security training to carry out their duties;

20) Ensure development and implementation of an information security education, training, and awareness program, to include attending, monitoring, and presenting local AIS security training;

21) Develop, review, endorse, and recommend action by the designated approval authority (DAA) of system certification documentation;

22) Ensure approved procedures are in place for transfer, release, or disposal of automated information system equipment or products;

23) Conduct certification tests that include verification that the features and assurances are functional and support PL1 – PL5 accreditation, as needed;

24) Maintain a repository for all system certification/accreditation documentation and modifications;

25) Coordinate AIS security inspections, tests, and reviews;

26) Prepare policies and procedures for responding to security incidents, and for investigating and reporting security violations and incidents;

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

28) Ensure that security testing and evaluations are completed and documented;

29) Evaluate vulnerabilities to ascertain whether additional safeguards are needed;

30) Assess changes in the system, its environment, and operational needs that could affect the accreditation;

31) Ensure that certification is accomplished on each AIS;

32) Review AIS test plans;

33) Conduct periodic testing of the security posture of the AIS;

34) Research, write, and review additions, modifications, deletions to existing AIS SSP's including configuration, equipment, software and location changes;

35) Maintain System Security Plans (SSPs); review and make recommendations to PSOs on SSPs from DARPA performers;

36) Ensure configuration management (CM) for security-relevant AIS software, hardware, and firmware is maintained and documented;

37) Ensure that system recovery processes are monitored to ensure that security features and procedures are properly restored;

38) Ensure all AIS security-related documentation is current and accessible to properly authorized individuals;

39) Perform system audits on multiple systems; work closely with system administrators and ensure current security measures are sufficient and in compliance with approved policies and processes;

40) Participate in self-inspections (at DARPA and performer locations); identify security discrepancies and report security incidents;

41) Maintain a working knowledge of DARPA IT system functions, security safeguards, and operational security measures; as well as DARPA programs leveraging IT systems as their inherent capability;

42) Provide advice to SID Information Security and PSOs/PSRs regarding the control and accountability of magnetic and optical media of all types;

43) Perform virus and malicious code scanning on all computer media entering a facility, or provide the applicable certification and training of security administrators and PSRs to be able to conduct same;

44) Perform and conduct training, as required, for conducting secure file transfers between local systems to storage devices, this includes secure down writing of data between systems of different security levels;

45) Inspect incoming equipment to ensure it is what was ordered; inspect outgoing equipment to ensure proper disposal;

46) Provide technical advice and assistance, as required, and perform technical oversight over the development and implementation of new software database systems;

47) Provide technical advice and assistance, as required, and perform technical oversight on telecommunications requirements for Collateral, SAP, and SCI support;

48) In coordination with SID Emergency Management, review and provide AIS security relevant input to DARPA Emergency/Disaster plans and procedures;

49) Participate in Configuration Control Boards; and,

50) Assist in inquiries and investigations of possible security incidents involving local AIS.

8. IA SPECIALIST PERFORMING COMPUTER NETWORK DEFENSE (CND) FUNCTIONS

8.1 Contractor personnel assigned to perform CND functions on this contract perform the following functions: track, collect incident information, investigate, analyze, plan/coordinate, and direct all response and recovery activities related to computer security incidents.

8.2 The contractor shall perform a myriad of CND duties, to include:

1) Detection, respond, mitigate, and report on cyber threats affecting DARPA networks;

2) Maintain an understanding of the current vulnerabilities, response, and mitigation strategies used in cyber security operations;

3) Produce reports and briefings to provide an accurate depiction of the current threat landscape and associated risks;

4) Achieve acceptable configuration through passive evaluations (compliance audits) and active evaluations (penetration tests and/or vulnerability assessments);

5) Use data collected from a variety of CND tools (including intrusion detection system alerts, firewall and network traffic logs, and host system logs) to analyze events that occur within the DARPA environment;

6) Use of customer, community, and open source reporting to develop information on CND activities;

7) Analyze correlated information sources;

8) Facilitate the customer's posture to aggressively investigate cyber activity targeting customer information and its information infrastructure.

9) Maintain proficiency in the use and production of visualization charts, link analysis diagrams, and database queries;

10) Maintain knowledge of applicable CND policies, regulations, and compliance documents specifically related to DARPA assets;

11) Perform CND vulnerability assessments within the DARPA facility;

12) Perform assessments of systems and networks within DARPA and identify where those systems/networks deviate from acceptable configurations, DARPA policy, or local policy;

13) Perform CND vulnerability assessments within the DARPA facility, perform CND risk assessments within the DARPA facility, conduct authorized penetration testing of DARPA network assets;

14) Analyze and report cyber threats and assist in deterring, identifying, monitoring, investigating and analyzing computer network intrusions;

15) Investigate and perform incident analysis to include system, network, and malicious code analysis;

16) Participate in an Incident Response Team responsible for responding to computer security events;

17) Analyze site/enclave CND policies and configurations and evaluate compliance with regulations and DARPA directives;

18) Perform incident reporting with distribution to proper DoD channels and law enforcement/intelligence communities;

19) Additional duties may include providing intrusion support to high technology investigations in the form of computer evidence seizure, computer forensic analysis, data recovery, and network assessments;

9. SECURITY EDUCATION, TRAINING, AWARENESS AND OPERATIONS SECURITY (OPSEC) SPECIALIST

A key component of SID's protection mission for DARPA is to administer and conduct a comprehensive Security Education, Training and Awareness Program. Security awareness is the knowledge and attitude that members of an organization possess regarding the protection of the physical and, especially, information assets of the organization. In that regard SID manages an aggressive and on-going Security, Education, Training, and Awareness program. Many of the DARPA PMs and their supporting Systems Engineering and Technical Assistance (SETA) contractors come to DARPA with little, or no, experience working in the DoD or in an environment involving classified information. The SID security education program is a graduated one, tailored to the needs of its varied audience. It encompasses basic DARPA building access procedures, handling of classified information, intelligence and terrorist threats that may be directed against DARPA or its employees, the basics of OPSEC, and procedures to be followed in the event of an emergency. For selected individuals, additional security-related education is provided to acquaint, or reinforce, knowledge related to the safeguarding of SAP, SCI, and COMSEC materials, as well as other more specialized training needs. Periodic re-training is also managed and documented.

OPSEC is a Presidentially-mandated process (via National Security Decision Directive 298) and is implemented within the DoD by DoD Directive 5205.02. It is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

9.1 The contractor shall perform the following duties related to Security Education, Training & Awareness:

1) Develop briefings, write scripts, develop charts/graphics for use during NISPOM required training;
2) Distribute program classified briefings (indoctrinations and updates);
3) Distribute security awareness products electronically
4) Conduct training needs analysis
5) Prepare and publish annual Agency security awareness training plan, short-term goals and long-term goals; update as required;
6) Write quarterly security awareness newsletters for general population;
7) Write security awareness newsletter for security educators;
8) Develop, review, and produce security awareness products that reflect adverse security trends;
9) Write training plans for quarterly awareness training and specific training modules; update as required;
10) Support DSS Academy's security awareness products web site and security professionalism initiative;
11) Liaison with the Defense Security Service (DSS) Academy;
12) Support DSS Academy's collateral and SAP security professionalism certification program and disseminate information to DARPA SID leadership, PSOs, and PSRs.
13) Write training plans for DSS Academy's SAP curriculum, as requested;
14) Support DSS Academy as an adjunct instructor for special program training curriculum, as required;
15) Support and conduct DARPA newcomer training;
16) Provide input for the rewrite of requirements documents to include the NISPOMSUP Overprint;
17) Convene, and conduct, quarterly security awareness meetings;

18) Assist in the development and maintenance of a DARPA security education products web site;

19) Write special reports of security topics of interest for community;

20) Schedule, convene, conduct, and participate in miscellaneous meetings discussions with other service or Agency security educators (DSSA, Navy, etc.);

21) Update security awareness products to maintain accuracy;

22) Schedule personnel to attend off site training; and,

23) Disseminate policy documentation and correspondence to the community, as requested.

9.2 The contractor shall be an integral team member of the DARPA OPSEC process. The contractor will work in close cooperation with the DARPA OPSEC Manager to ensure that the Agency's information, personnel, and programs have the appropriate OPSEC posture to counter adversary collection. The contractor, in cooperation with other elements (contractor and government) of SID and DARPA, shall perform the following duties related to OPSEC:.

1) Become thoroughly familiar with the DARPA organization, and with the programs (and the performers) that the Agency is currently pursuing, and remain current on emerging programs;

2) Working closely with Technical Office PMs, their SETA staffs, PSOs, PSRs and External Relations personnel, shall develop, and maintain currency of Essential Elements of Friendly Information (EEFI) for DARPA and its programs to be used to preclude inadvertent public release/disclosure of critical or sensitive information;

3) Identify Critical Information: Identifying information on DARPA programs vitally needed by an adversary (which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive unclassified information);

4) Identify Threats: working with SID and CI staff, assemble information and perform the research and analysis of intelligence, counterintelligence, and open source information to identify likely adversaries DARPA and selected programs;

5) Examine each aspect of DARPA to identify OPSEC indicators that could reveal critical information, and comparing those indicators with adversary's intelligence collection capabilities of identified threat entities;

6) Working with SID intelligence/counterintelligence assets and DARPA Technical Office PMs analyze vulnerabilities identified and identify possible OPSEC countermeasures to mitigate each vulnerability.

7) Assist PMs and their SETA staffs in examining specific OPSEC countermeasures which should be selected for execution based upon a risk assessment to weigh the impacts on program costs, schedule, and ultimate program capability maintenance.

8) Assist PMs, their SETA staffs, and performer staffs, if necessary, in the application of appropriate OPSEC countermeasures;

9) Document the complete OPSEC process in program-specific OPSEC plans;

10) The contractor will, by maintaining contact with the Interagency OPSEC Support Staff (IOSS), develop or import, appropriate OPSEC awareness products and or training materials and make them available to DARPA personnel and its contractors;

11) The contractor will, working with the SID staff, coordinate the execution of an annual OPSEC Assessment of DARPA. An OPSEC assessment is an intensive application of the OPSEC process to an existing operation or activity by a multidisciplinary team of experts. Assessments are essential for identifying requirements for additional OPSEC measures and for making necessary changes in existing OPSEC measures;

12) The contractor shall, working with the DARPA OPSEC Manager, PSOs, PSRs, and other SID elements, organize and participate in OPSEC Surveys of selected DARPA program activities, as required; and,

13) The contractor shall ensure that the Overarching DARPA Operations Security Plan is periodically monitored, in light of evolving DARPA program thrusts, and is updated, as required, to remain current.

10. <u>INTERNATIONAL SECURITY (INCLUDING TREATY COMPLIANCE) SPECIALIST</u>

SID's International Security program is a cooperative effort which involves PSRs, CI, Industrial/ Information Security, DARPA SAPCO, and the DARPA SSO. The primary purpose of SID's International Security program is to ensure the appropriateness of the disclosure of information to foreign entities and to ensure that adequate protection for such information is provided through appropriate agreements and procedures. The SID International Security program is integral to ensuring the Agency's equities are protected through the review and coordination on Export Licenses, Commodity Jurisdictions (CJ's), Committee on Foreign Investment in the United States (CFIUS) cases, as well as oversight and monitoring of the foreign national visit and exchange programs at DARPA.

10.1 The contractor shall perform the following tasks, which include, but are not limited to:

1) Prepare materials and documents required for assessing the exchange of information with Foreign Governments, Foreign Nationals, and international organizations to assure compliance with requirements in the National Disclosure Policy (NDP), Arms Export Control Act (AECA), Export Administration Regulations (EAR), and other relevant policies, statutes, and instructions; provide rationale and recommendations for release or non-release decisions.
2) Research, determine, and recommend how export requests should be processed; draft security compromise damage assessments;

3) Apply EAR, AECA and NDP to DARPA technologies, including but not limited to:
    a) Aeronautics systems
    b) Armaments and energetic materials
    c) Chemical and biological systems
    d) Directed and kinetic energy systems
    e) Electronics
    f) Ground systems
    g) Guidance, navigation and vehicle control
    h) Information systems
    i) Information warfare
    j) Manufacturing and fabrication
    k) Marine systems
    l) Materials
    m) Nuclear systems
    n) Power systems
    o) Sensors and lasers
    p) Signature control
    q) Space systems
    r) Weapons effects and countermeasures
4) Determine, recommend, and prepare input relative to treaty compliance issues and inspections pertinent to DARPA programs;
5) Develop an understanding of the nature and extent of pertinent bilateral and multilateral security and information exchange agreements which apply to DARPA programs and technical areas;
6) Develop an understanding of the AECA and its application to DARPA activities;
7) Assist program managers, where required, in the application of the Department of State Form DSP-85, "Application/License for Permanent/Temporary Export or Temporary Import of Classified Defense Articles and Classified Technical Data", to DARPA activities;
8) Complete data entry into the Security Policy Automated Network (SPAN) and such other databases that may be identified;
9) Apply the procedures for the international transfers of classified material, and the release of U.S. classified material to foreign persons;
10) Maintain familiarity with CFIUS reports;
11) Determine, recommend, and prepare input relative to CFIUS cases;
12) Working with SID Industrial/Information Security, determine whether U.S. companies engaged in DARPA efforts, or proposed as potential DARPA performers, are under Foreign Ownership, Control, or Influence (FOCI), to include the nature, and extent of FOCI and ownership or control, in whole or in part, by a foreign government;
13) Implement FOCI case processing guidance and procedures;
14) Assist DARPA PMs and their SETA teams with drafting Technical Assistance Agreements (TAA);
15) In coordination with the SID Industrial/Information Security Section, be aware of the record of firms' engaged in DARPA efforts, or proposed as potential DARPA performers, compliance with pertinent U.S. laws, regulations, and contracts;
16) Review material and make recommendations relative to its appropriateness for public release;
17) Monitor the visits and requests to visit DARPA by Foreign Nationals, ensuring that requests to visits are processed through proper channels and, as appropriate, that any assignment of Foreign Nationals are processed in accordance with the

Defense Personnel Exchange Program (DPEP) agreements or the International Visit Program (IVP), providing rationale for approving or rejecting the visit;

18) Working with the DARPA SAPCO, identify issues relative to DARPA SAP activities and their relationship in context to treaty compliance options to adhere to or challenge treaty language;
19) Recommend and prepare proposed changes to policy, directives, treaties, and/or SAP security implementation to address compliance issues;
20) Assist in the development, writing, review, edit, and execution of treaty compliance plans (TCPs);
21) Prepare for and attend security compliance reviews, as required;
22) Maintain and keep up to date those International Arms Control Agreements and treaties which apply to DARPA efforts;
23) Maintain and keep up to date documentation associated with the Defense Treaty Inspection Readiness Program (DTIRP);
24) Apply to international security issues involving DARPA efforts or information those elements governed by the Atomic Energy Act of 1964, and the handling of Restricted Data (RD), Formerly Restricted Data (FRD) information, and Critical Nuclear Weapons Design Information (CNWDI).
25) Provide advice and assistance, as required regarding International Contracts involving classified information;
26) Provide advice to DARPA staff on the following:
    a. Bilateral Security Agreements;
    b. Project Arrangements
    c. Industrial Security Agreements
    d. Export Authorizations
    e. Manufacturing License Agreement
    f. Letters of Offer and Acceptance
    g. Procurement contracts awarded to Foreign Contractors (prime or subcontractor)
    h. Grants, or other contract vehicles, awarded to foreign universities

11. <u>INTERNATIONAL RELATIONS (INTERNATIONAL COOPERATION) SPECIALIST</u>

The Director SID is dual-hatted as the Director International Cooperation and administers and implements DARPA's Science and Technology International Cooperation. This function requires maintaining close working relationships with DoD Acquisition Technology and Logistics, International Cooperation (AT&L/IC), DARPA leadership and DARPA Technical Offices, and requires extensive intra-SID cooperation between International Security, , Industrial/Information Security, and Intelligence & Counterintelligence offices to ensure that the Director, DARPA's International Cooperation goals are successfully met.

11.1 The contractor International Relations Specialists shall lead and execute DARPA's International Cooperation engagement in areas of interest with government agencies, the academic business and legal communities, and non-commercial interests. They shall provide timely, pertinent recommendations to SID and other DARPA personnel.

11.2 The contractor shall perform the following duties, which include, but are not limited to:

1) Monitor, identify and analyze international developments, public policy issues and trends, and impact on strategy in regions of interest to DARPA, and translate data developed into practical plans;
2) Analyze local and regional developments and create reports and communications such as position papers and reports to communicate DARPAs international strategy;
3) Engage in regional and international governance dialogues, including strategy to address issues affecting DARPA;
4) Work in partnership with appropriate internal orgauizations to develop and carry out educational activities to familiarize employees/contractors on international issues which might affect DARPA;
5) Provide advice, assistance, and input on issues relevant to regions of interest to DARPA;
6) Seek internal DARPA guidance on issues relevant to regional success;
7) Serve as an expert for the organization in specific region(s), maintain area expertise and prepare reports, briefs, presentations and media releases;
8) Engage with regional and international inter-governmental forums, as requested by DARPA;
9) Identify public policy influences, political issues, trends, that impact DARPA;
10) Identify and implement improvements for DARPAs global work;
11) When directed by DARPA examine the central concerns of international relations, including diplomacy, foreign policy analysis, international organizations, global development, and international relations theory. Explore global economies, societies, and cultural issues.
12) Analyze requests by foreign entities to determine potential DARPA program applicability. Discuss the request with appropriate country desk officers at the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)) and prepare correspondence for DARPA senior leadership;
13) Conduct detailed research, author correspondence, and manage an Agency-level international program. Integrate security, public affairs guidance and counterintelligence in all elements of international activities;
14) Analyze proposed visits of foreign persons to DARPA/DARPA events, or events where DARPA senior leadership may be in attendance. Prepare position paper/read-ahead/trip & country books as required;
15) Assist with the planning and execution of foreign visits to DARPA that have senior leadership attention. Prepare position paper/read-ahead/trip & country

books as required; identify, develop, and present foreign trip planning to meet the Agency's requirements. This will involve, but is not limited, to:

a. Documentation on countries to be visited;
b. Working with US government agencies and foreign embassies on scheduling, meetings, events, flights, hotels, etc.; and,
c. Preparing draft and final proposed subjects, attendee lists, etc., and presenting these to senior management.
d. Managing all trip logistics.

16) Plan/Manage and support DARPA hosted international workshops and other forums. Prepare, coordinate and track post workshop action items, meeting minutes, and other correspondence;

17) Develop a working relationship with counterparts in key international offices, such as:

a. Office of the Deputy Undersecretary of the Air Force for International Affairs (SAF/IA);

b. Office of Naval Research (ONR)

c. US Air Force Material Command, Air Force Research Laboratory (AFRL)

d. Technical Support Working Group (TSWG)

e. Office of the Secretary of Defense (OSD)

f. Department of the Army (DoA)

g. Navy International Program Office (NIPO)

h. OUSD(AT&L)

i. US and foreign embassies

18) Participate in working groups, forums and other gatherings to remain current and represent DARPA interests;

19) Work with OUSD (AT&L)/IC and other necessary offices in developing Project Agreements (PA) to support specific DARPA programs. Prepare, or cause to be prepared, all PA documentation, Summary Statement of Intent (SSOI's), Request for Authority to Develop and Negotiate (RAD's), Request for Final Approval (RPA's), Program Security Instruction (PSI), briefings to LO/CLO, briefings to OUSD(AT&L), etc;

20) Develop and maintain an International document database. Include all contracts, grants, cooperative agreements, other transactions and PA's, associated country specific information, treaties, information exchange agreements, and other relevant documentation. Prepare reports and presentations as required from the database information, and;

21) Recommend to DARPA program management the appropriate instrument for international engagements associated with program execution.

22) Identify, develop, and present foreign trip planning to meet DARPA requirements. This will involve, but is not limited to:

a. Documentation on countries to be visited;

b. Working with US governmental agencies and foreign embassies on scheduling, meetings, events, flights, hotels, etc., and;

c. Preparing draft and final proposed subjects, attendee lists, etc., and presenting these to senior management.

12. INTELLIGENCE/COUNTERINTELLIGENCE ANALYST

DARPA's organic counterintelligence (CI) program includes detecting, identifying, accessing, and, in conjunction with the assigned counterintelligence support activity, analyzing information on adversary intentions and capabilities. This may include developing programs, systems, and procedures designed to counter intelligence collection efforts and activities of foreign entities, including sabotage and terrorist activities. DARPA's organic CI program is completely integrated with and informed by all SID functional disciplines. The end-product of DARPA's organic CI program includes recommending cost-effective protective measures and countermeasures for DARPA personnel, programs, and activities. Contractor Intelligence/Counterintelligence analysts will enable DARPA's organic CI program to realize the positive attributes inherent in combining the IC resources of the resident Naval Criminal Investigation Service (NCIS) Special Agent with a trained/qualified internal multi-disciplined security team in applying Intelligence/CI context to protecting DARPA programs. This nascent internal structure will develop or adapt existing programs, systems, and procedures to proactively counter foreign intelligence collection efforts and activities, including sabotage and terrorist activities. The activities of the organic DARPA Intelligence/Counterintelligence will always be conducted in coordination with the assigned counterintelligence support activity staff. At no time will any contractor assigned to the contract perform any act, obtain (or retain) any document or computer file of any type in contravention of provisions of any portion of the United States Code, Executive Orders, Director of National Intelligence (DNI) Intelligence Community Directives (ICDs) or DoD Directive.

12.1 The contractors assigned as Intelligence/Counterintelligence Analysts shall perform the following tasks:

1) Determine essential elements of information, and conduct activities to detect, identify, assess, exploit, and proactively counter or neutralize hostile intelligence collection, sabotage, and terrorist activities;

2) Plan special analytical projects in response to client assignments which include analytical approach, schedule, personnel requirements, data collection, travel, assessment criteria, and costs;

3) Research and collect required data, perform analyses, and summarize findings in response to client requests;

4) Compile detailed reports of analyses clearly defining the problem or issue, factors considered, findings, and provide clear, concise conclusions and recommendations;

6) Develop innovative and proactive analytical methodologies; refining existing program protection analytical methodologies to meet evolving program needs;

7) Provide Intelligence/Counterintelligence input and assisting PSRs, PMs, and SETAs in developing Program Protection Plans;

8) Review and provide comments on Program Protection Plans, Test Plans, OPSEC Plans, and other planning documentation as required;

9) Assist Technical Office management, PMs, SETAs security personnel in performing SAP lifecycle threat analyses;

10) Apply analytical methodologies to existing programs to review, and readdress if necessary, their protection needs to remain consistent with changes in diplomatic, political, and military environments;

11) Assess and postulate international diplomatic, political, and military responses to proposed program actions and activities;

12) Perform short-notice contingency and exposure analyses, summarizing implications, and providing viable responses and recommended courses of action;

13) Working with individual program management personnel to assist in analyzing and developing solutions to unique or difficult CI-related issues;

14) Review organizational mission statements and associated publicly available information for inconsistencies which may reveal sensitive information;

15) Review, analyze, and, where appropriate, make recommendations to long-term program protection policies and practices;

16) Provide intelligence and counterintelligence threat data and analyses to support assessments and surveys of Agency-wide OPSEC programs;

17) Assist DARPA PMs in identification of program CPI and assist in the development of Agency-wide and program-specific OPSEC plans, and make recommendations for additions or changes where appropriate;

18) Participate, as appropriate, in program management and planning meetings, and working sessions to provide an intelligence/CI perspective; and,

19) Receive and act on information of CI value from a DARPA polygraph examination and Technical Security Programs.

20) Prepare and deliver comprehensive briefings to increase CI awareness and to inform senior DARPA leadership.

13. <u>INFORMATION / INDUSTRIAL SECURITY SPECIALIST</u>

The contractor shall support the DARPA Information Security program which entails safeguarding, accountability, integrity, reliability and privacy of classified or controlled unclassified information by preventing disclosure, access or release of information to unauthorized personnel. The DARPA Industrial Security program is structured to provide the Agency with a capability to ensure that its contractor performance entities are fully in compliance with both National Industrial Security Policy, as codified in the National Industrial Security Program Operating Manual (NISPOM) and other governing regulations. DARPA executes these responsibilities by being the sole entity for issuing Contract Security Classification Specifications (DD Form 254) for all DARPA-funded efforts. The DARPA Industrial Security program is executed through the Defense Security Service (DSS) for non-SAP efforts. For SAP efforts, DARPA provides all security oversight and compliance verification activities for DARPA contractor performers. The scope of the program includes the identification, marking, accountability, transmission, and safeguarding of collateral, SAP, and Sensitive Compartmented classified and controlled unclassified information as well as information falling under the protection of the Privacy and Freedom of Information Act, ITAR, EAR, and For Official Use Only (FOUO) information.

13.1 The contractor, through dedicated Information/Industrial Security Specialists, shall administer a National Industrial Security Program for DARPA contractors involved in collateral, SAP, and SCI efforts in accordance with the NISPOM, the Department of Defense Supplement, and appropriate Director, National ICDs (formerly Director, Central Intelligence Directives (DCID)). This assistance shall include the verification of, and, as necessary, the processing of facility security clearances for contractor and consultant facilities, determining the data requirements and preparation of the DD Form 254, Contract Security Classification Specification, the coordination and preparation of National Interest Determinations (NIDS), coordinating security requirements with DARPA performers, maintaining a database of performer Facility Security Officers (FSO)and other contacts, coordinating security and other requirements with the DSS, and arranging or providing security oversight and compliance verification activities for DARPA contractors.

13.2 The contractor shall perform the following duties, including, but not limited to:

1) The contractor shall continuously assess the application of the most current DoD and DARPA policy and practices for the protection of classified and controlled unclassified information (CUI) and make recommendations for improvements.

2) Develop and prepare security classification guides, that determine appropriate classification and declassification of material;

3) Apply and/or advise technical office personnel on the application, of appropriate classification markings;

4) Review material to determine the appropriateness of release to the public;

5) Develop and implement programs for controlling and destroying classified and controlled unclassified information;

6) Determining appropriate security requirements for contract efforts;

7) Develop and prepare DD Forms 254, Contract Security Classification Specifications for all DARPA-funded efforts, regardless of contracting agent;

8) Develop, prepare, and coordinate NIDs;

9) Prepare sponsorship documentation and coordinate the granting of facility security clearances (FCL), including interim FCL;

10) Process and document any administrative termination or downgrading of an FCL;

11) Monitor events requiring FCL invalidation, revalidation, or FCL revocation; including FCLs issued in error;

12) Coordinate and conduct, as appropriate, oversight compliance verification visits;

13) Establish, organization and maintain the Facility Files folders, documenting all changing conditions affecting a FCL;

14) Provide advice to SID PSOs and PSRs regarding program performance facilities located on a government installation;

15) Coordinate with SID Personnel Security to facilitate personnel clearances required in connection with FCL application;

16) Review applicable documentation and render a determination if U.S. company performing on DARPA efforts is under FOCI;

17) Research, and make recommendations on potential impacts on contractor's eligibility for access or continued access to classified information;

18) Be familiar with performer's/proposed performer's record of compliance with pertinent U.S. laws, regulations, and contracts;

19) Research ownership, or control, in whole or in part, by a foreign government of performers/prospective performers on DARPA efforts; and,

14. <u>PLANS, POLICIES, AND PROCEDURES (PPP) SPECIALIST</u>

SID is responsible for remaining current on emerging Department of Defense (DoD) security-related policy and procedure documents and for analyzing them and providing the DARPA leadership with recommendations. When necessary, SID initials and staffs Agency implementing guidance. Additionally, SID conducts an ongoing comprehensive review of existing DARPA security-related policies to ensure that they remain relevant to the security objectives of the Agency; initiating updates, as required.

14.1 The PPP specialist shall be responsible for the preparation and maintenance of all SID plans, policies, and procedures. These products must remain current and in compliance with applicable DoD guidance. The PPP specialist will liaise with policy departments within DoD and DARPA to maintain awareness of policy related to SID areas of responsibility. The PPP specialist will coordinate with the appropriate Subject Matter Experts (SMEs), both internal and external to DARPA, and provide SID management with a comprehensive analysis; compile and draft SID comments, as applicable, describing potential impacts to SID and DARPA; and, create or update SID documentation as necessary.

14.2 The contractor PPP specialists' duties shall include, but are not limited to, the following tasks:

1) Research and collect required data, perform analysis, and summarize findings in response to changes in policy (internal and external to DARPA);

2) Draft, coordinate, and maintain currency of comprehensive SID guidance;

3) Compile detailed reports of analysis which include: clearly define problems or issues, factors considered, findings, and provide clear, concise conclusions and recommendations;

4) Develop innovative and proactive analytical methodologies; refine existing program methodologies to meet evolving needs;

5) Review, analyze, and, where appropriate, make recommendations to long-term SID plans, policies, and procedures;

6) Review and provide comments on other planning documentation as required;

7) Develop comprehensive briefings to inform SID and DARPA leadership;

8) Draft position papers, and other planning documentation, as required; and,

9) Participate, as appropriate, in planning meetings and working sessions.

10) Develop a basic understanding of DARPA, its technology thrusts, and the DoD organizational structure.

11) Maintain an up-to-date database of current DoD security policy and procedures.

12) Review changes to, or issuances of new, DoD security policy documents within 30 days of promulgation and notify Director, SID.

15. FREEDOM OF INFORMATION ACT SPECIALIST

SID is responsible for administering the Agency's Freedom of Information Act (FOIA) program in accordance with Public Law, Executive Orders, and the implementing guidance contained in DoD Directives and Instructions. As a result of the FOIA and its implementing guidance, SID is required to open, monitor, and respond to FOIA requests in a timely manner. SID, as the DARPA element responsible for FOIA actions under the purview of the OSD Office of Freedom of Information (OFOI), responds to FOIA requests from the public, Congress, and other government agencies through the OFOI. The SID FOIA Office provides guidance and advice to DARPA staff to ensure compliance with Federal laws, regulations, and policies to senior management officials. This advice, coordinated with the OFOI, shall be specific to Federal disclosure laws and governmental procedures with respect to disclosure of agency records. The SID FOIA Office is also responsible for developing and coordinating with appropriate DARPA staff elements: the Agency disclosure framework; FOIA training; disclosure policy; and, program development to promote adherence to information disclosure principles.

15.1 The contractor shall perform the following duties including, but not limited to:

1) Develop and recommend implementation of agency-level FOIA compliance and program oversight structures;

2) In conjunction with the OFOI, DARPA External Relations Offiee, and General Counsel, recommend implementation of agency-wide FOIA policies and procedures including internal procedures and guidelines based upon new or revised legislation or recommendations;

3) Receive, log-in, suspense, and monitor FOIA requests received from OFOI to ensure they are handled in a timely manner, in accordance with DoD guidance contained in DoD Regulation 5400.7;

4) In coordination with the General Counsel and External Relations Office, interpret regulations and agency policy regarding release of information under the FOIA for DARPA personnel;

5) Develop and recommend refinements to FOIA projects, and keep abreast of these projects providing the capability to support DARPA compliance with the Electronic Freedom of Information Act Amendments of 1996 (E-FOIA);

6) Develop and be prepared to apply the guidance associated with the Freedom of Information Act, restrictions on dissemination/withholding of material to the public, principles of classification as embodied in Executive Orders, DoD Directives and Instructions, and Security Classification Guides;

7) The collection, organization, and analysis of qualitative and quantitative data needed for annual reporting of FOIA activities for DARPA FOIA actions is accomplished by OFOI;

16. DATABASE/WEB SYSTEMS ADMINISTRATOR

Provides program support regarding tool/database design and development. Plans, documents, and coordinates the phased development of an integrated management information system with associated interfaces to both COTS and GOTS software applications.

16.1 The Database Systems Administrator shall be responsible for the performance, integrity, and security of databases to include planning, development, implementation, and troubleshooting. The Database Systems Administrator shall perform the following functions in supporting the DARPA SID:

1) Establish the needs of users and monitor user access and security.

2) Monitor performance and manage parameters to provide fast query responses to front end users.

3) Map out the conceptual design for a planned database in outline form.

4) Refine the logical design so that it can be translated into a specific data model.

5) Refine the physical design to meet system storage requirements.

6) Coordinate the installs and tests new versions of the database management system.

7) Write database documentation, including data standards, procedures, and definitions for the data dictionary.

8) Control access permissions and privileges.

9) Develop, manage, and tests backup and recovery plans.

10) Ensure that storage, archiving, backup, and recovery procedures are functioning correctly.

11) Analyze the data stored in the databases and make recommendations relating to performance and efficiency of that data storage.

12) Communicate regularly with onsite technical, applications, and operational staff to ensure database integrity and security.

13) Support critical business operations involving scheduled and dynamic requests, receipt, and transmission of data to internal and external clients and partners as requested.

14) Oversee requirements gathering sessions with SID personnel, assimilate information and maintain effective internal data standards and capabilities while meeting customer expectations.

15) Provide a program to assure that all system users are trained in the use of the database systems and provide an audit program to verify the accuracy of data entry.

16) Coordinate maintenance and repair activities for the automated database systems.

17) Maintain an inventory and a configuration control file of the database systems, and ensure system maintenance, software upgrades, data archiving, and tests are conducted to assure the system is run at peak efficiency and that historical data is not lost.

18) Review and recommend requirements to assess disposition, upgrade, and/or update technology.

19) Other duties and responsibilities as assigned by SID management to assure peak efficiency of the systems.

20) Design, develop, program, test, and debug new software and upgrades to existing software using VB.net or others as appropriate.

21) Prepare software demonstrations, and associated documentation including technical references and user manuals.

17. IT ANALYST/ENGINEER

Supports DARPAs multi-level secure enterprise solutions operating at Protection-level four (4) and distributed nationwide. Currently there are between sixty (60) and one-hundred (100) distributed sites. The IT Analyst/Engineer will have the primary responsibility to evaluate, analyze, validate, specify, and manage the proposed and actual technical implementation of the customer requirements. The technical solutions will include software development efforts as well as the deployment of COTS or GOTS hardware or software tools to be used in the office automation environment.

17.1 The IT Analyst/Engineer shall perform the following functions in supporting the DARPA SSO/SID:

1) Work with the government, customers, and the Operations & Maintenance (O&M) contractor technical leads to evaluate the effectiveness of proposed and implemented technical solutions;
2) Identify functional areas impacted by proposed changes to the Enterprise Architecture;
3) Validate the viability of proposed technical solutions in the current IT environment;
4) Determine areas of potential improvement through new or currently un-used technologies;
5) Manage the architecture specifications and high-level design for technical changes;
6) Provide input into the prioritization of technical changes and projects by providing information on the impact of the changes/projects;
7) Manage requirements traceability information throughout the projects;
8) Lead and support the creation of risk analysis during all the stages of development;
9) Manage changes to the IT environment through effective application of change control processes and tools;
10) Assist with the development of the government's requirements engineering policies, procedures, and tools;
11) Identify ways to assist the government customers through the introduction of new technologies to the back office and customer business processes;
12) Interact with customer and third parties as a technical SME on various topics relating to systems development, engineering, and administration;
13) Critically evaluate the information gathered from multiple sources, reconcile conflicts, decompose high-level information into details, abstract up from low-level information to a more general understanding, distinguish presented user requests from the underlying true needs, and distinguish solution ideas from requirements;
14) Work with the vast array of information gathered during elicitation and analysis and deal effectively with rapidly changing information;
15) Explore and identify new areas of unmet customer needs by validating data obtained via other techniques;
16) Negotiate priorities and resolve conflicts among project stakeholders (such as customers, Product Management, and Engineering);
17) Orchestrate and coordinate information exchange between higher, adjacent, and subordinate commands, other DoD/government agencies and contract vendors;

18. POLYGRAPHER

The Polygraph Examiner will screen and vet individuals in support of DARPA's mission and to assess the protection of highly classified information. Polygraph Examiner accomplishes this by questioning individuals to detect deception or to verify truthfulness, using polygraph equipment and standard polygraph techniques. DARPA operates a random counter-intelligence polygraph program with a single polygrapher.

18.1 Contractor Polygraph Examiner's tasks shall include, but are not limited to, performing the following tasks:

1) Polygraph Examiners shall adhere to all requirements of law and regulation, to include DoD Directive 5210.48, DoD Instruction 5210.91, the Employee Polygraph Protection Act (EPPA), Equal Employment Opportunity Commission (EEOC), Americans with Disabilities Act (ADA), and other applicable bodies of law;
2) Contractor Polygraph Examiners shall, at all times, follow the strict procedures and protocols outlined in DoD Instruction 5210.91, Polygraph and Credibility Assessment Procedures.
3) Contractor Polygraph Examiners shall only address issues pertinent to the type of examination at hand;
4) Ensure that the results of the examination and the Polygrapher assessment are QC'ed by an appropriately qualified polygrapher;
5) Prepare reports of findings and conclusions and submit them to appropriate organizations; keep records of the examinations;
6) Provide information to the SID Personnel Security Office to update Joint Personnel Adjudication System (JPAS) records to reflect polygraph examinations completed;
7) Contractor Polygraph Examiners shall not render an opinion concerning the truthfulness of an examinee until after all data suitable for analysis has been analyzed.
8) To assure examiner compliance with the listed recommendations, and to sustain the quality of the testing program, an independent quality assurance review of each examiners' work product shall take place regularly.

19. PRIVACY SPECIALIST

Responsible and accountable for ensuring implementation of DARPAs information privacy protections, including compliance with federal laws, national policy and DoD regulations relating to privacy for internal and external programs. The contractor shall maintain a Privacy Program within DARPA consistent with 5 U.S.C Section 552a "The Privacy Act of 1974 as amended, and DoD Directive 5400.11 and 5400.11-R "DoD Privacy Program". The Privacy Specialist will administer existing processes and procedures, or establish new or revised processes and procedures to ensure that DARPA is in full compliance with legislative privacy requirements and information requests and all existing directives and instructions.

19.1 The contractor shall perform the following duties in the execution of privacy related tasks:

1) Establish administrative processes and procedures to manage and implement a comprehensive privacy program;
2) Formulate, plan and manage a privacy program to protect personal information and information systems from unauthorized use, access, disclosure, or sharing;

3) Ensure that DARPA processes minimize unnecessary collection of personal information;
4) Ensure DARPA compliance with legislative privacy requirements and information requests;
5) Prepare System of Records Notices (SORNs) and Privacy Impact Assessments (PIAs) and coordinate with the DoD Privacy Office to ensure compliance for publication and auditing requirements;
6) Conduct training consistent with public law, DoD regulation and DARPA initiatives to ensure proper handling of privacy information which includes collection, processing, storage and retrieval of personally identifiable information to agency personnel who work with privacy information;
7) Assist with technology assessments on impacts of technology on the privacy and personal information;
8) Establish and manage an internal review of DARPA's privacy program to include a bi-annual review of SORNs;
9) Communicate and coordinate with the DoD Privacy Office on DARPA related privacy issues;
10) Prepare and submit reporting requirements to the DoD Privacy Office;
11) Responsible and accountable for ensuring implementation of information privacy protections, including compliance with federal laws, national policy and DoD regulations relating to privacy for internal and external programs;
12) Provide inputs on Privacy related information to support the Security Education Awareness training program;
13) Develop Privacy education bulletins, directives, security plans, procedures and controls as required;
14) Prepare and protect files, records and other information;
15) Coordinate with other security offices, organizations, and personnel in support of mission requirements;
16) Maintain and follow-up on suspense records for correspondence or action items;
17) Prepare a wide variety of recurring and nonrecurring correspondence, reports and other documents;
18) Gather information, verify facts, and assemble background materials, reference material, and reports for executive level officials for meetings and conferences;
19) Proof read, QC, DoD and DARPA Format compliance, task tracking and disposition;
20) Establish and manage workflow staffing process;
21) Support the coordination of executive correspondence/products to resolve issues/obtain concurrences for planned actions; receive guidance on choosing appropriate courses of policy/programmatic or administrative actions; and,
22) Make recommendations for the best use of present resources and assist with planning for future resource needs, estimating both short and long-range

personnel, budgetary, space, and equipment needs, and implements new resources.

20. BUDGET ANALYST

The contractor supports the DARPA Comptroller in managing the DARPA SAP budget, which involve systems/program management execution support, business review facilitation, business process improvement, independent budget analysis, financial management support, business oversight reviews, management training, technology transfer, quality assurance support, and the preparation of annual SAP reports to congress.

20.1 The contractor shall perform the following duties in the execution of budget analyst tasks:

1) Prepare and protect files, records and other information;
2) Coordinate with other security offices, organizations, and personnel in support of mission requirements;
3) Maintain and follow-up on suspense records for correspondence or action items;
4) Prepare a wide variety of recurring and nonrecurring correspondence, reports and other documents;
5) Gather information, verify facts, and assemble background materials, reference material, and reports for executive level officials for meetings and conferences;
6) Proof read, QC, DoD and DARPA Format compliance, task tracking and disposition;
7) Establish and manage workflow staffing process;
8) Support the coordination of executive correspondence/products to resolve issues/obtain concurrences for planned actions; receive guidance on choosing appropriate courses of policy/programmatic or administrative actions; and,
9) Make recommendations for the best use of present resources and assist with planning for future resource needs, estimating both short and long-range personnel, budgetary, space, and equipment needs, and implements new resources.

20.2 The following tasks represent the primary nature of the work to be performed by the Budget Analyst within three (3) Key Functional Areas:

1) Internal Control which shall include assisting the government client in providing internal control for all classified financial management units assigned to DARPA as directed by the government client and includes the following specific tasks:

   a. Provide internal control support for all financial management units assigned to DARPA as directed by the government client;
   b. Establish and implement management controls to monitor and track classified budget execution;

c. Work with DARPA programming staff to establish a classified financial database;
d. Conduct special studies and analyses;
e. Analyze accounting system reports to ensure compliance with budget, tracking, and reporting requirements;

2) Plans and Operating Procedures which shall include documenting the budgetary responsibilities assigned under the Internal Control Task including the following:

a. Prepare implementation plans;
b. Develop standard operating procedures;
c. Provide financial management procedural guidance to financial management units as directed by the government client;

3) Funding Authorization, Budget Execution and Policy which shall include providing budget execution support and includes the following:

a. Assist the government client in distributing funding authorization documents;

b. Prepare and brief managers on budget execution processes;

SECTION 3 - DELIVERABLES

OVERVIEW: The contractor shall be required to submit plans, studies, white papers, reports and other documents, on a scheduled or as-needed basis in furtherance of the DARPA security program. The contractor shall provide the following reports and deliverables in accordance with the requirements below:

1. **MONTHLY MANAGEMENT REPORTS**: The contractor shall prepare and submit *Monthly Management Reports* within 5 calendar days after the month being reported to depict the status and progress of work efforts, schedules, and costs as further described below. The contractor shall recommend any other formatting for the report not addressed in this section to the COR for approval before initial submission.

1. Contractor's name and address;
2. Contract number;
3. Date of report;
4. Period covered by report;
5. Cost curves portraying proposed/initial estimates, actuals, and Estimates to Complete through contract period;
6. Cost incurred for the reporting period and total contractual expenditures as of report date.

The format for providing incurred costs shall be in the same format as that provided nnder Cost Proposal Summary – Format Requirements. Labor costs for Subcontractor and Consultant

Personnel (both those in the Contractor's team and that provided under the ODC CLIN) may be shown as a Fully Loaded Labor Rate for each subcontractor and consultant personnel. However, for each subcontractor's fully loaded labor rates a notation shall be provided indicating the fee/profit percentage that is incorporated into each subcontractor rate. Other Direct Costs shall be separated and detailed by cost category (Travel, Material, Maintenance, Consultants, etc). Special Projects shall be detailed separately, if requested. Also note that the cost information from these reports shall be traceable to the invoices;

7. Cost and technical status of projects and/or equipment directed or approved by Director, SID. This shall include:

   i. For projects, percentage of completion, date project was approved, original start date, estimated milestone and completion dates, explanation for adjustment to milestone and completion dates, projected costs and breakdown of actual costs by component, funds associated with the project, funds remaining, and problems and achievements.

   ii. For equipment or material, status of order (e.g., in process, date order approved by government, date order placed, expected delivery date), anticipated cost and actual cost, a breakdown of costs by component, to include contractor fees.

8. Description of progress made during period reported, including problem areas encountered, recommendations, if any for subsequent solution beyond the scope of this contract;
9. Trips and significant results;
10. Plans for activities during the following period;
11. A personnel status (authorized, present, vacant) and security clearance status (clearance level and date submitted), and overtime usage;
12. Staffing Plan and/or Organization Chart
13. Employee Roster
14. Projected staffing issues for the next reporting period such as, employee planned absences (sick, vacation, leave of absence, etc.), terminations, resignations, new hires, etc.
15. Other contract related data as required by SID management.

2. **SELF-INSPECTION PLAN AND OUTCOME REPORT:** The contractor shall assist with implementing and maintaining a DARPA-wide Self-Inspection Program that meets the requirements of DoD Regulation 5200.1, Information Security Program. The development of the program shall include the development and recommendation of an implementation plan and schedule, and upon approval, the use of checklists that can be used to identify inspection areas and record observations and findings. A detailed self-inspection shall be conducted of all DARPA areas on an annual basis. The contractor shall submit an initial *Self*-Inspection *Plan and Outcome Report* when requested and updates to the plan/report shall be made on an annual basis thereafter. The Outcome Report section shall contain the results of the self-inspection activity. The contractor shall recommend the format and content of the report to the COR for approval before initial submission.

3. **REVIEWS OF DOD POLICY AND PROCEDURE DOCUMENTS:** The contractor shall prepare and submit the *Reviews to DoD Security Policy Document Changes or Revisions* to new DoD security policy documents or changes in policy documents within 30 days from the date the policy is promulgated. The contractor shall recommend the format of the report to the COR for approval before initial submission.

4. **FUNCTIONAL AREA STANDARD OPERATION PROCEDURES:** The contractor shall prepare, where one does not already exist, an SOP for each functional area. These SOPs will be approved by the Government and will be kept updated and reviewed annually. Changes proposed will be approved by the Government. The results of the reviews, and the changes proposed will be provided for Government approval not later than ten days after the completion of the contract year.

5. **DARPA SECURITY MANUAL UPDATES:** The contractor shall review the DARPA Security Manual annually and recommend changes or additions for inclusion. The contractor shall provide a *Security Manual Update Report* of the review and recommended changes to the Government within ten days after review completion.

6. **EQUIPMENT ACCOUNTABILITY AND REPORTING:** The contractor shall, in applicable cases, submit the Centrally Reportable Equipment Form, DD Form 1419, to the COR, PCO, and the DARPA Property Officer (DPO). The contractor shall submit on a quarterly basis or as-required a *Contractor Acquired Property Report* not later than the fifteenth of the month following the quarter being reported. The contractor shall recommend the format to the COR for approval before initial submission.

7. **INVESTIGATIONS AND INQUIRIES SUPPORT:** At the direction of DARPA SID staff, the contractor shall conduct inquiries and draft preliminary investigation reports relative to security violations and infractions, accidents, criminal acts, and counterintelligence activities. The contractor shall gather and record information relative to an event, and prepare a written report that will be submitted to the Director, SID, or his/her designee for concurrence/approval. The report shall clearly document the "who, what, where, when, and how" data elements that are critical to an investigation or inquiry and shall, in the case of classified information, contain the necessary information to prepare and submit a Damage Assessment in accordance with DoD Regulation 5200.1, Information Security. A database will be maintained to track progress on preparing these reports. This database will incorporate a capability to provide statistical reports and trend analysis reports involving security incidents and violations.

8. **SECURITY PROGRAM RECORDKEEPING AND STATISTICAL ANALYSIS REPORTS:** The contractor shall assist with establishing and sustaining a records system relative to the DARPA security program and the security work effort. The system shall comply with DoD records requirements, to include retention schedules, and with requirements mandated by the Privacy Act and the Freedom of Information Act, and other applicable law and regulation. The records shall be the property of DARPA and shall be available for inspection by DARPA representatives at any time. A document outlining the records system, to include the location of the records and the name of the custodian(s) of the records shall be provided to the COR initially within 30 days from contract award and subsequently as changes to the records system occur. The contractor shall, as directed, conduct various statistical analyses and provide various reports regarding the activities and efforts of the various functional areas.

9. **EXPERT SUPPORT TO THE CONTRACTOR:** The contractor shall, as necessary arrange for and provide personnel to support the performance of specialized tasks in support of the DARPA security program. It should be noted that the costs for these Experts relate to the Other Direct Costs (ODC) CLIN, which is intended to cover additional, "within scope" work that will be identified by the Government during thc contract performance.

10. **ANNUAL CLEAN-OUT PROCESS PLAN:** The contractor shall prepare and submit the *Annual Clean-Out Process Plan* within 180 days of contract start. The updates to the Plan shall be provided on an annual basis within 90 calendar days of the anniversary of the contract year.

11. **SECURITY CONTAINERS AND SECURITY AREA CONTROL STATISTICAL REPORTING:** The contractor shall prepare and submit *Security Containers and Security Area Control Statistical Reports* on an as-required basis or as changes occur.

12. **SPECIAL PROJECTS, STUDIES, ASSESSMENTS, AND ANALYSIS:** The contractor shall be required to support special projects, studies, assessments, and analysis on an as required basis. Special projects include such activities as security incident reporting, VIP visits and testing, Security personnel training effectiveness, feasibility studies, needs assessments, special courier, and transportation activities, etc., and other topics as requested by DARPA or SID management.

13. **SECURITY PROGRAM POLICY AND PROCEDURE DEVELOPMENT AND REVIEW:** The contractor shall remain current on DoD security policy and procedure documents and shall provide a written review on any new or revised policy and procedures that describes the potential impact to the SID security program and that recommends policies and procedures for application to the DARPA Security Program to assure compliance with regulatory guidance. Changes to or new DoD security policy documents shall be reviewed within 30 days of promulgation and brought to the attention of the Director, SID.

14. **EDUCATION AND TRAINING PRESENTATIONS:** The contractor shall develop and present security-oriented training and education classes, seminars, and workshops and maintain records and a database detailing student participation. Contractor staff assigned to the various functional areas within SID will be required to prepare and present various oral and/or written presentations, training, and reports relative to their functional area and their work activities. Presentations by the contractor shall use the most effective mix of written, oral, and audio/visual techniques and, where appropriate shall use computer based interactive training. The contractor shall reevaluate the training program during self-inspections and other oversight activities. The evaluation shall assess the quality, effectiveness, and appropriateness of the training program.

15. **NEWCOMER, INITIAL AND RECURRING INDOCTRINATION AND BRIEFING:** The contractor shall present all new DARPA employees and DARPA-badged contractors with an orientation on the procedures followed at DARPA in relation to security, in accordance with DoD Directives 5200.1, 5200.2, 5200.8, and the DARPA Security Manual. This orientation briefing shall outline at a minimum why security at DARPA is critical to their success; explain the SID directorate mission and organization; outline the security services that are provided; outline emergency and safety requirements, and highlight the individual's security responsibilities as a DARPA employee/contractor. The orientation training shall include, but not be limited to, addressing the threat and the techniques employed by foreign intelligence activities

attempting to obtain classified and sensitive unclassified information, and shall address issues or concerns identified during SID self-inspections and highlighted by the occurrence of security violations and infractions. Prior to newly assigned employees and contractors being granted access to classified information, the SID contractor shall assist the SID staff in ensuring that all persons granted a clearance shall have completed all documentation required and shall be scheduled to attend an initial indoctrination briefing. The contractor shall assist DARPA in conducting a termination briefing which shall be provided to all personnel upon termination of employment, administrative withdrawal of a security clearance, or contemplated absence from duty or employment from DARPA for 60 days or more. Individuals who are debriefed will be required to complete all documentation necessary, including but not limited to, the Security Debriefing Acknowledgment.

16. **AUTOMATED INFORMATION SYSTEM (AIS) INDOCTRINATION AND BRIEFING:** The contractor shall ensure that all personnel who are granted access to AIS are indoctrinated on their security responsibilities prior to gaining access to the system and at least annually thereafter. This indoctrination on security responsibilities will be documented via signed DARPA-employee/contractor agreements, copies of which will be maintained and updated, as required, while in individual has access to DARPA AIS.

17. **FOIA CASE REPORTS:** In addition to providing required FOIA case information to the OSD OFOI on cases referred to DARPA for processing, the DARPA FOIA office will compile periodic reports to the Director, SID, summarizing FOIA actions conducted. These periodic reports may include statistical data from the reports provided to OFOI, and should also include narrative data capturing problems, difficulties, or positive actions in the following listed areas that affected the operation of the FOIA section:

1) Logging cases;
2) Researching information;
3) Preparing forms;
4) Writing responses;
5) Redacting documents;
6) Duplicating required copies;
7) Notifying submitters;
8) Negotiating with submitters;
9) Annotating file with actions taken;
10) Making telephone calls;
11) Providing meeting minutes;
12) Writing and responding to e-mails;
13) Coordinating with Agents;
14) Coordinating with PMs and other DARPA support offices (SID, COMPT, CMO); and,
15) Closing out files.

18. **INVENTORY REPORTS:** The Contractor shall maintain a database that will allow computer tracking of property assigned to the project and shall provide an Initial *Inventory of* Government *Furnished Equipment (GFE)* thirty working days following the award of the contract. The contractor shall also provide an annual *Intermediate Inventory Report* of GFE 30

calendar days prior to the end of each contract year. The contractor shall recommend the format of the database to the COR for approval before initial submission. The contractor shall provide a *Final Inventory Report* of GFE, ten working days prior to the expiration of the last contract year, or at the direction of the Government.

SECTION 6 - APPLICABLE DOCUMENTS/FORMS

1. U.S.C., Title 5, Section 552, As Amended By Public Law No. 104-231, 110 Stat. 3048 , The Freedom of Information Act
2. U.S.C., Title 5, Section 552a, As Amended, The Privacy Act of 1974
3. U.S.C, Title 10, Section 119, SAPs; Congressional Oversight
4. U.S.C., Title 50, War and National Defense, Chapter 15, National Security
5. Executive Order 12968, Access to Classified Information, 4 Aug, 95
6. Executive Order 13526, National Security Information, 29 Dec 09
7. National Security Decision Directive (NSDD) 298, Operations Security, January 22, 1988
8. National Archives and Records Administration, Information Security Oversight Office (ISOO), Directive No. 1, Classified National Security Information, 22 Sep03
9. DARPA Security Guide, 26 Feb 09
10. DoD Directive 2000.12, DoD Antiterrorism (AT) Program, 8 Aug 03
11. DoD Directive 5000.1, The Defense Acquisition Program, 12 May 03
12. DoD Directive 5200.1, DoD Information Security Program, 13 Dec 96
13. DoD Directive 5200.2, DoD Personnel Security Program, 9 Apr 99
14. DoD Directive 5205.02, DoD Operations Security Program, 6 Mar 06
15. DoD Directive 5205.07, SAP Policy, 5 Jan 06
16. DoD Directive 5210.48, Jan 25 07 Polygraph and Credibility Assessment Program, 25 Jan 07
17. DoD Directive 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 1 Dec 82
18. DoD Directive 8000.1, Management of DoD Information Enterprise, 2 Oct 09
19. DoD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 Apr 04
20. DoD Directive 8500.1E, Information Assurance (IA), 24 Oct 02
21. DoD Directive O-8530.1, Computer Network Defense (CND), 1 Aug 01
22. DoD Directive 8570.1, Information Assurance (IA) Training, Certification, and Workforce Management, 15 Aug 04
23. DoD Instruction 0-2000.16, DoD Anti-Terrorism Standards, , 2 Oct 06
24. DoD Instruction 5200.39 Critical Program Information (CPI) Protections within the Department of Defense, 16 Jul 08
25. DoD Instruction O-5205.11, Management, Administration, and Oversight of DoD SAPs, 1 Jul 97
26. DoD Instruction 5210.91, Polygraph and Credibility Assessment Procedures, 12 Aug 10
27. DoD Instruction 5240.5, DoD Technical Surveillance Countermeasures (TSCM) Survey Program, 22 Feb 06

28. DoD Instruction C-5240.08, Counterintelligence Security Classification Guide (U), 7 Dec 05
29. DoD Instruction 8410.02 NETOPS for the Global Information Grid (GIG), 19 Dec 08
30. DoD Instruction 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP) , 18 Nov 07
31. DoD Instruction O-8530.2, Support to CND, 9 Mar 01
32. DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM), 13 Aug 04
33. DoD 5200.1-PH, DoD Handbook for Writing Security Classification, November 1999
34. DoD Handbook O-2000.12H, DoD Antiterrorism Handbook, 1 Feb 04
35. DoD 5200.1-R, Information Security Program, January 1997
36. DoD 5200.2-R, Personnel Security Program, January 1987
37. DoD Regulation 5200.8, Physical Security Program, 9 Apr 07
38. DoD 5220.22-R, Industrial Security Program, December 1985
39. DoD Regulation 5400.7, DoD Freedom of Information (FOIA) Program, 4 Sep 98
40. DoD Regulation 5400.11, DoD Privacy Act Program, 14 May 07
41. DoD Manual 5105.21-M-l, Sensitive Compartmented Information (SCI) Administrative Security Manual, Aug 98
42. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 1 Feb 06
43. DoD 5220.22-M-Supl (NISPOM Supplement), 29 Dec 94
44. DoD Overprint to the National Industrial Security Program Operating Manual Supplement, DoD 5220.22-M Supl, Rev 1, 1 Apr 04
45. DoD S-5240.05-M-l, "The Conduct of Technical Surveillance Countermeasures, Volume 1 (U), 14 May 07
46. DoD S-5240.05-M-2, "The Conduct of Technical Surveillance Countermeasures, Volume 2 (U), 13 Nov 07
47. Department of Defense UG-2045-SHR, Physical Security Equipment Users Guide, current edition.
48. Department of State, International Traffic in Arms Regulations (ITAR)
49. Department of Commerce, Export Administration Regulations (EAR)
50. Director, Central Intelligence Directive (DCID) 6/2, Technical Surveillance Countermeasures
51. Director of Central Intelligence Directive, DCID 6/3, Protecting SCI within Information Systems, June 5, 1999
52. Director of Central Intelligence Directive, DCID 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to SCI, July 2, 1998
53. Director, Central Intelligence Directive (DCID) 6/9, Physical Security Standards for SCI Facilities
54. DNI Intelligence Community Directive (ICD) #704 - Personnel Security Standards and Procedures Governing Eligibility for Access to SCI and Other Controlled Access Program Information, effective 1 Oct 2008
55. DNI Intelligence Community Policy Guidance (ICGP) #704.2 – Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to SCI and other Controlled Access Program Information, effective 2 Oct 2008.
56. Joint Air Force Army Navy Manual, JAFAN 6/0, SAP Security Manual, 20 Dec, 07

57. Joint Air Force Army Navy Manual, JAFAN 6/3, Protecting SAP Information Within Information Systems, October 15, 2004
58. Joint Air Force Army Navy Manual, JAFAN 6/4, SAP Tier Review Process, Revision 1, May 9, 2006
59. Joint Air Force Army Navy Manual, JAFAN 6/9, Physical Security Standards for SAP Facilities, March 23, 2004 with SAP issued Change 1 – December 20, 2005
60. Title 41, Code of Federal Regulations, Chapter 101, Federal Property Management Regulations
61. Defense Technical Information Center, Militarily Critical Technologies List (MCTL) http://www.dtic.mil/mctl/
62. NSTISSI 4000, National Security Telecommunications and Information Systems Security Instruction Communications Security Equipment Maintenance and Maintenance Training
63. Federal Standard 809 (FED-STD-809), Neutralization and Repair of GSA Approved Containers, dated April 1, 1998.)
64. DD Form 254 – DoD Contract Security Classification Specification
65. DD Form 441 – Security Agreement
66. DD Form 441-1 – Appendage to Security Agreement
67. DD Form 1540 – Registration for Scientific and Technical Information Services
68. DD Form 1847 – SCI Indoctrination Memorandum
69. DD Form 1847-1 – SCI Nondisclosure Agreement
70. DD Form 1848 – SCI Debriefing Memorandum
71. DD Form 1879 – Request for Personnel Security Investigation
72. DD Form 2024 – DoD Security Classification Guide Data Elements
73. DD Form 2056 – Telephone Monitoring Notification Decal
74. DD Form 2835, Program Access Request
75. DD Form 2836, SAP Indoctrination Agreement
76. DD Form 2501 – Courier Authorization
77. Defense Industrial Security Clearance Office, DIS FL 381-R – Letter of Notification of Facility Security Clearance
78. Defense Industrial Security Clearance Office, DISCO Form 2 – Request for Forms
79. Defense Industrial Security Clearance Office, DISCO Form 560 – Letter of Consent
80. Department of Justice, Federal Bureau of Investigation, FD Form 258 – Applicant Fingerprint Card
81. SF 85 – Questionnaire for Non-Sensitive Positions
82. SF 85P – Questionnaire for Public Trust Positions
83. SF 85P-S Supplemental Questionnaire for Selected Positions
84. SF 86 – Questionnaire for National Security Positions
85. SF 86C Standard Form 86 Certification
86. SF 87 – Fingerprint Card
87. SF 153 – COMSEC Material Report
88. SF 311 – Agency Information Security Program Data
89. Defense Courier Service, DCS Form 1 – Defense Courier Service Receipt for Material
90. Defense Courier Service DCS Form 10 – Defense Courier Service Authorization Record
91. OF 79 – Request for Security Clearance
92. Defense Security Service, DSS Form 147 – Record of Controlled Area
93. Department of State Form DSP-94, "Authority to Export Defense Articles Sold Under the Foreign Military Sales Program"

94. Department of State Form DSP-83, "Non-Transfer and Use Certificate"
95. Department of State Form DSP-119, "Application for Amendment to License for Export/Import of Defense Articles"
96. SAP Format 1- JFAN Edition, Program Access Request
97. SAP Format 2- JFAN Edition, SAP Indoctrination Agreement
98. DSS Security Professional Education Development (SPED)

ACRONYMS & ABBREVIATIONS

ADA – Americans with Disabilities Act

AFOSI – Air Force Office of Special Investigations

AFRL – Air Force Research Laboratory

AIS – Automated Information System

APACS – Aircraft and Personnel Automated Clearance system

AT – Anti-terrorism

AT/FP – Anti-terrorism / Force Protection

AT&L/IC – Acquisition, Technology & Logistics/International Cooperation

BAA – Broad Agency Announcement

CBRNE – Chemical, Biological, Radiological, Nuclear, and Explosives

CCI – Controlled Cryptographic Item

CCIR – Commander's Critical Information Requirements

CCTV – Closed Circuit Television

CDR – (DARPA) Classified Document Registry

CFIUS – Committee on Foreign Investment in the United States

CI – Counterintelligence / Critical Information

CJ – Commodity Jurisdiction

CM - Countermeasures

CND – Computer Network Defense

CNWDI – Critical Nuclear Weapons Design Information

COG – Continuity of Government

COMSEC – Communications Security

CONUS – Continental United States

COOP – Continuity of Operations Plan

COR -- Contracting Officer's Representative

CPI – Critical Program Information

CTTA – Certified TEMPEST Technical Authority

CUI – Controlled Unclassified Information

DAA – Designated Approval Authority

DARPA – Defense Advanced Research Projects Agency

DCC – Document Control Center

DCID – Director, Central Intelligence Directive

DIACAP – DoD Information Assurance and Accreditation Process

DMS – Defense Message System

DNI – Director, National Intelligence

DoA – Department of the Army

DoD – Department of Defense

DoDGARS – DoD Grant and Agreements System

DPEP – Defense Personnel Exchange Program

DPO – DARPA Property Officer

DSS – Defense Security Service

DSSA – Defense Security Service Academy

DTIRP – Defense Treaty Readiness Program

DTS – Defense Travel System

EAR – Export Administration Regulations

EDTS – Electronic Data Transfer System

EEFI – Essential Elements of Friendly Information

EEOC – Equal Employment Opportunity Commission

E-FOIA – Electronic-Freedom of Information Act

EM – Engineering Management

EPPA – Employee Polygraph Protection Act

FAL – Functional Area Lead

FAR – Federal Acquisition Regulations

FCL – Facility Clearance Level

FOCI – Foreign Ownership, Control, or Influence

FOIA – Freedom of Information Act

FOUO – For Official Use Only

FRD – Formerly Restricted Data

FSO – Facility Security Officer

HUMINT – Human Intelligence

IA – Information Assurance

IC – Intelligence Community

ICD – Intelligence Community Directive

IDS – Intrusion Detection System

IOSS – Interagency OPSEC Support Staff

IPT – Integrated Product Team

IR – Incident Report

ISOPREP – Isolated Personnel Program

ISSM – Information Security System Manager

ISSO – Information System Security Officer

IT – Information Technology

ITAR – International Traffic in Arms Regulation

ITC – Interagency Training Center

IVP – International Visit Program

JIT – Just-in-Time

JPAS – Joint Personnel Adjudication System

JWICS – Joint World-wide Intelligence Communications System

LO/CLO – Low Observable/Counter Low Observable

MASINT – Measurement and Signature Intelligence

MOA – Memorandum of Agreement

NACLC – National Agency Check with Local Agency Check and Credit Check

NCIS – Naval Criminal Investigative Service

NDP – National Disclosure Plan

NID – National Interest Determination

NIPO – Navy International Program Office

NISPOM – National Industrial Security Program Operating Manual

ODC – Other Direct Costs

OFOI – Office of Freedom of Information

ONR – Office of Naval Research

OPSEC – Operations Security

OSD – Office of the Secretary of Defense

OUSD(AT&L) – Office of the Undersecretary of Defense (Acquisition, Technology and Logistics)

PA – Project Agreement

PDR – Preliminary Design Review

PDS – Practices Dangerous to Security

PHOTINT – Photographic Intelligence

PIR – Priority Intelligence Requirements

POAM – Program of Action and Milestones

PPP – Program Protection Plan

PPSM – Ports, Protocols, and Services Management

PSI – Program System Instructions

PSO – Program Security Officer

PSQ – Personnel Security Questionnaire

PSR – Program Security Representative

QC – Quality Check

RAD – Request for Authorization to Develop and Negotiate

RD – Restricted Data

RDT&E/S&T – Research, Development, Test and Evaluation / Science and Technology

RFI – Request for Information

RFP – Request for Proposal

RPA – Request for Final Approval

SAF/IA – Office of the Undersecretary of the Air Force for International Affairs

SAP – Special Access Program

SAPCO Special Access Program Central Office

SCC – Security Control Center

SCG – Security Classification Guide

SCI – Sensitive Compartmented Information

SCIF – Sensitive Compartmented Information Facility

SETA – Systems Engineering and Technical Assistance

SI – Security Instructions

SID – Security and Intelligence Directorate (DARPA)

SIGINT – Signals Intelligence

SIPRNet – Secret Internet Protocol Network

SME – Subject Matter Expert

SOP – Standard Operating Procedure

SOW – Statement of Work

SPAN – Security Policy Automated Network

SSA – Special Security Agreement

SSAA – System Security Authorization Agreement

SSBI – Single Scope Background Investigation

SSO – Special Security Office / Support Services Office (DARPA)

SSOI – Summary Statement of Intent

SSP – System Security Plan

TAA – Technical Assistance Agreement

TCP – Transmission Control Protocol

TSCM – Technical Surveillance Countermeasures

TSIMG – Technical Surveillance Integrated Management Group

TSWA – Temporary Secure Work Area

TSWG – Technical Support Working Group

USPS – United States Postal Service

VCC – Visitor Control Center

VTC – Video Teleconferencing