DATA ITEM DESCRIPTION

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

Number: DI-MGMT-81826B **Approval Date: 20140423**
AMSC Number: N9463 **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 Guides applicable for the F/A-18 (All Series) and EA-18G Aircraft and Systems.

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.

This DID DI-MGMT-81826B cancels and replaces DI-MGMT-81826A.

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The Contractor shall utilize the available databases for all updated / superseded amendments, notices and/or revisions of the reference documents identified below: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 CJCSI Documents see: http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm
- For OPNAV / SECNAV / Navy Documents see: http://doni.daps.dla.mil/default.aspx
- For DoD Documents see: http://www.dtic.mil/whs/directives/
- For Mil Documents see: http://quicksearch.dla.mil/
- For PMA / Classified Documents formally request from PCO / PMA265.
- Documents are also available via the internet

a. Chairman Joint Chiefs:

(1)	CJCSI 6211.02D	Defense Information System Network (DISN): Responsibilities (24 Jan 12)

b. DoD Publications / Manuals:

(1)	DoDM 5200.01	Vol 1, DoD Information Security Program: Overview, Classification, and Declassification (24 Feb 12.)
(2)	DoDM 5200.01	Vol 2, DoD Information Security Program: Marking of Classified Information (24 Feb 12, C-2 19/3/13)
(3)	DoDM 5200.01	Vol 3, DoD Information Security Program: Protection of Classified Information (24 Feb 12, C-2 19/3/13)
(4)	DoDM 5200.01	Vol 4, DoD Information Security Program: Controlled Unclassified Information (CUI) (24 Feb 12).
(5)	DoD 5200.1-M	DoD Acquisition System Protection Program (16 Mar 94)
(6)	DoD 5200.08-R	Physical Security Program (9 Apr 2007 C-1, 27 May 09) (also see DTM-09-012 and DTM-08-004
(7)	DoD 5205.02M	DoD OPSEC Program (3 Nov 08)
(8)	DoD M O-5205.13	Defense Industrial Base (DIB) Cyber Security and Information Assurance (CS / IA) Program Security Classification Manual (SCM) (26 Apr 12) (IA)
(9)	DoD 5220.22 M	National Industrial Security Program Operating Manual (NISPOM) (1 Feb 06) (also see DTM-09-019)

c. DoD Directives:

(1)	DoDD 5000.01	The Defense Acquisition System (12 May 03; Certified Current as of 20 Nov 2007)
(2)	DoDD 5205.02E	DoD OPSEC Program (20 June 12))
(3)	DoDD 5230.09	Clearance of DoD Information for Public Release (22 Aug 08, Cert Current Thru 22 Aug 15)
(4)	DoDD 5230.11	Disclosure of Classified Military Information to Foreign Governments and International Organizations (16 Jun 92)
(5)	DoDD 5230.20	Visits and Assignments of Foreign Nationals (22 Jun 05)
(6)	DoDD 5230.25	Withholding of Unclassified Technical Data From Public Disclosure (6 Nov 84; Incorporating Change 1, 18 Aug 95)
(7)	DoDD 8100.02,	Use of Commercial Wireless Devises, Services and Technologies in the DoD Global Information Grid (14 Apr 04, Cert. Current as of 23 Apr 07)

d. DoD Instructions:

(1)	DoDI 4140.01	DoD Supply Chain Materiel Management Policy (14 Dec 11)
(2)	DoDI 4140.67	DoD Counterfeit Prevention Policy (26 Apr 13)
(3)	DoDI 4160.28	DoD Demilitarization (DEMIL) Program (7 Apr 11)
(4)	DoDI 5000.02	Operation of the Defense Acquisition System INTERIM (25 Nov 13)
(5)	DoDI 5200.01	DoD Information Security Program and Protection of Sensitive Compartmented Information (9 Oct 08, C-1 13 Jun 11)
(6)	DoDI 5200.39	Critical Program Information (CPI) Protection Within the DoD (16 Jul 08, C-1, 28 Dec 10)
(7)	DoDI 5200.44	Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) (5 Nov 12)
(8)	DoDI 5230.24	Distribution Statements on Technical Documents (23 Aug 12)
(9)	DoDI S-5230.28	Low Observable (LO) and Counter Low Observable (CLO) Programs (U), CLASSIFIED DOCUMENT (26 May 05) Authorized users may contact the OPR / COR. (OPR: USD (AT&L), 703-697-0016)
(10)	DoDI O-5240.24	Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA), (8 Jun 11, C-1 15 Oct 13)

e. Department of the Navy (OPNAV/SECNAV):

(1)	OPNAVINST 3432.1A	Operations Security, (4 Aug 11)
(2)	OPNAVINST 3750.6R	Naval Aviation Safety Program, (8 Apr 09 with C- 1-4)
(3)	OPNAVINST 3811.1E	Threat Support to the Defense Acquisition System, (04 Jan 12)
(4)	OPNAVINST 5239.3A	Navy Implementation of DoD Intelligence Information System (DODIIS) Public Key Infrastructure (PKI) (18 Jan 08)
(5)	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, (most current version)
(6)	OPNAVINST 5530.14E,	Navy Physical Security and Law Enforcement Program (28 Jan 09, C-1 19 Apr 10)
(7)	SECNAVINST 5200.39A	Participation in the Government Industry Data Exchange (GIDEP), (25 Dec 05)
(8)	SECNAVINST 5510.36A	DoN Information Security Program (ISP) Instruction (6 Oct 06)
(9)	SECNAV M- 5510.36	DoN Information Security Program, (Jun 06)

d. Military Standards

(1) MIL-HDBK-350 A Guide for MIL-STD-1520C Corrective Action and Disposition System for Nonconforming Material (7 Jun 91)

(2) MIL-STD-882E DoD Standard Practice: System Safety (11 May 12)

e. Other Applicable Documents:

(1) EO 13526, Classified National Security Information (Dec 29, 2009)

(2) National Security Presidential Directive (NSPD) 54 / Homeland Security Presidential Directive (HSPD) 23 "Cybersecurity Policy" (8 Jan 08)

(3) NSDD 298, National Operations Security Program (22 Jan 88)

(4) OMB A-130 Appendix III, Security of Federal Automated Information Resources

(5) Pub L. 104-106, Information Technology Management Reform Act Division E, (Clinger-Cohen Act)

(6) Title 18 Section 1831 et seq of, Economic Espionage (Jan 08)

(7) DFAR 252.217-7026, Identification of Sources of Supply

(8) OMB Policy Letter 91-3, GIDEP (9 Apr 91

(9) Directive-Type Memorandum (DTM) 09-016, Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems

(10) Defense Authorization Act 254, National Defense Authorization Act, Senate Report 109-254

(11) NSTISSAM TEMPEST/2-95, with NSTISSAM TEMPEST/2-95A Amendment, Red/Black Installation Guidance, 2/3/00 (Document is FOUO)

(12) NSTISSAM TEMPEST/1-92, Compromising Emanations Laboratory Test Requirements, Electromagnetics, 12/15/92 (Confidential Document)

(13) CNSS Advisory Memorandum TEMPEST 01-02, NONSTOP Evaluation Standard, 10/1/02 (Confidential Document)

(14) CNSS No. 7000, TEMPEST Countermeasures for Facilities (18 Jun 94) (U) (Classified Document)

(15) NSTISSI 7001, NONSTOP Countermeasures (15 Jun 94) (Classified Document)

(16) NSTISSI 1000, National Information Assurance Certification and Accreditation Process (NIACAP) (Apr 00)

(17) FISMA, Federal Information Security Management Act of 2002 (FISMA)

(18) SAE-AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition

(19) The Defense Acquisition Guidebook (DAG) (Interim) Chapter 13)

(20) NISTIR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems (16 Oct 12)

(21) F/A-18E/F and EA-18G Program Protection Plan (PPP) (14 Mar 07) (PMA265)

(22) 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:
   a. 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.
   b. 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 Contractor's PPIP shall contain the following:
   a. Security Management.
   b. A section detailing the Contractors approach to the PPIP.
   c. General methodologies that will be applied to protection requirements.
   d. Critical Program Information (Critical Components (CC) / Critical Program Information (CPI) / Critical Systems (CS) / Critical Technologies, (CT) hereafter identified as CPI.
   e. The Contactor's 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.
   f. A section describing an effective and efficient protection of CPI; which shall include the following:
      (1) The Contractor's Program Security / OPSEC Management structure, including relationships with the corporate hierarchy and program subcontractors and suppliers.
      (2) An overview of all Contractor's activities, operations, tests, and other associated activities to be undertaken in performance of the contract; identifying those in which classified information could manifest itself; identifying 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 (DoDM 5200.01, Vol 1 through Vol 4, DoDI 5000.02, DoDI 5200.01, OPNAVINST 5513.2C, OPNAVINST 5530.14E, Title 18 Section 1831 et seq, DAG).
      (3) 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 (DoDD 5230.11, DoDI 5230.24, DoDD 5230.25, EO 13526.)
      (4) An Assessment of 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) (DoDI 5200.39, DoDD 5230.11, DoDD 8100.02, EO 13526, OPNAVINST 5513.2C.)

(5) Identification of 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 (DoDI 5200.01, DoDI 5200.39, DoDD 5230.11, EO 13526, OPNAVINST 5239.3A, Title 18 Section 1831 et seq.)

(6) All 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 (DoD 5200.1-M, DoDI 5200.01, DoD 5200.08-R, DoD 5200.1M, DoDD 5230.25, DoDI 4160.28, DoDI 4160.28, DoDI 5200.39, EO 13526, OPNAVINST 3750.6R, OPNAVINST 3811.1E, Title 18 Section 1831 et seq, DAG, F/A-18 All Series and EA-18G Aircraft and Systems security Guidance.)

(7) A Description of the process that will be used to assess new acquisitions (Incremental / Spiral upgrades, Engineering Change Proposal(s) (ECP's)) for CPI (DoD 5200.1-M, DoDI 5200.39, DoDD 5230.11, DoD S-5230.28, DAG.)

(8) A Description of 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 (DoDI 5000.02, DoDI 5200.39, DoDD 5230.11, DoDD 5230.25, EO 13526.)

(9) A Description of the Contractor's procedures for public release of program information (DoDD 5230.09, DoDD 5230.11, DoDD 5230.25.)

(10) A Description of the Contractor's Information Security Program (ISP) as a part of their PPIP. As an integral part of the ISP, describe the Contractor procedures for identifying, reporting and resolution of Facility Security Breaches; Classified Information Compromises, and Spillages including notification of DSS, DCMA, and Government Program Security Manager (DoDM 5200.01, Vol 1 through Vol 4, DoD 5220.22 M, DoDI 5000.02, DoDI 5200.01, SECNAVINST 5510.36A, SECNAV M- 5510.36, DoDD 5230.25, (1) CJCSI 6211.02D, EO 13526) and within the constraints specified in the DD 254 / CDRL / Contract.

(11) Describe the how Security classification guidance and original classification authority (OCA) for DIB information shall be developed in order to mitigate risks to critical DoD unclassified information supporting present and future DoD warfighting capabilities and residing on, or transiting, the Contractors / Sub-contractors private networks (DoDM 5200.01, Vol 1 through Vol 4, DoD M O5205-13, EO 13526, DoDI 5200.01.)

(12) Describe how the contractors Defense Industrial Base (DIB) Cyber Security is addressed in the Contractors facility and addressed in subcontracts and how incidents are addressed and reported

to DSS / DCMA. Framework Agreements and contracts that contain DIB cyber security requirements for safeguarding DoD classified and unclassified information. DIB participants shall handle classified and sensitive unclassified information, such as controlled unclassified information (CUI) (which includes For Official Use Only (FOUO) information); CPI (as described in DoDI 5200.39, as required by law and regulation, the Framework Agreement, contracts (NSPD 54 / HSPD 23, DoD M O-5205.13, EO 13526, DoDI 5200.01.)

g Supply Chain Risk Management (SCRM)

(1) The Supply Chain Risk Management (SCRM) portion of the PPIP shall include the establishment of a SCRM program tailored to fit the contractor's acquisition program identifying how supply chain risks are addressed across the entire system lifecycle through a defense-in-breadth approach to managing the risks to the integrity of information and communications technology (ICT) within covered systems (NSPD 54, HSPD 23, Defense Authorization Act 254, DTM 09-016, OMB Policy Letter 91-3, SAE-AS5553, DFAR 252.217-7026, MIL-STD 882E, MIL-HDBK-350, DAG, DoDD 5200.39, DoDD, 5000.01, DoDD 5230.25, DoDI 4140.01, DoDI 4140.67, DoDM 5200.01, Vol 1 through Vol 4, DoDI 5200.02, DoDI 5200.39, DoDI 5200.44, DoDD 8500.01E, SECNAVINST 5200.39A, and EO 13526, OPNAVINST 5513.2C, DAG, NISTIR 7622, DTM-09-016.)

(2) The Contractor shall establish policy and a defense-in-breadth strategy for managing supply chain risk to information and communications technology (ICT) within DoD critical information systems and weapons systems in accordance with NSPD 54 / HHSPD23, DoD M O-5205.13, DoD 5220.22 M. (The PPIP shall also address how the following elements / requirement are addressed in the Contractors Product Specification / Acquisition Strategy / Statement of Work (SOW) / Contract.) shall be addressed:

(a) Incorporation of all-source intelligence analysis into assessments of the supply chain for covered systems. (CPI/CT Review using the Tool (CPI/CT TOOL v4.1 or current version))

(b) Processes to control the quality, configuration, and security of software, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources (DoDI 4140.01, DoDI 4140.67.)

(c) Processes to detect the occurrence, reduce the likelihood of occurrence, and mitigate the consequences of products containing counterfeit components or malicious functions (DoDI 4160.28.)

(d) Processes to ensure that the fabrication of integrated circuits that are custom-designed and / or custom-manufactured (generally referred to as "application-specific integrated circuits") for a specific DoD end use within covered systems are, as appropriate to the risk, performed by suppliers of integrated circuit-related services accredited through an authority designated by

the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), unless expressly waived by the Milestone Decision Authority (MDA) established pursuant to DoDD 5000.01.

(e) The Plan shall describe how the contractor will report via Government Industry Data Exchange Program GIDEP Counterfeit / malicious modified parts (DoDI 5230.24, DoDI 4140.67, and DoDI 4160.28.)

h. 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 (DoD 5205.02M, DoD 5220.22M (NISPOM), DoDD 5205.02E, DoDD 8100.02, DoDI 8500.2, DoDI 8580.1, OPNAV 3432.1A, EO 13526, SECNAVINST 5510.36A, SECNAV M- 5510.36, (1) CJCSI 6211.02D, NSDD 298, OMB A-130, Appendix III, Pub L. 104-106.)

The following shall also be addressed:

(1) 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 (DoDM 5200.01, Vol 1 through Vol 4.)

(2) 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.

(3) 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 (DoDM 5200.01, Vol 1 through Vol 4; DoDD 5230.20, DoDI O-5240.24.)

(4) 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. National security information shall not be compromised by emanations from Classified Information Processing Systems (CLIPS) (NSTISSAM TEMPEST/2-92 with NSTISSAM TEMPEST/2-95A Amendment of 3 Feb 2000 shall be used as guidance for the installation of CLIPS.) The Aircraft / System shall meet the requirements of CNSS AM TEMPEST 01-02 of 1 Oct 2002, and NSTISSAM TEMPEST/1-92 Level II of 15 Dec 1992, CNSS Advisory Memorandum TEMPEST 01-02, CNSS No. 7000, NSTISSI 7001, NSTISSI 1000, FISMA, NSDD 298, CJCSI 6211.02D.

(5) 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.

(6) Organizational OPSEC Communications and Interfaces: A description as to how the Plan will be communicated to personnel supporting the program.

(7) The Plan shall identify all OPSEC interfaces internal to the corporation such as Senior Corporate Leadership, OPSEC Working Group, OPSEC Coordinators, and program personnel (DoDI 5200.02.)

(8) The Plan shall identify all external points of contact; Contracting activity, Defense Contract Management Agency (DCMA), defense Security Service (DSS), Federal Bureau of Investigation (FBI) and local Law Enforcement. The Plan shall identify the contacts primary role within the OPSEC program. Subcontractor and supplier OPSEC points of contact shall be similarly identified.

(9) The categories of Potential Critical Information (CI) that shall be protected and planned for in the PPIP are:

(a) Current and Future Operations

(b) Travel Itineraries

(c) Usernames and Passwords

(d) Access / Identification Cards

(e) Operations Planning Information

(f) Personal Identification Information

(g) Entry / Exit (Security) Procedures

(h) Capabilities and Limitations

(i) Address and Phone Lists

(j) OPSEC Budget Information

(k) Building Plans

(l) VIP / Distinguished Visitor Schedules

(10) Describe how the contractors Defense Industrial Base (DIB) Cyber Security and Information Assurance (CS / IA) Program is addressed in the Contractors facility; and also addressed in subcontracts and how incidents are addressed and reported to PMA265 Program Security Manager (PSM), DCMA/ DSS / FBI. Framework Agreement and contracts that contain DIB cyber security requirements, for safeguarding DoD classified and unclassified information. DIB participants shall handle classified and sensitive unclassified information, such as controlled unclassified information (CUI) (which includes Unclassified//For Official Use Only (FOUO) information), CPI (as described in DoDI 5200.39, as required by law and regulation, the Framework Agreement, contracts (NSPD 54 / HSPD 23, DoD M O-5205.13, CJCSI 6211.02D, EO 13526, DoDI 5200.01.)

(11) Describe how the contractors Counterintelligence Awareness and Reporting (DoDD 5240.06), and the contractors plan to comply with the training and reporting requirements of the above reference document.

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

4. END OF DI-MGMT-81826B.