

Performance Work Statement (PWS) For
MODIFICATION TO ACQUISITION PACKAGE J8-09-0059
GENERAL ANALYTIC, WARGAMING, AND TECHNICAL SUPPORT SERVICES

J8 SAGD Analytical On-site Support
Technical Instruction #3

Date: 12 August 2009
Prepared By: Mr. Paul Balash III

GENERAL INFORMATION

Description of Services

Introduction

The purpose of this requirement is to acquire Contractor Advisory and Assistance Service (CAAS) for J8 Studies, Analysis, and Gaming Division (SAGD). SAGD anticipates a continued requirement for a minimum of two contractor personnel; one analyst assistant to provide on-site analytical support for gaming facility administration, security and facility support, and one operational research analyst to provide on-site analytical support during development, planning, execution and assessment (post-execution activities) of studies, war games, seminars, workshops and analyses. Some of the more recent gaming efforts requiring contractor on-site support were gaming and facilitation efforts in support of Operational Availability (OA-08) and (OA-09), Irregular Warfare-3 war game, Mobility Capabilities Requirements Study (MCRS), New Administration Transition Team, Special CJCS-series of table top exercises, and the Quadrennial Defense Review 2010. These efforts are anticipated to continue on a recurring frequency concurrent with the continued high level of operational commitments worldwide.

More sensitive gaming events for both domestic and overseas contingency operations dictate that facilitation and gaming support contractors are cleared for ACCM level of security.

Scope

The contractor shall provide all personnel staffing necessary to perform the tasks as defined in this TI. The contractor shall perform to the standards in this TI. In this effort, the contractor shall provide strictly non-personal services and shall work as an independent contractor not subject to supervision and control by the Government.

General Information

Period of Performance

The period of performance for Task Descriptions within sections 1.1 and 1.2 shall commence upon the Date of Award.

The period of performance for Task Descriptions within sections 1.3 and 1.4 shall commence on 1 October 2009.

Place of Performance

The primary place of performance for this effort is J8 SAGD, Room ME800, The Pentagon.

Travel

Travel for this effort is not anticipated. However, if travel is required, all travel shall be conducted in accordance with FAR 31.205-46 Travel Costs and the Joint Travel Regulations (JTR) and shall be pre-approved by the COR.

Location / Duration / Number of Trips / Number of Persons

NA

Security Requirements

Clearance Level

TS/SCI: Operational Research Analyst contractor person shall possess a current Top Secret (TS) Clearance based on a Single Scope Background Investigation (SSBI) completed within the last 5 years with Sensitive Compartmented Information (SCI) eligibility. TS: Analyst Assistant contractor person shall possess a current Top Secret (TS) Clearance based on a Single Scope Background Investigation (SSBI) completed within the last 5 years.

Designated Focal Point Programs/Alternative Compensatory Control Measures (ACCM) must comply with current and appropriate Program Security Plan (PSP) and Security Classification Guide (SCG).

TASK DESCRIPTIONS

1.0 Task Description

Reference Strategic Contract GENERAL ANALYTIC, WARGAMING, AND TECHNICAL SUPPORT SERVICES PWS, Section 4.4.2, Specific Analytic, Assessment, and Technical Support Requirements. Conduct operational support of programmed studies, quick-reaction analyses, responses to Joint Staff actions, and other tasks. This support shall include: development of reports, briefs, and graphs; maintenance of files.

1.1 Schedule

1.1.1 Program Management Support

The contractor shall assist in providing technical program management support to the Government. Additionally, the contractor shall provide administrative and clerical assistance to support the work performed under this Technical Instruction Performance Work Statement. The contractor shall provide program operational support and business operations services in support of various programs' day-to-day operations and missions. The contractor shall provide program coordination support for the development and coordination of program related assessments, studies, reports, and strategies explained within this Technical Instruction. The contractor shall support business operations to achieve office functionality, process, and control. This includes schedule management, quality control and coordination of documents, establishing business process procedures, and resource management.

1.1.2 Kick-Off Meeting

The contractor shall schedule and conduct a joint Government, contractor kick-off meeting to review PWS requirements.

1.1.3 Project Schedule

The contractor shall deliver and maintain an integrated project schedule using Microsoft Project or other Government approved media that shows all resource-loaded tasks through Level 2, durations, dependencies, and deliverables.

1.2 Cost Reporting

1.2.1 Expenditures

The contractor shall provide cost reporting to the TOM. The reporting shall provide technical, schedule, and fiscal status by comparing planned versus actual expenditures.

1.2.2 Problems and Shortfalls

The reporting shall also be used to identify potential problems. The contractor shall identify any anticipated technical or funding shortfall or irregularity during the specified period of performance, in writing, not later than four (4) months prior to the anticipated shortfall.

1.3 Quality

1.3.1 Quality Control Plan

The contractor shall implement a Quality Control Program for this effort. The contractor shall prepare and provide a Quality Control Plan that detail and describes the contractor's framework and processes for delivering quality

products and services required by the tasks in this TI. The contractor shall implement a Quality Control Program to ensure all work will be performed in accordance with the contract requirements. The contractor shall provide the requisite staffing and procedures to meet the quality, quantity, timeliness, responsiveness, customer satisfaction, and service delivery and performance requirements of this effort. The contractor shall identify in the Quality Control Plan, the applicable processes and metrics used to self-assess performance, in addition to the resources to be applied to this effort.

1.4 Technical

Reference Strategic Contract GENERAL ANALYTIC, WARGAMING, AND TECHNICAL SUPPORT SERVICES PWS, Section 4.4.2, Specific Analytic, Assessment, and Technical Support Requirements. Conduct operational support of programmed studies, quick-reaction analyses, responses to Joint Staff actions, and other tasks. This support shall include: development of reports, briefs, and graphs; maintenance of files.

1.4.1 Monthly Progress Reports

Reference Strategic Contract GENERAL ANALYTIC, WARGAMING, AND TECHNICAL SUPPORT SERVICES PWS, Section 4.4.1, Monthly Progress Reports. The contractor shall submit monthly progress reports delivered in a format and/or media approved by the TPOC. Electronic media shall be used whenever practical. First Monthly Progress Report due NLT 15 days after the first full reporting month. Subsequent reports are due NLT 15 days after the last day of each calendar month. These managerial reports shall include the following elements:

- Contractor's name and address
- Contract number and SubCLIN number
- Date of report
- Period covered by report
- Man hours expended by discipline for the reporting period, and cumulatively during the contract
- Cost curves portraying actual/projected conditions through the technical instruction when appropriate
- Cost incurred for the reporting period and total contractual expenditures as of report date
- Description of progress made during period reported, including problem areas encountered and recommendations, if any for subsequent solution beyond the scope of this contract
- Trips and significant results
- Plans and recommendations for activities during the following period
- Problems encountered
- Contractor performance assessment

All reports resulting from this contract shall contain the following disclaimer statement on the report cover , "The views, opinions and findings, contained in this report are those of the author(s) and should not be construed as an official Department of Defense (DoD) position, policy, or decision, unless so designated by other official documentation."

1.4.2 Technical Reports

Reference Strategic Contract GENERAL ANALYTIC, WARGAMING, AND TECHNICAL SUPPORT SERVICES PWS, Task Section 4.4.3, Additional Reporting Requirements. The contractor shall provide a listing keyed to specific tasks identifying the minimum reporting deliverables associated with each task. Deliverable: All efforts applied to the functions listed above shall be documented in a detailed Monthly Technical Report. Supporting briefs, recommendations, and database updates shall be provided to the Government and documented in the technical report. The technical report shall contain enough detail so it will stand alone as a useful tool for the Government to utilize in the acquisition process, while also fully documenting the value added by the contractor's efforts. Reporting should be in sufficient detail and of a quality to meet standards and will include, but not be limited to:

- Technical reports, data compilations, program master schedule, evaluations, and analyses
- Testing procedures, requirements, assessments, calibrations, and schedules
- Specifications, tabulations, engineering drawings, multi-media graphics, designs, concepts, diagrams, and circuits

- Life-cycle maintenance requirements, guidelines, schedules, procedures, instructions, corrective actions, etc.
- Conference agenda, conference minutes, and presentation materials
- Purchase descriptions, proposals, equipment illustrations, program planning, support, and budget documentation and funding plans

All reports resulting from this contract shall contain the following disclaimer statement on the report cover , “The views, opinions and findings, contained in this report are those of the author(s) and should not be construed as an official Department of Defense (DoD) position, policy, or decision, unless so designated by other official documentation.”

1.4.3 Administration

The contractor shall provide full-time, on-site technical and administrative analytical support (security and gaming center (ME800) support).

1.4.3.1 Security

The contractor shall support the management and execution of ME800 access control for authorized personnel; shall ensure all visitors are properly escorted when inside ME800 including office/gaming room spaces; and shall comply with applicable Government, Joint Staff and SAGD security procedures and Standing Operating Procedures (SOPs).

1.4.3.2 Office Administration

The contractor shall support the management and execution of SAGD administrative activities and functions to ensure compliance with applicable Joint Staff instructions and SOPs. The contractor shall evaluate and provide recommendations on the organization, methods and procedures for providing administrative support under purview of SAGD as well as conducting analysis by researching and investigating new or improved best business and administrative management practices for potential application to SAGD operations. The contractor shall also support the improvement and simplification of SAGD administrative reporting requirements.

1.4.3.3 Facility Support

The contractor shall support the planning, scheduling, maintenance, and management of SAGD (ME800) gaming rooms. The contractor shall communicate with users to process requests, coordinate, and schedule meetings, games, workshops and seminars; shall maintain necessary calendars, logs, records and files; shall provide end-user support. The contractor shall analyze facility usage and maintenance trends to support and assist the SAGD Division Chief and Deputy Chief’s evaluation and determination of current and future requirements.

1.4.3.4 Video-Teleconferencing (VTC) Support

The contractor shall support the planning, scheduling, maintenance, and management of SAGD (ME800) VTC capabilities. The contractor shall communicate with users to coordinate up to 20 VTCs per month; shall maintain necessary calendars, logs, records and files; and shall provide end-user support. The contractor shall monitor and document VTC usage and maintenance trends to support and assist the SAGD Division Chief and Deputy Chief’s evaluation and determination of current and future requirements. Contractor personnel shall maintain VTC training and credentials in accordance with DISA Defense Video Services training policy document of 5 April 2005.

1.4.4 Support for On-going and Future Analyses and Gaming Efforts

The contractor shall provide full-time, on-site analytical support during planning, development, execution, and post-execution of war games, seminars, workshops and analyses.

1.4.4.1 Planning, Development and Preparation

The contractor shall support the Division Chief, Deputy Chief, game directors and action officers in all required tasks to plan, develop and prepare for war games, seminars, workshops and analyses activities by participating in initial planning meetings to analyze the task and evaluate the range of analysis; recommend possible courses of action and methodologies; assist in the definition and integration of objectives; assist in determining data requirements and in developing effective ways of displaying and manipulating that data; and assisting in developing and producing game, seminar, workshop, or event materials e.g., agendas, data sheets, briefing slides, rosters and read-aheads.

1.4.4.2 Execution

The contractor shall support the Division Chief, Deputy Chief, game directors and action officers in all required tasks to execute assigned war games, seminars, workshops and analyses activities by refining or modifying attendee lists, verifying security clearances, and developing participant rosters; refining briefings, visual aids required for event execution; and assist in capturing usable data from these events, analyzing the data, and synthesizing it into material for SAGD and senior leader review.

1.4.4.3 Assessments

The contractor shall support the Division Chief, Deputy Chief, game directors and action officers in all required post-execution tasks for executed war games, seminars, workshops by gathering key insights and observations and packaging this information in a draft game report or out briefing; participating in the after action review and analysis of the data; assisting in writing final game reports, coordinating with the participating organizations, and finalizing the report for game sponsor concurrence; and development of post-game compilation of data, notes, briefs and game reports.

1.4.4.4 Studies, Analyses and Evaluation Support

The contractor shall evaluate, research, study, appraise, and analyze, historic and topical information in order to provide recommendations to the Division Chief, Deputy Chief, game directors and action officers during the planning, development, execution and post-execution of war games, seminars, workshops and analyses activities occurring approximately one to two times per month. The contractor shall participate in SAGD after-action-reviews; analyze game design, methodology, effectiveness, and outcomes; and develop recommendations for review by the Division Chief, Deputy Chief, and game directors.

1.4.4.5 Create or Update Official Information

The contractor shall create or update official information (OI) using Joint Staff approved OI transfer tools, e.g., wikis, blogs, chats, and email in support of SAGD mission requirements.

PERFORMANCE REQUIREMENTS SUMMARY

Task Paragraph	Tasks	Delivery Date	Performance Standard
1.1	Schedule		
1.1.2	Schedule and conduct a contract kick-off meeting.	DOA + 10 Days	One Time
1.1.3	Deliver and maintain an integrated project schedule using a Government approved media that shows all tasks, both recurring and unscheduled, through the duration of the period of performance	DOA + 10 Days (initial). By the 10 th day of each month thereafter.	Monthly (updated with each monthly report)
1.3	Quality		
1.3.1	Prepare and provide a Quality Control Plan	DOA + 10 Days	One Time
1.4	Technical		
1.1.1 1.4.1	Monthly Progress Reports that contain required information specified in the strategic contract	By the 15 th day of each month.	Updated monthly
1.1.1 1.4.2	Technical Reports – To include, at a minimum, monthly updates for tasks included in sections 1.4.3 through 1.4.4 of this TI.	By the 15 th day of each month. By the 15 th day of each month.	Updated monthly
1.4.3	Accomplish administrative support tasks	Daily as documented in a daily log included in the monthly technical report.	Updated monthly in the technical report (1.4.2)

1.4.4	Accomplish analytical support tasks for on-going and future analyses and gaming efforts	Daily as documented in a daily log included in the monthly technical report.	Updated monthly in the technical report (1.4.2)
--------------	---	--	---

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING			
				a. FACILITY CLEARANCE REQUIRED Top Secret			
				b. LEVEL OF SAFEGUARDING REQUIRED None			
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>			3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>				
<input checked="" type="checkbox"/>	a. PRIME CONTRACT NUMBER N00178-08-D-5318-FG01 (TI #3)			a. ORIGINAL <i>(Complete date in all cases)</i>	DATE (YYYYMMDD) 20090828		
	b. SUBCONTRACT NUMBER		<input checked="" type="checkbox"/>	b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO. 3 DATE (YYYYMMDD) 20100305		
<input checked="" type="checkbox"/>	c. SOLICITATION OR OTHER NUMBER J8-09-0059	DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 5 in all cases)</i>	DATE (YYYYMMDD)		
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.							
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____							
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>							
a. NAME, ADDRESS, AND ZIP CODE ADDX 4900 Seminary Road Alexandria, VA 22311		b. CAGE CODE 1XPA3	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> Defense Security Services (IOFCK2) 241 18th Street South Suite 100A Arlington, VA 22202				
7. SUBCONTRACTOR							
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>				
8. ACTUAL PERFORMANCE							
a. LOCATION Joint Staff J-8 SAGD 8000 JS Pentagon Room ME800 Washington, D.C. 20318-8000		b. CAGE CODE N/A	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> Joint Staff Security Office, Personnel Security Room 2D819 9300 Joint Staff Pentagon Washington, DC 20318-9300				
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT J8 SAGD Analytical On-site Support (Technical Instruction #3)							
10. CONTRACTOR WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			<input checked="" type="checkbox"/>	a. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		<input checked="" type="checkbox"/>	
b. RESTRICTED DATA			<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY			<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL			<input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA			<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE			<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION			<input checked="" type="checkbox"/>	e. PERFORM SERVICES ONLY			<input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)		<input checked="" type="checkbox"/>		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES			<input checked="" type="checkbox"/>
(2) Non-SCI		<input checked="" type="checkbox"/>		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER			<input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION			<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT			<input checked="" type="checkbox"/>
g. NATO INFORMATION			<input checked="" type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS			<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION			<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS			<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION			<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE			<input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION		<input checked="" type="checkbox"/>		l. OTHER <i>(Specify)</i>		<input checked="" type="checkbox"/>	
k. OTHER <i>(Specify)</i> See Block 13 ACCM		<input checked="" type="checkbox"/>		See Block 13			

12. PUBLIC RELEASE. Any information (*classified or unclassified*) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (*Specify*)

Director, Joint Staff, ATTN: OCJCS/PA, 4000 JS Pentagon, Washington, DC 20318-4000

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (*Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*)

10e(1). TS/SCI: Operational Research Analyst contractor person shall possess a current Top Secret (TS) Clearance based on a Single Scope Background Investigation (SSBI) completed within the last 5 years with Sensitive Compartmented Information (SCI) eligibility. See SCI Addendum.

10e(2). TS: Analyst Assistant contractor person shall possess a current Top Secret (TS) Clearance based on a Single Scope Background Investigation (SSBI) completed within the last 5 years. See NATO Addendum.

10g. Contractor may require access to North Atlantic Treaty Organization (NATO) Top Secret information for reference only at Joint Staff. This means information belonging to, and circulated by, NATO. Special briefings required for access to NATO. Prior approval of the contracting activity is required for subcontracting. Access to classified NATO information requires a final U.S. Government clearance at the appropriate level and special briefings. If contractor is read into ATOMAL, an annual re-brief is required. (NISPOM Chapter 10, Section 7, Para 10-706)

10j. FOUO Information under this contract shall be safeguarded as specified in DOD 5400.7R "Protecting For Official Use Only Information."

10k. Contractor may require access to ACCM. Designated Focal Point Programs/Alternative Compensatory Control Measures (ACCM) must comply with current and appropriate. See ACCM Addendum


11a. Contract performance is restricted to Joint Staff J-8 SAGD, Room ME800, The Pentagon, Washington, D.C.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. Yes No
(*If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.*)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. Yes No
(*If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.*)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (<i>Include Area Code</i>)
Ms. Erika H. Langerman	Director, Joint Staff Security	(703) 614-0535

d. ADDRESS (<i>Include Zip Code</i>) Joint Staff Security Office Washington, DC 20318-9300 Phone: 703.614.0535	17. REQUIRED DISTRIBUTION	
	<input checked="" type="checkbox"/>	a. CONTRACTOR
e. SIGNATURE 	<input type="checkbox"/>	b. SUBCONTRACTOR
	<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
	<input type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
	<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY

JOINT STAFF ACCM/FP ADDENDUM (Block 13)

ACCM Security Requirements

Individuals working with ACCM/FPP will be required to have additional training on the handling and safeguarding of ACCM/FPP material and shall comply with the following:

1. All ACCM/FPP work will be done “onsite” at the government facility.
2. The contractor will safeguarding all ACCM/FPP information in accordance with CJCSM 3213.02C, 01 Feb 09, “Joint Staff Focal Point Program”:
 - a. Control Measures. Section 4.1 of Executive Order 12958 (reference a) mandates that organizations electronically processing FP information must have a system of control measures in place that ensure access to the information is limited to those with appropriate need-to-know base on a lawful and authorized purpose. Appendix A to this enclosure provides a sample of organizational actions to assist in maintaining the NTK requirement of FP material handled electronically.
 - (1) The FPPCO will coordinate identification of the authorized users for each FP program processed by the agency or organization. Access to FP information shall be limited to only those with a specific association with operational task, mission, or specific contract deliverable.
 - (2) FPPCO will coordinate with local Chief Information Officer (or equivalent Information Management System Administrator) for the establishment of protected folder(s) on a restricted hard drive for each FP Program active in the organization. Contractors will only store Focal Point information in the protected folders.
 - (a) Processing of all FP material, to include attachments from email or material hand carried on electronic storage media should be conducted using the specified protected folder(s) established for each FP program only.
 - (b) Users of AIS that can be subsequently accessed by other personnel should consider deleting any temporary files created prior to logging off the system. The FPPCO should consult with local system administrators and establish and/or promulgate local rules as required.
 - (c) FPPC will review and update on a regular basis the access authorizations and/or restrictions for each FP protected folder.

b. Access

- (1) A list of authorized users shall be maintained as an ACL, which will define the individuals or groups, granted access to FP information. ACLs will be maintained at both the program and local enclave-level. Program sponsors will publish a list of command, agency, or organization participants (designated FPPCOs for each specific FP program), disseminate that list to all participants and update the list as necessary to maintain positive control of material. At a minimum, participant lists will be updated and published at least semi-annually or more frequently as required. List dissemination will be via DMS message or SIPRNET email. The participant list shall be used to establish authorized DMS SPECAT/ACCM "PROGRAM NICKNAME" message and SIPRNET e-mail recipients.
- (2) THE FPPCO of each participating agency or organization shall maintain and routinely validate ACL, which will define the individuals or groups granted access to FP/ACCM information within the agency or organization (intra-enclave). Each FP/ACCM program will have a separate ACL; however some individuals may accessed to more than one program. The FPPCO for the designated program will be the owner of the ACL and will control additions and deletions of users. FPPCOs for separate FP programs may collate information into a centrally managed database provided each primary and alternate FPPCO are accessed into all the FP programs maintained in the collated list.
- (3) The ACL shall be used to grant access to information, establish protected electronic file folders, identify authorized e-mail senders and/or recipients, and to identify authorized DMS message senders and/or recipients. (The ACL meets the criteria for an authorized user list as required by reference b).
- (4) The FPPCO will audit the ACL on a quarterly basis to ensure no unauthorized modifications to the list.
- (5) A record of each ACL, and any changes, shall be maintained during the duration of the FP program and will be archived and filed with other program record when the programs is terminated.

JOINT STAFF INDUSTRIAL SECURITY ADDENDUM TO DD FORM 254 FOR SCI

1. All contractors must be eligible for or currently hold a **Top Secret clearance** in order to meet contractual security requirements.
2. Prospective contractor employees shall submit completed DD Form 1557 to the Joint Staff Security Office, Personnel Security Branch, no less than 30 days before the starting date of the contract or 30 days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee or vendor.
3. The Contracting Officer's Technical Representative (COTR) is responsible for notifying the contracting company that the employee is eligible for SCI and can start working on the contract, or that the employee was denied SCI eligibility, and is ineligible for contract performance. **NOTE:** Joint Staff Security Office, Personnel Security Branch, will not be responsible for due process for contractors not meeting SCI criteria.
4. The Servicing Agency/FSO for the location where the work is to be performed must be notified of all terminations/resignations within five days of occurrence. (NOTE: The FSO will be responsible for due process). The contractor will return any expired identification cards and/or building passes, or those of terminated employees to the COTR. If identification card or building pass is not available to be returned, a report must be submitted to the COTR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card and reason for non-return. Report will be forwarded to the Joint Staff Security Office, Personnel Security Branch for review and accountability.
5. The contractor will report any adverse information coming to their attention to the Joint Staff Security Office, Personnel Security Branch (The subsequent termination of employment of an employee does not obviate the requirement to submit the report).
6. The recipient will afford the information a material degree of protection equivalent to that afforded it by the releasing government. The National Industrial Security Program DOD 5220.22M shall govern security Classification(s).
7. Classified material generated under this contract must be assigned a security classification as specified by the classification of the source document used.
8. Classified ADP is authorized at the TOP SECRET level. Access to TOP SECRET SCI material is required.
9. Access to the Joint Staff Information Network (JSIN-C) requires the individual to be cleared for NATO Secret. Individuals with access to NATO Confidential information or higher must have a briefing in accordance with the United States

Security Authority for NATO Affairs Instruction I-69 (5100.55 Encl 2), "United States Implementation of NATO Security Procedures, Section VI". The briefing ensures individuals with access to NATO information are aware of pertinent security regulations for safeguarding NATO classified information and the consequences of negligent handling.

10. The Contractor's Facility Security Officer (FSO) will provide a copy of the briefing certification using the format in USSAN 1-69, section VII, along with the visit request to the Joint Staff. All individuals with access to JSIN require a Joint Staff entry badge and verification of the NATO Briefing prior to access. JSIN access requests cannot be processed until the Contractor's Facility Security Officer (FSO) presents the required documentation.

11. Within 30 days of arrival to the Joint Staff, the contractor is required to attend Security Indoctrination Blocks of the Joint Staff Training Program, if they have not previously attended.

12. All abstracts, cards, computer tapes, and other classified material containing information extracted from information provided to the contractor will be maintained, controlled, handled, safeguarded, transmitted, and accounted for in accordance with the provisions of the National Industrial Security Manual (NISPOM).

13. The contractor may require access to TOP SECRET SCI material in this contract. Any material generated under this contract which contains information obtained or extracted from other classified material will be assigned the classification and group category of the extracted or obtained information. Proper clearance, safeguarding, capability, and need-to-know must be established by a requester before any classified material can be transmitted to him in accordance with provisions of the NISPOM.

14. Contractor not authorized to destroy classified materials.

JOINT STAFF INDUSTRIAL SECURITY ADDENDUM (Block 13)

1. Contractors who will work on-site at the Joint Staff must be eligible for or currently hold a **Top Secret clearance** in order to meet contractual security requirements.
2. Prospective contractor employees shall submit completed DD Form 1557 to the Joint Staff Security Office, Personnel Security Branch, no less than 30 days before the starting date of the contract or 30 days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee or vendor.
3. The Servicing Agency for the location where the work is to be performed must be notified of all terminations/resignations within five days of occurrence. The contractor will return any expired identification cards and/or building passes, or those of terminated employees to the COTR. If identification card of building pass is not available to be returned, a report must be submitted to the COTR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card and reason for non-return. Report will be forwarded to the Joint Staff Security Office, Personnel Security Branch for review and accountability.
5. The contractor will report any adverse information coming to their attention to the Joint Staff Security Office, Personnel Security Branch (The subsequent termination of employment of an employee does not obviate the requirement to submit the report).
6. The recipient will afford the information a material degree of protection equivalent to that afforded it by the releasing government. The National Industrial Security Program DOD 5220.22M shall govern security Classification(s).
7. Classified material generated under this contract must be assigned a security classification as specified by the classification of the source document used.
8. Classified computer processing is authorized at the **TOP SECRET**. Access to **TOP SECRET** material is required.
9. Access to the Joint Staff Information Network (JSIN-C) requires the individual to be cleared for NATO Secret. Individuals with access to NATO Confidential information or higher must have a briefing in accordance with the United States Security Authority for NATO Affairs Instruction I-69 (5100.55 Encl 2), "United States Implementation of NATO Security Procedures, Section VI". The briefing ensures individuals with access to NATO information are aware of pertinent security regulations for safeguarding NATO classified information and the consequences of negligent handling.
10. The Contractor's Facility Security Officer (FSO) will provide a copy of the briefing certification using the format in USSAN I-69, section VII, along with the visit request to the Joint Staff. All individuals with access to JSIN require a Joint Staff entry badge and verification of the NATO Briefing prior to access. JSIN access requests cannot be

processed until the Contractor's Facility Security Officer (FSO) presents the required documentation.

11. Within 30 days of arrival to the Joint Staff, the contractor is required to attend Security Indoctrination Blocks of the Joint Staff Training Program, if they have not previously attended.

12. All abstracts, cards, computer tapes, and other classified material containing information extracted from information provided to the contractor will be maintained, controlled, handled, safeguarded, transmitted, and accounted for in accordance with the provisions of the National Industrial Security Manual (NISPOM).

13. The contractor may require access to classified up to **TOP SECRET** material in this contract. Any material generated under this contract which contains information obtained or extracted from other classified material will be assigned the classification and group category of the extracted or obtained information. Proper clearance, safeguarding, capability, and need-to-know must be established by a requester before any classified material can be transmitted to him by the Center in accordance with provisions of the NISPOM.

14. Contractor not authorized to destroy classified materials.