DATA ITEM DESCRIPTION

Title:F/A-18 - EA-18 Aircraft / System Program Protection Implementation Plan

Number: DI-MGMT-81826 **Approval Date: 20100716**
AMSC Number: N9153 **Limitation: N/A**
DTIC Applicable: N/A **GIDEP Applicable: N/A**
Office of Primary Responsibility: AS/PEO (T) PMA265 / AIR-7.4.3
Applicable Forms: N/A

Use/relationship: The Contractors F/A-18 (All Series) and EA-18G Program Protection Implementation shall be defined within the F/A-18 - EA-18 Aircraft / System Contractors Program Protection Implementation Plan (PPIP) which is a result of the program protection requirements set forth in the DD-254, Statement of Work (SOW), DoD Contract, the Government's F/A-18 E/F and EA-18G Program Protection Plan (PPP) (including Annexes)) most current issuance, the Security Guidance for F/A-18 Hornet (All Series) and the EA-18G Growler Aircraft / Systems and Security Classification Guide for the F/A-18 (All Series) and EA-18G.

This Data Item Description (DID) contains the format, content, and intended information for the data product resulting from the work task described in the contract SOW.

Requirements:
1. Reference Documents:

The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions, shall be as available at the time of the solicitation.

The contractor is required to utilize the available databases for all updated/superseded amendments, notices and/or revisions of the reference documents identified below:

Note: For Reference Documents see:

- For OPNAV / SECNAV / Navy Documents see: http://doni.daps.dla.mil/default.aspx
- For NAVAIR Documents see: http://directives.navair.navy.mil/index.cfm?fuseaction=browse&foldertoopen=432393
- For MIL Documents see: http://assist.daps.dla.mil/quicksearch/
- For PMA / Classified Documents formally request from PCO / PMA265.

CJCSI 3312.01A	Joint Military Intelligence Requirements Certification (23 February 07)
CJCSI 6510.01E	Chairman of the Joint Chiefs of Instruction, Information Assurance (IA) and Computer Network Defense (CND) (15 Aug 07) (Directive current as of 12 Aug 08))
CJCSI 6211.02C	Chairman of the Joint Chiefs of Instruction, Defense Information System Network (DISN): Policy, Responsibilities and Processes (9 July 08)
CJCSI 6212.01E	Interoperability and Supportability of Information Technology and National Security Systems (Dec 08)
CJCSM 6510.01A	Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program) (24 June 09)
DoD 5200.1-M	Acquisition System Protection Program (16 Mar 94)
DoD 5200.1R	DoD Information Security Program (Certified current 24 Nov 03)

DoD 5205.02M	DoD OPSEC Program (3 Nov 08)
DoD 5220.22 M	National Industrial Security Program Operating Manual (NISPOM) (1 Feb 06)
DoDI 5000.02	Operation of the Defense Acquisition System (8 Dec 08)
DoDI 5200.01	DoD Information Security Program and Protection of Sensitive Compartmented Information (9 Oct 08) (cnx DoDD 5200.1)
DoDI 5200.39	Critical Program Information (CPI) Protection Within the Department of Defense (16 Jul 08)
DoDI 8500.2	Information Assurance (IA) Implementation (6 Feb 03)
DoDI 8510.01	DoD Information Assurance Certification and Accreditation Process (DIACAP) (28 Nov 07)
DoDI 8520.2	Public Key Infrastructure (PKI) Enabling (1 Apr 04)
DoDI 8580.1	Information Assurance (IA) in the Defense Acquisition System (9 Jul 04)
DoDD 5000.01	The Defense Acquisition System (12 May 03 Certified Current as of 20 Nov 2007)
DoDD 5205.02	DoD OPSEC Program (6 Mar 06)
DoDD 5230.09	Clearance of DoD Information for Public Release (22 Aug 08)
DoDD 5230.11	Disclosure of Classified Military Information to Foreign Governments and International Organizations (16 Jun 92)
DoDD 5230.20	Visits and Assignments of Foreign Nationals (22 Jun 05)
DoDD 5230.24	Distribution Statements on Technical Documents (18 Mar 87)
DoDD 5230.25	Withholding of Unclassified Technical Data From Public Disclosure (6 Nov 84 Incorporating Change 1, 18 Aug 95)
DoDD 8100.02	Use of Commercial Wireless Devises, Services and Technologies in the DoD Global Information Grid (14 Apr 04 Certified Current as of 27 Apr 07)
DoDD 8500.01E	Information Assurance (IA) (24 Oct 02 Certified Current as of 23 Apr 07)
DoDD 8570.01	Information Assurance Training, Certification, and Workforce Management (15 Aug 04 Certified Current as of April 23, 2007)
DoD S-5230.28	Low Observable (LO) and Counter Low Observable (CLO) Programs (U), CLASSIFIED DOCUMENT (26 May 05) Authorized users may contact the OPR identified below. (OPR: USD (AT&L), 703-697-0016)
EO 12958	CLASSIFIED NATIONAL SECURITY INFORMATION (17 Apr 95)
SECNAVINST 5239.3B	Department of the Navy Information Assurance (IA) Policy (17 June 09)
OPNAVINST 5239.3A	Navy Implementation of DoD Intelligence Information System Public Key Infrastructure (PKI) (18 Jan 08)
SECNAVINST 5510.36A	Department of the Navy (DoN) Information Security Program (ISP) Instruction (6 Oct 06)
SECNAV M- 5510.36	Department of the Navy (DoN) Information Security Program (6 Oct 06)
OPNAVINST 5513.2C	Security Classification Guide (SCG) (21 Jul 08) (Encl (02-26) for the

	F/A-18 Hornet (All Series) and Electronic Attack EA-18G Aircraft, (25 Jan 2010)
MCTL	The Military Critical Technologies List
MIL-STD-461F	DoD Interface Standard: Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment (Dec 07)
MIL-STD-464A	DoD Interface Standard: Electromagnetic Environmental Effects Requirements for Systems (19 Dec 02)
CNSS No. 7000	TEMPEST Countermeasures for Facilities (18 Jun 94) CLASSIFIED DOCUMENT (C)
NSTISSI 7001	NONSTOP Countermeasures (15 Jun 94) CLASSIFIED DOCUMENT (S NOFORN)
NSTISSI 1000	National Information Assurance Certification and Accreditation Process (NIACAP) (Apr 00)
NSDD 298	NATIONAL OPERATIONS SECURITY PROGRAM (22 Jan 88)
FISMA	Federal Information Security Management Act of 2002 (FISMA)
OMB A-130	Appendix III, Security of Federal Automated Information Resources (Circular No A-130)
Pub L. 104-106	Information Technology Management Reform Act Division E, (Clinger-Cohen Act)
Title 18	Section 1831 et seq of, Economic Espionage (Jan 08)

DoD Anti-Tamper Guidelines (available through the DoD Anti-Tamper website www.at.dod.mil)
Department of the Navy Anti-Tamper Desk Reference (available from DoN AT Office at anti.tamper@navy.mil)
The Defense Acquisition Guidebook (DAG) (Interim) Chapter 8 (15 Jun 09)
F/A-18E/F and EA-18G Program Protection Plan (PPP) (14 Mar 07) (PMA265)
Security Guidance F/A-18 Hornet (All Series) and the EA-18G Growler Aircraft / Systems, (6 Jan 10) (PMA265))

2. Format. The required document shall be in Contractor format:
   - The PPIP shall be used as a focal point for the Contractors Program Security. The PPIP is derived from the PPP and should not restate what is written in the PPP but simply state **"how"** the contractor will implement Program Protection.
   - The PPIP is used to identify and monitor how a Contractor develops and performs Program Protection activities during performance of the contract.

3. Content. The Contractors PPIP shall contain the following:
   - Security Management
   - Critical Program Information (CPI) / Critical Technologies (CT) / Critical Systems (CS)
   - Operational Security (OPSEC)
   - Information Assurance (IA)
   - A section detailing the Contractors approach to the PPIP
   - General methodologies that will be applied to the protection requirements
   - The Contactors process for identifying any existing / proposed CPI during developmental and RDT&E phases, and its protection / identification in the ECP process prior to ECP acceptance by the Government
   - A section describing an effective and efficient protection of CPI, CT and CS, which shall include the following:

- The Contractor's Security Management structure, including relationships with subcontractors and suppliers.
- An overview of all Contractors activities, operations, tests, and other associated activities to be undertaken in performance of the contract; identifying those in which classified information will manifest itself; identify the topics of the classification guide that specify the information that is classified; determine how, where, and when the classified information is embodied in the hardware, software or operations; determine what type access (visual, physical) permits knowledge of the classified information.
- Identification of the CPI physical locations under the Contractor's or its subcontractors' control and how the CPI is to be managed / tracked / secured throughout the CPIs life-cycle.
- Assess the vulnerability of the CPI to intelligence collection in the following areas: Human Intelligence (HUMINT), Open Source Intelligence (OSINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), and Computer Network Operations (CNO).
- Identify the planned countermeasures at each site where CPI is utilized / secured from the following security domains: Physical security; personnel security; telecom and network security, application, systems development, cryptography, and security architectures.
- Address any special handling procedures required for CPI, and procedures for recovering CPI in the event of a mishap; address these procedures for all phases of the program, including: Program / System Technology Development, System Development & Demonstration, RDT&E, Production Deployment, Operations, Maintenance, Logistics, Transportation, Training, and Disposal under this contract for which the Contractor has control.
- Describe the process that shall be used to assess new acquisitions (Incremental / Spiral upgrades, Engineering Change Proposal(s) (ECP's)) for CPI and CT.
- Describe how the Contractor shall comply with procedures for ensuring compliance with U.S. Government export statutes and regulations that affect CPI in a contracted program.
- Describe the Contractors procedures for public release of program information.
- The OPSEC portion of the PPIP shall include establishment of an OPSEC support capability that provides for program development, planning, training, assessment, surveys, and readiness training. Additionally the contractor shall include the results of the five-step OPSEC analysis Identifying CPI, Analyzing Threats, Analyzing Vulnerabilities, Assessing Risk, and Applying Countermeasures including those aspects of the foreign intelligence threat that are applicable to the specific contract. The following shall also be addressed:
  - General. Details of the OPSEC management concept to include contract identification, assignment of responsibilities, definition of milestones with target dates, provisions for continuous analysis, and how periodic revision as the contract activities evolve and become more specific and detailed.
  - Threat. The known threats to the contracting activity and include only that portion deemed applicable to the specific contract activities. The PPIP shall identify how these threats will be mitigated.
  - Sensitive Aspects of the Contract. An overview of all activities, operations, tests, etc. to be undertaken in performance of the contract; identifying those in which classified information will manifest itself; identify the topics of the classification guide that specify the information that is classified; determine how, where, and when the classified information is embodied in the hardware, software or

operations; determine what type access (visual, physical) permits knowledge of the classified information, what tools / equipment / capability are required, and the specific national defense advantage provided by that information if it is protected. Use of electromechanical equipment is an operation that shall be included, as are subcontracting, hardware-in-the-loop testing, calibration and check-out, fabrication, static tests, breadboard and brassboard fabrication and testing, and laboratory experiments. A list of critical information, based on the above analysis, shall include all the information considered essential to the success of the effort, and all the information that must be protected to preserve the military advantage potentially provided by the effort. Additionally, the list shall include all the activities, operations, and tests that could reveal the "critical" information to foreign intelligence.

- Vulnerabilities. The vulnerabilities derived by comparing identified threats to sensitive activities to determine which activities can be observed by foreign intelligence. "Observe" is defined to include all physical and chemical properties that can be noted and recorded by any type sensor. One such property is unintentional electromagnetic emanations, which may convey classified information. On this basis, TEMPEST is a part of OPSEC, and TEMPEST vulnerabilities shall be identified and mitigated.
- Countermeasures. The unacceptable risks of the vulnerabilities identified above shall include; the protective measures deemed appropriate to negate or reduce the potential damage to the project.

  - The categories of Potential Critical Information that shall be protected and planned for in the PPIP are:
    - Current and Future Operations
    - Travel Itineraries
    - Usernames and Passwords
    - Access / Identification Cards
    - Operations Planning Information
    - Personal Identification Information
    - Entry / Exit (Security) Procedures
    - Capabilities and Limitations
    - Address and Phone Lists
    - Budget Information
    - Building Plans
    - VIP / Distinguished Visitor Schedules

- The Information Assurance (IA) section of the PPIP shall:
  - Contain a section that identifies the countermeasures at each site where CPI is utilized / secured, from the following security domains (as applicable): Network Security and Information Technology (IT) access control and tracking. Describe the network architecture the Contractor shall use to support the contracted program and the architecture for connectivity with subcontractors and suppliers.
  - Define how Information Assurance (IA) practices are to be implemented.
  - Define how the Contractor and its subcontractors shall implement a plan for complying with the Department of Defense (DoD) PKI policy.
  - Define how the Contractor shall implement the following IA, IT and INFOSEC standards where applicable:
    - Define the Contractors process for identifying any existing / proposed CPI during developmental and RDT&E phases, and its protection / identification in the ECP process prior to ECP acceptance by the Government.

- Define how the Contractor shall coordinate with the Program Manager (PM), Information Assurance Officer (IAO) for newly developed systems to determine the Information Assurance (IA) requirements for Certification and Accreditation (C&A), or Platform Information Technology (PIT). This is to include Platform IT systems including all ground-based support systems that connect to the platform.
- Define the Contractors process for appropriately marking documents developed for this effort in accordance with the appropriate Security Classification Guide (SCG) and DoD document(s).
- Define the Contractors security training program, including types of training, frequency, methods, course material, topics, and venues (e.g. classroom, virtual)

- Anti-Tamper (AT) is identified in a separate SOW, CDRL, DID requirement.

4. END OF DI-MGMT-81826.