DATA ITEM DESCRIPTION

Title: F/A-18 - EA-18 AIRCRAFT / SYSTEM PROGRAM PROTECTION IMPLEMENTATION PLAN

Number: DI-MGMT-81826C	**Approval Date:** 20141203
AMSC Number: 9505	**Limitation:** N/A
DTIC Applicable: N/A	**GIDEP Applicable:** N/A
Preparing Activity: AS	**Project Number:** MGMT-2015-012
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-81826C cancels and replaces DI-MGMT-81826B.

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 specified in the contract.

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 Publications (http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm):
   (1) CJCSI 6211.02D, Defense Information System Network (DISN), Responsibilities (24 Jan 12)
   (2) CJCSM 6510.01B, Cyber Incident Handling Program (10 July 12)

b. DoD Publications / Manuals (http://www.dtic.mil/whs/directives/):
   (1) DoDM 5200.01, Volume 1, DoD Information Security Program: Overview, Classification, and Declassification (24 Feb 12)
   (2) DoDM 5200.01, Volume 2, DoD Information Security Program: Marking of Classified Information (24 Feb 12, C-2 19/3/13)

(3) DoDM 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information (24 Feb 12, C-2 19/3/13)
(4) DoDM 5200.01, Volume 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)
(9) DoD 5220.22 M, National Industrial Security Program Operating Manual (NISPOM) (1 Feb 06) (also see DTM-09-019)
(10) DoD 5230.25-PH, Control of Unclassified Technical Data with Military or Space Application (06 Nov 1984, C-1, 18 Aug 1995)
(11) DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons, (1 Dec 82) also see DTM 08-052, DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters (17 Jun 09 Incorporating Change 3, 30 Jul 12) and DTM-08-011, Intelligence Oversight Policy Guidance (26 Mar 2008 Incorporating Change 3, 27 Jul 12)

c. DoD Directives (http://www.dtic.mil/whs/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 (http://www.dtic.mil/whs/directives/):
(1) DoDI 2040.02, International Transfers of Technology, Articles, and Services (27 Mar 14)
(2) DoDI 4140.01, DoD Supply Chain Materiel Management Policy (14 Dec 11)
(3) DoDI 4140.67, DoD Counterfeit Prevention Policy (26 Apr 13)
(4) DoDI 4160.28, DoD Demilitarization (DEMIL) Program (7 Apr 11)
(5) DoDI 5000.02, Operation of the Defense Acquisition System INTERIM (25 Nov 13)
(6) DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information (9 Oct 08, C-1 13 Jun 11)
(7) DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB) (10 Dec 2005, C-1, 19 May 10) (Also see DTM-08-004, DTM-09-012)
(8) DoDI 5200.39, Critical Program Information (CPI) Protection Within the DoD (16 Jul 08, C-1, 28 Dec 10)
(9) DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and

Networks (TSN) (5 Nov 12)
(10) DoDI 5230.24, Distribution Statements on Technical Documents (23 Aug 12)
(11) 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)
(12) DoDI O-5240.24, Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA) (8 Jun 11, C-1 15 Oct 13)
(13) DoDI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies (3 Nov 09)
(14) DoDI 8500.01, Cybersecurity (14 Mar 14)
(15) DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) (IA) 12 Mar 14
(16) DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PKI) Enabling (21 May 11) (IA)
(17) DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System (9 Jul 04) (IA)
(18) DoDI 8582.01, Security of Unclassified DoD Information on Non-DoD Information Systems (6 Jun 12) (IA)

e. Department of the Navy (OPNAV/SECNAV) (available via http://doni.daps.dla.mil/SECNAV.aspx):
(1) OPNAVINST 3432.1A, OPSEC, (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 5000.2E, DoN Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System (1 Sep 11)
(8) SECNAVINST 5200.39A, Participation in the Government Industry Data Exchange (GIDEP), (25 Dec 05)
(9) SECNAVINST 5510.36A, DoN Information Security Program (ISP) Instruction (6 Oct 06)
(10) SECNAV M- 5510.36, DoN Information Security Program, (Jun 06)

f. Other DoD / Navy Publications (Available via ASSIST / internet):
(1) Memorandum for Secretaries of The Military Departments, Overarching DoD Counterfeit Prevention Guidance (dated 16 Mar 12)
(2) DoD CIO MEMO, Encryption of Sensitive Unclassified Data at rest on Mobile Computing Devices and Removable Storage Devices (7 Jul 07) (Available via internet)
(4) DAG Chapter 13, Program Protection (The Defense Acquisition Guidebook) (Most current Defense Acquisition University version) (Available via DAU on the internet)
(5) Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program (25 Feb 10)
(6) DI-QCIC-80125B, Government Industry Data Exchange Program (GIDEP) Alert/Safe-Alert Report (05 May 03) (Available via internet)

(7) DI-QCIC-80126B, Government Industry Data Exchange Program (GIDEP) (05 May 03) (Available via internet)

g. Presidential Executive Orders (Available via internet) / Public Laws (P.L.) (Available via internet):

(1) E.O. 12968, Access to Classified Information, (2 Aug 95, as amended)
(2) E.O. 13526, Classified National Security Information (29 Dec 09)
(3) E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 7 Oct 11
(4) NSPD-54/HSPD23, National Security Presidential Directive 54, in conjunction with Homeland Security Directive-23 (2 Mar 10)
(5) NSDD 298, National Security Decision Directive, National Operations Security Program (22 Jan 88)
(6) OMB A-130 Appendix III, Security of Federal Automated Information Resources (Circular No A-130) (IA)
(7) OMB Policy Letter 91-3, Reporting Nonconforming Products, (9 Apr 1991)
(8) Defense Authorization Act 254, National Defense Authorization Act, Senate Report 109-254
(9). P.L. 87-794, Trade Expansion Act of 1962 (76 Stat. 872, enacted October 11, 1962, 19 U.S.C. § 1801)
(10) P.L. 96-72, Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq) (1979)
(11) P.L. 104-106, Information Technology Management Reform Act, Division E, (Clinger-Cohen Act) (10 Feb 1996)
(12) P.L. 104-231, Freedom of Information Act, As Amended By 104-231, 110 Stat5 U.S.C. § 552, 3048
(13) P.L. 112-81, Section 818 (f)(2) and (c)(2), Defense Auth. Act for Fiscal Year 2012
(14) P.L. 112-239, Section 833, Defense Auth. Act for Fiscal Year 2013

h. Federal Acquisition Regulations (FARS) / Defense Acquisition Regulations (DFARS) (Available via internet / COR / PCO):

(1) DFARS 252-204-7012, Safeguarding of Unclassified Controlled Technical Information (18 Nov 13)
(2) DFARS 246.407, Nonconforming Supplies/Services, Government Contract Quality Assurance (1 Aug 10)
(3) DFARS 252.246-7003, Defense Federal Acquisition Regulations Supplement "Notification of Potential Safety Issues" (Revised March 3, 2008)
(4) DFARS 2012-D055, Detection and Avoidance of Counterfeit Electronic Parts
(5) DFARS 2013-27311, Requirements Relating to Supply Chain Risk
(6) FAR 45.101, Demilitarization
(7) FAR Subpart 46.4, Government Contract Quality Assurance
(8) FARS 252.217.7026, Identification of Sources of Supply

i. Other Applicable National Standards / Publications (Available via internet / COR / PCO):

(1) NSTISSAM TEMPEST/2-95, With NSTISSAM TEMPEST/2-95A Amendment, Red/Black Installation Guidance, (Document is FOUO) (IA) (Controlled Document Contractors formally request via PCO/Contracting Officer)
(2) NSTISSAM TEMPEST/1-92, Compromising Emanations Laboratory Test Requirements, Electromagnetics, (Document is Confidential) (IA) (Controlled Document Contractors formally request via PCO / Contracting Officer)
(3) CNSSI 1001, National Instruction on Classified Information Spillage (Feb 08) (Available via

internet)

- (4) CNSS-NSTISS 7000, TEMPEST Countermeasures for Facilities (U) (May 04) (S/NF) (De-CLASSIFIED 1993 DOCUMENT)) (IA) ((Formally request via PCO/Contracting Officer)
- (5) CNSSI 4009, National Information Assurance (IA) Glossary (26 April 10) (Available via internet)
- (6) CNSSD 505, Supply Chain Risk Management (SCRM) (7 Mar 12)
- (7) FISMA, Title III, Public Law 107-347; Federal, Information Security Management Act of 2002 (H. R. 2458-48) (& Dec 2002) (IA) (Available via internet)
- (8) Title 18 Section 1831, Economic Espionage, et seq of, (Jan 08) (Available via internet)
- (9) Title 22, Chapter 39, Arms Export Control Act, (U.S.C., Sec 2751, et seq.) (4 Jan 12) (Available via internet)
- (10) NIST SP 800-59, Guideline for Identifying an Information System as a National Security System (Aug 03) (Available via internet/NIST)

j. Military Standards (Available via ASSIST @, http://quicksearch.dla.mil/)

- (1) MIL-HDBK-350, Corrective Action and Disposition System for Nonconforming Material (7 JUNE 1991)
- (2) MIL-STD-461F, DoD Interface Standard: Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment (10 Dec 2007)
- (3) MIL-STD-464C, DoD Interface Standard: Electromagnetic Environmental Effects Requirements for Systems (01 Dec 2010)
- (4) Mil-STD 882E, Department of Defense safety Standard Practice System (SCRM) (11 May 2012)

k. Supply Chain Risk Management (SCRM) Program Management (Available via Internet / NIST / commercial sources)

- (1) SO300-BT-PRO-010, Government Industry Data Exchange Program (GIDEP) Operations Manual (W/ 10 Sep 10 Updates)
- (2) NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View (Mar 11)
- (3) NIST SP 00-59, Guideline for Identifying an Information System as a National Security System
- (4) NIST IR 7622, Piloting Supply Chain Risk Management Practices for Federal Information Systems (Jun 10)
- (5) NIST SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (Feb 10)
- (6) DoD Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program (25 Feb 10)
- (7) CNSS No. 505, Supply Chain Risk Management (7 Mar 12)

l. SCRM Industry Standards (pertain to electronic components, standard industry practice available via commercial sources):

- (1) ANSI / EIA-4899, Standard for Preparing an Electronic Component Management Plan (2002)
- (2) IDEA-STD-1010B, Acceptability of Electronic Components Distributed in the Open Market (Apr 11)
- (3) AS9120 Rev C, Quality Management Systems for Aerospace Product Distributors (Jun 12)
- (4) SAE-AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and

Disposition (2009)

m. Program Office applicable Documents (Formally request via PCO/Contracting Officer)
   (1) F/A-18E/F and EA-18G Program Protection Plan (3/14/07)
   (2) Security Guidance F/A-18 Hornet (All Series) and EA-18 G Growler

2. Format. The required document shall be in Contractor format:
   a. The PPIP will 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 including the following Critical Components (CC), Critical Program Information (CPI), Critical Systems (CS), and Critical Technologies, (CT).
   e. The Contactor's process for identifying any existing / proposed CC / CPI / CS / CT 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 CC / CPI / CS / CT ; whichever are applicable and 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.
      (3) Identification of the CC / CPI / CS / CT physical locations under the Contractor's or its subcontractors' control and how the CC / CPI / CS / CT is to be managed / tracked / secured throughout the CC / CPI / CS / CT life-cycle.
      (4) An Assessment of the vulnerability of the CC / CPI / CS / CT 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.)
      (5) Identification of the planned countermeasures at each site where CC / CPI / CS / CT is utilized / secured from the following security domains: Physical security; personnel security; telecom and network security, application, systems development, cryptography, and security architectures.
      (6) All special handling procedures required for CC / CPI / CS / CT, and procedures for recovering CC / CPI / CS / CT 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.

(7) A Description of the process that will be used to assess new acquisitions (Incremental / Spiral upgrades, Engineering Change Proposal(s) (ECP's)) for CC / CPI / CS / CT.

(8) A Description of how the Contractor shall comply with procedures for ensuring compliance with U.S. Government export statutes and regulations that affect CC / CPI / CS / CT in a contracted program.

(9) A Description of the Contractor's procedures for public release of program information.

(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 within the constraints specified in the DD 254 / CDRL / Contract.

(11) Describe how the Contractor will implement Department of Defense (DoD) PKI policy. PKI encryption is the chosen compliant DoD standard for protecting Controlled Unclassified Information (CUI) during transmission. CUI encompasses For Official Use ONLY (FOUO) and Sensitive Information. Failure to encrypt CUI during electronic transmission is considered a security weakness and shall be reported to the PSM / IAO.

(12) Describe the how Security classification guidance and original classification authority (OCA) for Defense Industrial Base (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.

(13) Describe how the contractors 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 CUI (which includes FOUO information); CC / CPI / CS / CT (as described in applicable DoD documents, as required by law and regulation, the Framework Agreement, contracts.

g Supply Chain Risk Management (SCRM) / Counterfeit Prevention:

(1) The Supply Chain Risk Management (SCRM) / Counterfeit Prevention portion of the PPIP shall include the establishment of a SCRM / Counterfeit Prevention program tailored to fit the contractor's acquisition program identifying how supply chain risks will be 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 / applicable systems.

(2) The PPP requires the contractor to establish policy and a defense-in-breadth strategy for managing supply chain risk to information and communications technology (ICT) within DoD critical information systems / weapons systems and will describe in the Contractors PPIP. The PPIP will include the following elements / requirement as described in the Contractors Product Specification (Parts, Materials and Processes Selection List (PMPSL) / "As Designed" and "As Built" Parts List.)

(a) Incorporation of all-source intelligence analysis into assessments of the supply chain for covered systems. (CC / CPI / CS / CT Review using the Navy Standard CPI Identification WBS Tool (current version))

(b) Procurement practices and procedures to include procurement of all parts and materials from original qualified parts/materials equipment manufacturer (OEM) or it franchised/authorized distributor.

(c) Procurement practices and internal processes used for exceptions to buying from OEM or OEM franchised distributors in cases where items are no longer available including a process to qualify/certify non-OEM parts & materials.

(d) Monitoring procedures to include the delivery of test results from random sampling and supply chains surveillance that does not assume any source is safe to identify possible penetration of OEM supply chain.

(e) Processes to control the quality, configuration, and security of software, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources. Monitor processes at all subcontractor levels processes and verify compliance through on-site audits.

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

(g) 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).

(h) Describe how the contractor will report suspected counterfeit / malicious / counterfeit parts via Government Industry Data Exchange Program GIDEP Counterfeit / malicious modified parts.

h. The OPSEC portion of the PPIP will include establishment of an OPSEC support capability that provides for program development, planning, training, assessment, surveys, and readiness training. Including the results of the five-step OPSEC analysis Identifying Critical Information (CI), Analyzing Threats, Analyzing Vulnerabilities, Assessing Risk; and Applying Countermeasures, including those aspects of the foreign intelligence threats that are applicable to the contract. The following will 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.

(2) Threat: The known threats to the contracting activity and include only that portion deemed applicable to the specific contract activities in addition to how 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 brass board 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.

(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) TEMPEST/2-95A Amendment of 3 Feb 2000 shall be used as guidance for the installation of CLIPS.

(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.

(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. 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), CC / CPI / CS / CT.

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

i. When contractually required, describe how the contractor will protect Anti Tamper (AT) Plans and associated information.

End of DI-MGMT-81826C