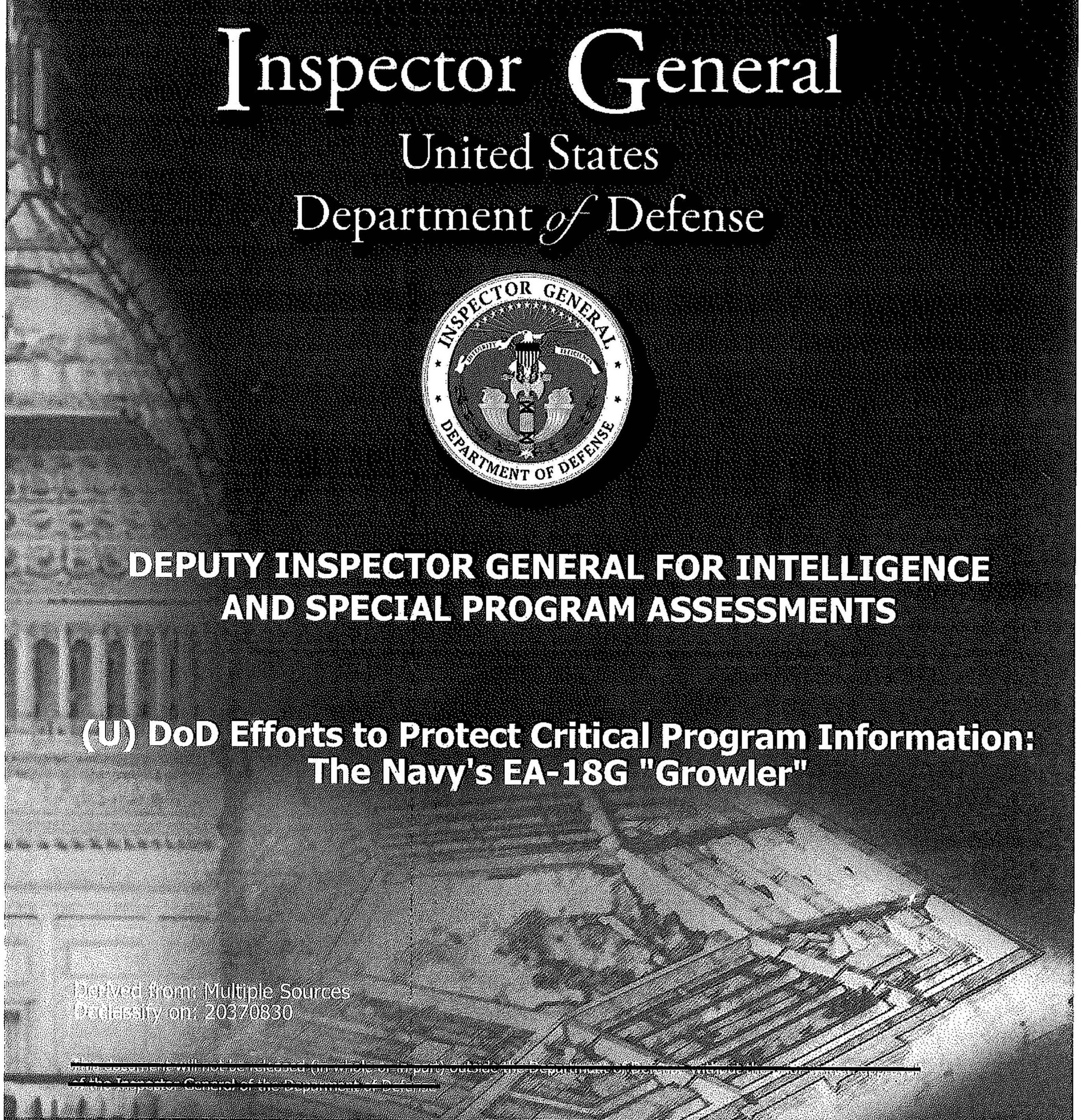
Report No. DoDIG-2012-124
August 30, 2012

Inspector General
United States
Department *of* Defense



DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE AND SPECIAL PROGRAM ASSESSMENTS

(U) DoD Efforts to Protect Critical Program Information: The Navy's EA-18G "Growler"

Derived from: Multiple Sources
Declassify on: 20370830

~~This document will not be released (in whole or in part) outside the Department of Defense without the approval of the Inspector General of the Department of Defense~~

(U) Additional Copies

(U) For information and to request copies of this report, contact the DoD Office of Inspector General at (703) 882-4818 or (DSN 381-4818).

(U) Suggestions for Audits and Evaluations

(U) To suggest ideas for or to request future audits or evaluations, contact the Office of the Deputy Inspector General for Intelligence and Special Program Assessments at (703) 882-4860 (DSN 381-4860) or UNCLASSIFIED fax (571) 372-7451. Ideas and requests can also be mailed to:

ODIG-ISPA (ATTN: Intelligence and Special Program Assessment Suggestions)
Department of Defense Inspector General
4800 Mark Center Drive (Room 10J25)
Alexandria, VA 22350-1500

(U) Acronyms and Abbreviations

ACAT	Acquisition Category
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer
ASN/RDA	Assistant Secretary of the Navy for Research, Development and Acquisition
CPI	Critical Program Information
DoN	Department of the Navy
NAVAIR	Naval Air Systems Command
NCIS	Naval Criminal Investigative Service
PM	Program Manager
RDA	Research, Development, and Acquisition
RDT&E	Research, Development, Test, and Evaluation
SECNAV	Secretary of the Navy
STILO	Science and Technology Intelligence Liaison Officer
SYSCOM	Systems Command
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

August 30, 2012

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR POLICY
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
ASSISTANT SECRETARY OF THE NAVY FOR RESEARCH, DEVELOPMENT, AND ACQUISITION
DIRECTOR, NAVAL CRIMINAL INVESTIGATIVE SERVICE
CHIEF OF NAVAL OPERATIONS/N-2, DIRECTOR OF NAVAL INTELLIGENCE
COMMANDER, NAVAL INSTALLATIONS COMMAND
COMMANDER, NAVAL AIR SYSTEMS COMMAND
PROGRAM EXECUTIVE OFFICER, TACTICAL AIR
PROGRAM MANAGER, EA-18G

SUBJECT: (U) DoD Efforts to Protect Critical Program Information: The Navy's EA-18G "Growler" Report No. DoDIG 2012-124 (Project No. D2008-DINT01-0242.003)

(U) We are providing this report for your information and use. We issued a draft of this report on March 26, 2012. We considered comments from the Under Secretary of Defense for Policy, the Under Secretary of Defense for Intelligence, the Assistant Secretary of the Navy for Research, Development, and Acquisition, the Director, Naval Criminal Investigative Service, the Commander, Navy Installations Command, and the EA-18G Program Manager. Management concurred with our recommendations, and proposed actions and actions taken to date satisfy the intent of those recommendations. Therefore, we will not require further comment.

(U) We appreciate the courtesies extended to the staff. Please direct questions to DoD OIG (b)(6) at (703) 882-DoD OIG (b) (DSN 381-DoD OIG (b)(6)) or the Project Manager at (703) 882-DoD OIG (b) (DSN 381-DoD OIG (b)(6)) or. If you desire, we will provide a formal briefing on the results.

James R. Ives
Acting Deputy Inspector General
for Intelligence and Special
Program Assessments

Report No. DoDIG 2012-124 (Project No. D2008-DINT01-0242.003) August 30, 2012

(U) Results in Brief: DoD Efforts to Protect Critical Program Information: The Navy's EA-18G "Growler"

(U) What We Did

(U) This is the third and final in a series of assessments to determine how DoD protects critical program information. The Navy's EA-18G "Growler" program is an acquisition category ID program we used as a case study to assess the Navy's effectiveness in protecting critical program information. We conducted this assessment in coordination with DoD research, development, acquisition, counterintelligence, and security subject matter experts. We assessed eight key issue areas related to program protection. Protecting critical program information is imperative in order for the U.S. to maintain the technologically-dependent cutting edge of its weapons systems.

(U) What We Found

(U) We found that while DoD and Navy policy to protect critical program information has progressed in recent years, there is still a need for improvement. The Navy has developed a standardized process for identifying critical program information that is required to be used by all Program Managers and technology directors. This standard operating procedure integrates security and counterintelligence specialists with rigorous system security engineering processes. However, Navy efforts to protect critical program information are not integrated and synchronized to the greatest extent possible and they are not optimizing the ability to provide uniform research, development, and acquisition protection.

(U) DOD OIG (b)(7)(E) [redacted]

(U) Additionally, although DoD component training in the protection of critical program information exists, not all program, security, and counterintelligence personnel receive adequate training through DoD managed acquisition and security training enterprises. While we make no recommendations regarding the shortage of resources, because of upcoming budget cuts, DoD management at all levels needs to ensure that the correct skills are available, leverage existing resources, and identify and mitigate the risk associated when requirements are not met.

(U) What We Recommend

~~(S//NF)~~ DIA: EO 13526, § 1.4(c), 1.4(g); NAVAIR: (b)(1), EO 13526, sec. 1.4(a) [redacted]

(U) Update the EA-18G program protection plan and technology assessment/control plan to better align protection efforts with DoD and Navy policy regarding foreign visits and foreign disclosure; conduct a program protection survey to ensure contractor implementation of the countermeasures articulated in the program protection plan and monitor the progress of the implementation; and provide the Defense Security Service with a copy of the program protection plan and the DD Form 254 that reflects the information needed to protect critical program information.

(U) Promulgate counterintelligence support specifically tailored to Program Management Air-265 within the Naval Air Station Patuxent River umbrella counterintelligence support plan.

(U) Management Comments and Our Response

(U) Management concurred with our recommendations, and proposed actions and actions taken to date satisfy the intent of those recommendations. Therefore, we will not require further comment.

(U) Table of Contents

(U) Introduction

(U) Protecting critical program information (CPI) is imperative in order for the U.S. to maintain the technologically-dependent cutting edge of its weapon systems. Critical program information is defined as elements or components of a research, development, and acquisition (RDA) program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse-engineer the technology or capability. Critical program information includes information about applications, capabilities, processes, and end items; elements or components critical to a military system's or network's mission effectiveness; and technology that would reduce the U.S. technological advantage if compromised.

(U) Objective

(U) The objective of this project was to determine how effectively DoD identifies and protects CPI. Specifically, we assessed the following eight key areas critical to effective program protection:

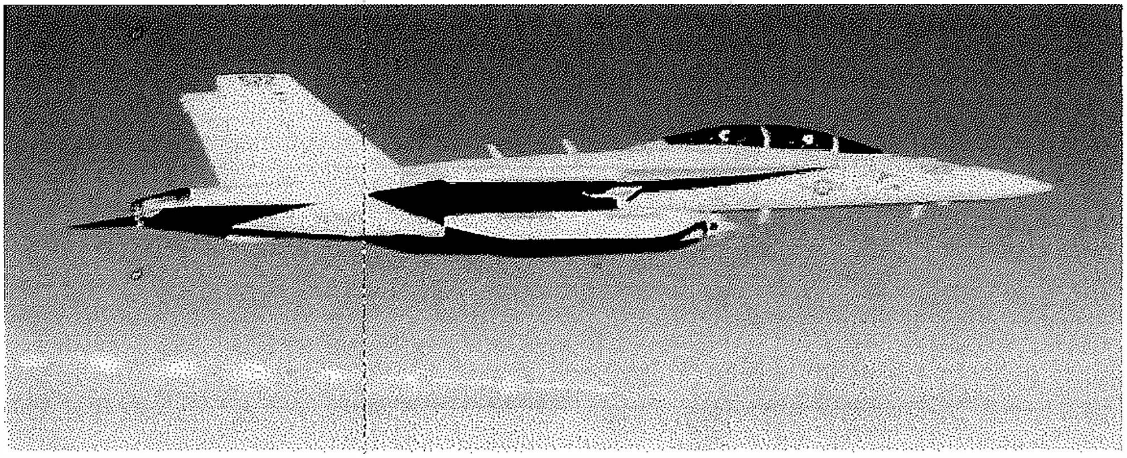
- (U) ability to identify CPI;
- (U) effectiveness in developing and implementing a program protection plan;
- (U) training efforts for the protection of CPI;
- (U) use of resources for the protection of CPI;
- (U) effectiveness of policies to protect CPI;
- (U) ability of counterintelligence, intelligence, and security to support the protection of CPI;
- (U) effectiveness of the foreign visit program; and
- (U) application of "horizontal protection" of CPI.

(U) On December 12, 2008, the DoD Office of the Inspector General, Deputy Inspector General for Intelligence and the Deputy Under Secretary of Defense (Acquisition and Technology) cosigned a letter announcing the concept of this program protection assessment. The goal of the project was to conduct assessments of three major programs to evaluate how effectively DoD and each Military Department identify and protect CPI. The Navy's EA-18G is the third and final acquisition category (ACAT) ID[1] program of record assessed. See Appendix A for a discussion of the scope and methodology.

[1] (U) Acquisition Category I programs are major Defense acquisition programs. A major Defense acquisition program is a program estimated by the USD(AT&L) to require eventual expenditure for research, development, test, and evaluation of more than $365 million or procurement of more than $2.19 billion, or those designated by the USD(AT&L) to be major Defense acquisition programs or special interest programs. Acquisition category I programs have two subcategories: The first subcategory is ACAT IC, for which the milestone decision authority is the DoD Component Head or, if delegated, the Component Acquisition Executive. The second subcategory is ACAT ID, for which the milestone decision authority is the USD(AT&L). The Defense Acquisition Board advises the USD(AT&L) at major decision points. The USD(AT&L) designates programs as ACAT ID or ACAT IC.

(U) Background

(U//~~FOUO~~) EA-18G Growler. The EA-18G Growler is a carrier-based radar and communication jammer aircraft that replaces the EA-6B Prowler. It is a variant of the combat-proven F/A-18F Super Hornet Block II and flies the airborne electronic attack mission. The EA-18G combines the capability of the Super Hornet with the latest airborne electronic attack avionics suite. The EA-18G's vast array of sensors and weapons provides the warfighter with a lethal and survivable weapon system to counter current and emerging threats. The EA-18G is used to support friendly air, ground, and sea operations by suppressing enemy radar and communications. The EA-18G's capabilities are used to jam integrated air defenses; support non-integrated air defense missions and emerging non-lethal target sets; enhance crew situational awareness and mission management; enhance connectivity to national, theater, and tactical strike assets; provide enhanced lethal suppression through more accurate high speed anti-radiation missile targeting; and provide the EA-18G crew air-to-air self protection with advanced medium range air-to-air missiles.



(U/~~FOUO~~) As a result of a multi-year procurement for the FA-18E/F and EA-18G described in the Department of the Navy (DoN) FY-2012 budget estimates for Navy Aircraft Procurement, the EA-18G program will produce 114 EA-18G aircraft through FY-2013. Additionally, the EA-18G aircraft has successfully completed its operational evaluation period, was found to be operationally effective and suitable, and has achieved initial operating capability. Naval Air Systems Command (NAVAIR) reported the total cost of $11.2 billion, including $1.9 billion in research, development, test, and evaluation (RDT&E) costs for producing the 114 EA-18G aircraft. Estimated program protection costs for the F/A-18E/F and EA-18G programs are $1.7 million per year. Currently, the program protection costs are obligated on the multi-year procurement III contract. The EA-18G will also be sold to a foreign government.

(U) Criteria

(U) DoD Policy and Implementation Guidance

(U) It is DoD policy to provide uncompromised and secure military systems to the warfighter by performing comprehensive protection of CPI through the integrated and synchronized application of counterintelligence, intelligence, security, systems engineering, and other defensive countermeasures to mitigate risk. Failure to apply consistent protection of CPI may result in the loss of confidentiality, integrity, or availability of CPI resulting in the impairment of the warfighter's capability and the degradation of DoD's technological superiority. Additionally, it is DoD policy to mitigate the exploitation of CPI; extend the operational effectiveness of military systems through the application of appropriate risk management strategies; employ the most effective protection measures, to include system assurance and anti-tamper; conduct comparative analysis of defense systems' technologies and in order that CPI protection is aligned horizontally throughout the DoD, document the measures in a program protection plan.[2]

(U) Furthermore, DoD policy requires that contracts supporting RDA programs wherein CPI has been identified shall contain contractual terms requiring the contractor to protect the CPI to DoD standards.

(U) DoD Instruction 5200.39 "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008, defines what constitutes CPI; establishes policy for the protection of CPI; and assigns responsibilities for counterintelligence, intelligence, security, and systems engineering support for the identification and protection of CPI. Furthermore, it details responsibilities relating to the identification of CPI and the implementation of program protection plans to DoD Components; and implements relevant parts of DoD Directive 5000.01, "The Defense Acquisition System," DoD Instruction 5000.02, "Operation of the Defense Acquisition System;" December 8, 2008, and continues to authorize the use of DoD 5200.1-M, "Acquisition Systems Protection Program," March 1994, to serve as implementation guidance. Also, DoD Instruction 5200.39 supplements existing policies and guidance related to the security of DoD personnel, information, resources, installations, and operations to include DoD contractors performing work or supporting DoD RDA efforts.

[2] (U) The program protection plan is designed as a dynamic planning tool to capture in a single document the most effective means to protect CPI from unauthorized foreign collection activities and unauthorized disclosure; and to develop those protection measures that will ensure a combat system's effectiveness throughout its lifecycle. When a determination of CPI is made, a program protection plan is required for milestone decision authority review and approval at all milestones. The program protection plan is required to address the foreign collection threat to the CPI that has been identified by intelligence and counterintelligence agencies; includes an annex for the Counterintelligence Support Plan; and a classified annex for the Anti-Tamper Plan that addresses anti-tamper countermeasures to be considered for the protection of CPI and critical technologies. Additionally, when the RDA program involves foreign military sales, international co-production arrangements, or other international activities, the program protection plan will include an annex for a Technology Assessment and Control Plan that addresses the risks involved in foreign access to CPI and critical technologies; the foreign participation in the program or foreign sales; and the development of access controls and other measures designed to protect the U.S. technological or operational advantage of the system.

(U) DoD Instruction O-5240.24 "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, establishes policy, assigns responsibilities, and provides procedures for the conduct of counterintelligence activities supporting RDA. It directs the integration of a Technology Targeting Risk Assessment with the appropriate counterintelligence analytical product to address foreign collection threats to RDA programs with CPI. It provides for threat analysis to support supply chain risk management, and establishes the Counterintelligence RDA Integrated Management Group, the principal forum for coordinating and sharing RDA information among the Defense counterintelligence components.

(U) DoD Instruction 5000.02 "Operation of the Defense Acquisition System," December 8, 2008, establishes within DoD acquisition policy that during the technology development phase, the technology development strategy shall document a listing of CPI and potential countermeasures, such as anti-tamper, in order to inform program protection planning and design integration. Further, CPI shall be identified as early as possible, and shall inform the preparation of the program protection plan. Additionally, during the engineering and manufacturing development phase, it states that the protection of CPI is implemented by applying appropriate system engineering and security techniques, such as anti-tamper. Moreover, DoD Instruction 5000.02, Enclosure 4 details "Statutory and Regulatory Information and Milestone Requirements" that apply to all acquisition programs; and details each milestone and decision point setting forth mandatory requirements relevant to the identification and protection of CPI.

(U) DoD 5200.1-M "Acquisition Systems Protection Program," March 1994, prescribes standards, criteria, and methodology for the identification and protection of CPI (described as Essential Program Information, Technologies, and/or Systems within this Manual) within DoD acquisition programs. The protection standards and guidance described within this Manual are required to prevent foreign intelligence collection and unauthorized disclosure of essential program information, technologies and/or systems during the DoD acquisition process.

(U) Defense Acquisition Guidebook, Chapter 8, "Intelligence, Counterintelligence, and Security Support," addresses actions required once CPI is identified within an acquisition program and identifies the critical elements in a comprehensive acquisition protection strategy, including:

- (U) the responsibilities of Program Managers (PM) in the prevention of inadvertent transfers of dual-use and leading-edge military technologies used in defense platforms;
- (U) the availability of intelligence, counterintelligence, and security support for acquisition programs and the requirement to use them; and
- (U) guidance and descriptions of support available for protecting technologies.

(U) Navy Policy and Implementation Guidance

(U) Secretary of the Navy Instruction 5000.2D "Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System," October 16, 2008, implements the DoD 5000 series issuances for all Navy acquisition programs. This policy sets forth responsibilities for key acquisition authorities, and states that the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN/RDA) is the Navy Service Acquisition Executive with direct oversight of all Program Executive Officers and PMs.

(U) This policy requires that a program protection plan be developed for all programs with CPI. Moreover, this policy requires the PM to use the "Standard Operating Procedures for the Standardized Critical Program Information Identification Process in Department of Navy Acquisition Programs, Version 1.01, of 26 September 2007," to identify CPI in all acquisition programs.

(U) Each Navy program that contains CPI or critical technology shall prepare a program protection plan that includes a PM-approved classified anti-tamper annex. Additionally, this policy sets forth intelligence support requirements wherein the Office of Naval Intelligence or the Marine Corps Intelligence Activity are required to provide life-cycle threat assessment and intelligence support for all categories of acquisition programs. Also, this policy requires DoN PMs and/or Program Executive Officers considering international cooperation to consult with the Navy International Program Office for development of a strategy that considers security; information release; technology transfer issues; bilateral versus multilateral cooperation; harmonization of military requirements; bilateral test and evaluation; and potential involvement of foreign industry and/or technology in the Navy program.

(U) Secretary of the Navy Manual M-5000.2 "Department of the Navy Acquisition and Capabilities Guidebook," December 2008, is a companion document to Secretary of the Navy (SECNAV) Instruction 5000.2D. Regarding the protection of CPI, this guidebook states that the program protection plan should encompass security, acquisition systems program protection, systems security engineering, counterintelligence, and operations security requirements. Also, since foreign military sales, direct commercial sales, co-development, sales, transfer, loss on the battlefield, or unintended diversion will expose critical technology to potential exploitation or reverse-engineering, this guidebook states that the program protection plan must include an anti-tamper annex. The DoN anti-tamper technical agent assists the PM in preparing and staffing the program protection plan anti-tamper annex. Furthermore, the final program protection plan anti-tamper annex is required to be submitted to the ASN/RDA-Chief Systems Engineer for review and approval.

(U) Department of the Navy "Anti-Tamper Desk Reference," February 1, 2009, provides guidance that assists PMs, System Engineers, and Integrated Product Team members in carrying out anti-tamper countermeasures for the protection of critical technologies inherent in weapons systems. Guidance contained therein details the DoN anti-tamper program's implementation of mandatory DoD 5000 series and DoD Instruction 5200.39 requirements for the protection of CPI.

(U) Secretary of the Navy Manual M-5510.36 "Department of the Navy Information Security Program," June 2006, establishes the Navy's information security program in accordance with SECNAV Instruction 5510.36A "Department of the Navy Information Security Program (ISP) Instruction." The information security program addresses the handling requirements for critical technologies and delineates that the program protection plan is the PM's single source document used to coordinate and integrate all protection efforts designed to deny access to CPI to anyone not authorized, or not having a need-to-know; and prevent inadvertent disclosure of leading edge technology to foreign interests. Moreover, this policy states that if there is to be foreign involvement in any aspect of the program, or foreign access to the system or its related information, the program protection plan must contain provisions to deny inadvertent or unauthorized access.

Additionally, this policy manual provides guidance on security education and the Navy's industrial security program.

(U) Office of the Chief of Naval Operations Instruction 3811.1D "Threat Support to Weapon and Information Technology Systems Planning and Acquisition," June 5, 2008, contains mandatory procedures for Navy implementation of intelligence threat support to U.S. Navy and joint weapon and information technology systems planning and acquisition processes, including threat support for the protection of CPI. This policy states that PMs and Project Leads for acquisition programs and research and development activities shall coordinate and maintain dialogue with the Office of Naval Intelligence or the Marine Corps Intelligence Activity to establish the proper intelligence support for their program. The Office of Naval Intelligence produces threat data and composite threat assessments, e.g. Capstone System Threat Analysis, to support specific classes of RDA programs. The Office of Naval Intelligence threat assessments provide the basic threat documentation for all Navy or Navy-lead joint programs (this includes support to Marine Corps aviation); while the Marine Corps Intelligence Activity provides life-cycle threat assessment and intelligence support for Marine Corps' non-aviation acquisition programs.

(U) Office of the Chief of Naval Operations Instruction 3880.6A "Scientific and Technical Intelligence Liaison Officer (STILO) Program and Intelligence Support for the Naval Research, Development, Test and Evaluation, and Acquisition Communities," November 5, 2007, implements the STILO program. The STILO program is a "community of interest" that strengthens the interface and flow of intelligence between the intelligence community and Navy components that are outside of the intelligence community, (e.g. RDA programs that require intelligence support). The Director of Naval Intelligence is responsible for the overall policy and coordination of the Navy STILO program. The Office of Naval Intelligence STILO is the program coordinator, and is responsible for the day-to-day operations and coordination with all other STILO offices.

(U) Secretary of the Navy Instruction 5430.107 "Mission and Functions of the Naval Criminal Investigative Service," December 28, 2005, establishes the Naval Criminal Investigative Service (NCIS) as the primary investigative and counterintelligence jurisdiction within the Navy. The Director, NCIS, is the senior official for criminal investigations, counterintelligence, and security within the Navy, as well as the senior Navy official responsible for terrorism investigations and related operations. Among its mission areas, the NCIS is required to support RDA protection by conducting counterintelligence activities that protect CPI, and critical technologies or systems.

(U) Additionally, NCIS operates the Navy Multiple Threat Alert Center to provide indications and warning of terrorist, foreign intelligence, cyber, and criminal threats to the Navy and to generate related analysis and production on matters of interest to the Navy, (e.g. the required multidisciplinary counterintelligence threat assessment[3] for RDA programs with identified CPI).

[3] (U) Multidisciplinary counterintelligence threat assessment is an assessment made by the cognizant DoD Component's counterintelligence organization that describes those foreign governments, entities, or activities that have the interest and capability to collect information about a system under development. In accordance with DoD Instruction 5200.39, this intelligence product is requested by the PM when CPI is determined to exist in a program. In order for the multidisciplinary counterintelligence threat assessment to assist in the development of cost effective

(U) Secretary of the Navy Instruction 3052.2 "Cyberspace Policy and Administration Within the Department of the Navy," March 6, 2009, establishes policies and responsibilities for the administration of cyberspace within the DoN. This policy states that horizontal protection of CPI, controlled unclassified information, and supply-chain risk management, is necessary to ensure secure cyberspace systems for the warfighter. The DoN established a capability in cyberspace, enabling the integration of NCIS law enforcement and counterintelligence capabilities throughout the DoN cyberspace domain and network operations centers; and synchronized cyberspace protection capabilities across the Navy RDA and sustainment domain, which includes the Navy supply-chain and Defense Industrial Base partners.

(U) Structure of Report

(U) We organized the results of this assessment into two findings. Finding A discusses the DoN's structure and policies that support CPI protection and details how the DoN's efforts to protect CPI through its foreign visit system could be strengthened to better protect DoN RDA programs and activities. In Finding B, we use the EA-18G as a case study to assess the eight issue areas. We address each issue area separately, focusing on standardization of protection processes and their application, oversight of the protection processes, and responsibility for the protection.

countermeasures, it should advise the PM of known and suspected collection threats to the identified CPI, and define where intelligence gaps exist.

(U) Finding A. Navy Policy and Structure Need Improved Integration for Maximum Protection of Critical Program Information

(U//~~FOUO~~) The DoN policies highlight the different roles and responsibilities of DoN organizations engaged in the protection of CPI and provide a fairly integrated approach for security, intelligence, and counterintelligence support to acquisition programs with CPI. DIA: (b)(3), 50 USC § 3024(i) [redacted]

(U) Players and Roles

(U) Assistant Secretary of the Navy for Research, Development, and Acquisition

(U) The ASN/RDA is the Service Acquisition Executive responsible for DoN acquisition with the authority, responsibility, and accountability for all acquisition functions and programs, and enforcement of USD(AT&L) procedures; and establishes policies and procedures for the management of DoN's RDA activities in accordance with the DoD 5000 series.

(U) As the DoN's principal foreign disclosure authority, the ASN/RDA oversees the foreign disclosure program for the DoN, and ensures that DoN foreign disclosure procedures are in compliance with national disclosure policy, and established foreign disclosure policy, procedures, criteria, and limitations. Moreover, the ASN/RDA is the only DoN official other than the Under Secretary of the Navy who is authorized to deal directly with the Secretary of Defense or Deputy Secretary of Defense regarding DoN requests for exemptions to national disclosure policy or other foreign disclosure matters.

(U) Deputy Assistant Secretary of the Navy for International Affairs, who is also the Director of the Naval International Programs Office, is responsible to the ASN/RDA for implementing policies and managing DoN participation in international efforts concerning RDA. The Director, Naval International Programs Office, makes release determinations for disclosure of classified and controlled unclassified information to foreign governments and organizations in compliance with national disclosure policy and manages certain personnel exchange programs with foreign governments.

(U) Chief of Naval Operations, Director of Naval Intelligence

(U) The Director of Naval Intelligence, is responsible for the development of intelligence policy to support acquisition and sustainment life cycle management. The Director of Naval Intelligence serves as the DoN sponsor for National Intelligence Program and Military Intelligence Program resources, and in coordination with the Marine Corps Director of Intelligence and the Director, NCIS, is responsible for the development of counterintelligence policy.

(U) Additionally, the Director of Naval Intelligence is responsible for overall policy direction and coordination of the DoN Scientific and Technical Intelligence Liaison Officer (STILO) program, with the Office of Naval Intelligence fulfilling the coordination role for the Director.

(U) Scientific and Technical Intelligence Liaison Officer Program was established in 1970 and is specifically designed by the DoN to provide consistent intelligence support, liaison, and coordination among the acquisition, RDT&E, and intelligence communities. The program incorporates a wide range of collaborative techniques and methodologies to ensure effective interagency networking. Efficiencies are gained through identifying, sharing, leveraging, and expanding collaborative relationships and best practices between participating STILO activities. The STILO channels and expedites intelligence flow from the intelligence community to Navy acquisition and research, development, test, and evaluation activities in a manner that consistently satisfies program requirements. This requires that the STILO, who may also be the Senior Intelligence Officer, at each of the Systems Command intelligence office obtain a system threat assessment report[4] for acquisition programs.

(U) Navy Criminal Investigative Service

(U) The Director, NCIS, reports directly to the SECNAV and supports the Director of Naval Intelligence in jointly ensuring the interoperability of intelligence, counterintelligence, security, and law enforcement related databases, systems, and capabilities to the maximum extent possible. Moreover, as the Special Assistant for Naval investigative matters and security to the Chief of Naval Operations, the Director, NCIS, is the senior official for criminal investigations, counterintelligence, and security within the DoN. The NCIS has exclusive jurisdiction within the DoN for providing counterintelligence support to RDA protection. Additionally, commanding officers, acquisition program managers, and technical directors responsible for executing program protection plans are required to incorporate NCIS counterintelligence support plans[5] when configuring plans for risk mitigation and threat countermeasures. NCIS supports DoN commanders, security managers, program managers, facility managers, and technical directors by providing counterintelligence services, including: counterintelligence awareness briefings, foreign intelligence service threat briefings, CPI protection awareness, and counterintelligence analytical products.

(U) Additionally, NCIS established the Multiple Threat Alert Center. The Multiple Threat Alert Center serves as the NCIS fusion center for law enforcement, intelligence, counterintelligence, security, and other threat information. The Multiple Threat Alert Center produces the multidisciplinary counterintelligence threat assessments in support of program protection planning requirements for those RDA programs with inherent and/or inherited CPI.

[4] (U) The system threat assessment report requirement is fulfilled by the production of a capstone system threat assessment. Per Office of the Chief of Naval Operations Instruction 3811.1D, the Office of Naval Intelligence will produce or identify the appropriate capstone system threat assessment or system threat assessment product(s) to support DoN or DoN-led joint programs that fall within the Defense Acquisition Board review authority.

[5] (U) A counterintelligence support plan is an agreement with the customer and the supporting NCIS counterintelligence activity that is used to integrate counterintelligence into the overall security effort. It is a living document that is modified as the technology and/or program, or its CPI transition. The counterintelligence support plan should be revalidated as necessary to ensure currency and relevancy.

(U) Commander, Navy Installations Command

(U) The Commander, Navy Installations Command provides operating forces support and mission support to enhance the Navy's combat power. The Commander, Navy Installations Command, is also responsible for the formulation and dissemination of Navy Security Program policies and standards, ensuring mission essential task standards, performance assessment tools, and force protection drills and exercises are aligned with the metrics and capabilities required.

(U) Naval Air Systems Command

(U) NAVAIR provides full life-cycle support to naval aviation aircraft, weapons, and systems operated by the DoN and the Marine Corps. NAVAIR provides support to Naval Aviation Program Executive Officers and their assigned PMs, who are responsible for the cost, schedule, and performance requirements of their assigned programs. Within NAVAIR, the RDA protection program is both comprehensive and integrated with assigned stakeholders and representatives from NAVAIR security, anti-tamper, foreign disclosure, and the NCIS. NAVAIR RDA protection program developed tools for use in the CPI identification process that were incorporated into the "Standard Operating Procedures (SOP) for the Standardized Critical Program Information Identification Process in Department of Navy Acquisition Programs, Version 1.01, of 26 September 2007." Furthermore, NAVAIR's security division utilizes embedded security personnel within the EA-18G program office that were part of the Procurement Planning Conference[6] process.

(U) Additionally, the DoN Anti-Tamper Technical Authority is located within NAVAIR and has developed tools that assist PMs, System Engineers, and/or Integrated Product Team personnel in the application of anti-tamper processes and techniques. The tools include: the "Anti-Tamper Implementation Checklist for Program Managers," program security management requirements, and the validation and verification process.[7]

[6] (U) The use of the Procurement Planning Conference was noted as a best practice by an USD(I) subject matter expert, since it provides a standard forum for the PM to solicit inputs from integrated product team members, including security from NAVAIR and anti-tamper specialists, who are concerned with developing cost effective countermeasures for the protection of CPI and critical technologies; thus increasing the integration and synchronization of security requirements for the protection of CPI in the acquisition strategy and planning.

[7] (U) Anti-tamper implementation is tested and verified during developmental test and evaluation and operational test and evaluation. The PM develops the validation plan and provides the necessary funding for the anti-tamper validation and verification on actual or representative system components. The validation and verification plan, which is developed to support Milestone C, is reviewed and approved by the Anti-Tamper Executive Agent, or any DoD Component-appointed Anti-Tamper Agent, prior to milestone decision. The program office conducts validation and verification of the implemented anti-tamper plan. The Anti-Tamper Executive agent witnesses these activities and verifies that the anti-tamper plan is implemented into the system and works according to the anti-tamper plan. The PM and the Anti-Tamper Executive Agent may negotiate for parts of the system that have undergone anti-tamper measures to be tested at the Anti-Tamper Executive Agent's laboratories for further analysis. The validation results are reported to the Milestone Decision Authority.

(U) Moreover, NAVAIR developed the Acquisition Security Database for horizontal protection of CPI, which has been adopted by the USD(AT&L) for the application of horizontal protection of all CPI resident in DoD programs.[8]

(U) The Naval Inspector General

(U) The Naval Inspector General inspects security, technology protection, and counterintelligence practices at RDT&E facilities annually. The inspections assess compliance with DoN guidance and identify for DoN leadership ways to improve programs and facility security and disseminate best practices. By focusing on the inspection results, the DoN Inspector General heightens awareness across the community and effectively addresses security vulnerabilities in DoN laboratories and across all DoN programs.

(U) Policies Establishing Roles for Research, Development, and Acquisition Protection

(U) DoD and the DoN continually seek ways to deal with the complexities of program protection because synchronization across so many commands and functional areas is a challenge. DoD policies identify requirements for the protection of CPI across the Services and commands. DoN policy establishes guidelines specific to DoN RDA programs to effect the protection of CPI. Optimally, DoD and DoN policies and practices should be parallel, integrated, and congruent.

(U) Department of Defense Policy

(U) DoD Instruction 5200.39 establishes the responsibilities of the USD(AT&L) for the protection of CPI in DoD acquisition programs. It instructs the USD(AT&L) to lead in the establishment of a consistent process for the identification and protection of CPI, and to require a program protection plan for RDA programs wherein CPI has been identified.

(U) As the milestone decision authority for major defense acquisition programs, the USD(AT&L) also has the lead in establishing procedures outlining program protection plan development and approval in collaboration with the Under Secretary of Defense for Intelligence (USD(I)), the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer (ASD(NII)/DoD CIO)), the Under Secretary of Defense (Policy), and with DoD Components.

(U) In addition, DoD Instruction 5200.39 authorizes the USD(AT&L) to provide direction and management oversight for the identification and protection of CPI for programs under the cognizance of the USD(AT&L).

[8] (U) On July 22, 2010, the USD(AT&L) issued a memorandum designating the Acquisition Security Database as the horizontal protection database for the protection of DoD Component CPI across Services and commands; and required that within 90 days, the Heads of DoD Components submit their respective plans for entering current, future, and legacy RDA programs/projects into the Acquisition Security Database and for updating those records at each milestone.

(U) Department of the Navy Processes and Practices

(U)The primary DoN policies that implement DoD mandates for the protection of CPI are incorporated within SECNAV Instructions 5000.2D, 5430.107, and 5510.36A; and SECNAV Manuals M-5000.2 and M-5510.36. Moreover, these SECNAV policies establish roles and responsibilities for DoN acquisition officials, supporting staff elements, and Systems Commands that fall under the control of the Chief of Naval Operations and the Commandant of the Marine Corps.

(U) On February 20, 2008, the ASN/RDA required the use of the "Standardized Process for the Identification of Critical Program Information (CPI) in DoN Acquisition Programs" in order to integrate a DoN standardized process for evaluating programs for the presence of CPI. Subsequently, these standard operating procedures were incorporated within SECNAV Instruction 5000.2D, and within the Naval Systems Engineering Technical Review Handbook, Version 1.0, which implements Naval Systems Command Systems Engineering Policy.

(U) The process detailed within the standard operating procedures calls for the formation of a multidisciplinary integrated product team, comprised of representatives from the acquisition; engineering; Systems Command RDA protection (e.g. security, operations security, anti-tamper, and threat/intelligence support personnel); Systems Command Foreign Military Sales/Foreign Disclosure Office, intelligence support from the Systems Command STILO; and counterintelligence support from the NCIS. Additionally, these standard operating procedures state that the PM will make personnel available for participating in the integrated product team; and approves the results of the integrated product team, or refers back to the integrated product team for further analysis.

(U) A unique feature within the standard operating procedure is the Program Office Protection Lead, who is appointed by the PM, and is assigned as the PM's primary point of contact for the process described within the standard operating procedures. The Program Office Protection Lead may be a military, government, or contractor person; and is responsible for carrying out or coordinating the process, tracking and documenting progress, and preparing and presenting process results to the PM.

(U) Implementing SECNAV Instruction 5000.2D within NAVAIR, Naval Air Systems Command Instruction 4200.37A "The Procurement Initiation Document Process," makes the PM accountable for overseeing the successful execution of the procurement requirements for assigned programs/systems. The PM will identify CPI for program protection plan purposes, and utilize the Procurement Planning Conference for advance procurement planning and engineering change proposals.

(U) The key Procurement Planning Conference events also serve as milestones to be used by the Program Executive Officer, PM, and the program team members to track the progress of the procurement and engineering change proposal actions that are equal to or greater than $1 million in value. Additionally, implementing guidance for the Procurement Planning Conference can be found in the Naval Air Systems Command Acquisition Guide.

(U) For acquisition programs with foreign involvement, SECNAV Instruction 5000.2D requires that PMs and/or Program Executive Officers consult with the DoN International Programs Office during development of the international element of the program's acquisition strategy to obtain: relevant international programs information; ASN/RDA policy and procedures regarding development, review, and approval of international armaments cooperation programs; and DoN technology transfer policy. Additional guidance found in SECNAV Manual 5000.2 states that if international access, participation, or sales are planned or anticipated, the program protection plan must include annexes regarding a technology assessment and control plan approved by the Milestone Decision Authority, and a delegation of disclosure authority letter approved by the ASN/RDA, who is the principal disclosure authority for the DoN.

(U) Per SECNAV Instruction 5430.107, NCIS supports RDA protection by conducting counterintelligence activities that protect CPI, critical technologies, or systems. The focus of this support is on DoN RDT&E efforts, designated acquisition programs, and systems currently deployed. Moreover, per SECNAV Instruction 3052.2, the NCIS Director is required to coordinate with the ASN/RDA to enhance law enforcement/counterintelligence capabilities and solutions for RDA protection efforts that support the DoN cyberspace domain; and, enable horizontal protection of CPI, controlled unclassified information, and supply-chain risk management across the DoN.

(U) Additionally, per SECNAV Instruction 5510.36A and SECNAV Manual M-5510.36, the Chief of Naval Operations' Special Assistant for Naval Investigative Matters and Security establishes, directs, and oversees the DoN Information Security Program; and is responsible for investigative, law enforcement, physical security, technical surveillance countermeasures, and counterintelligence policy and programs within the DoN.

(U) DIA (b) (3), 50 USC sec. 3024(i) [redacted]

~~(S//NF)~~ DIA (b) (1), EO 13526, secs. 1.4(a) 1.4(c), 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

(U) Key Policies and Directives for Foreign Visits

(U) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005, governs visits and assignments of foreign nationals to DoD Components and cleared contractor facilities, and directs that DoD sponsored visits by foreign nationals to the DoD Components, except visits at activities or events that are open to the general public, shall be documented using the Foreign Visits System – Confirmation Module, ***where practicable*** (emphasis added).

(U) The Directive assigns the Under Secretary of Defense for Policy responsibility to establish DoD policy for programs that entail visits and assignments of foreign nationals to the DoD Component and cleared contractor facilities. The Under Secretary of Defense for Policy also provides oversight of foreign visits and assignments programs covered by the Directive and directs the automation of the Foreign Visits System, the Foreign Visits System – Confirmation Module, and Security Policy Automation Network.

(U) Directive Type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009, directs the use of the Foreign Visits System-Confirmation Module as one of the government authoritative data sources for tracking and confirming visits approved through the Foreign Visits System.

(U) Department of the Navy Foreign Disclosure Manual, September 2007, Sections 20803 and 20808, provide instructions and procedures that implement DoD Directive 5230.20 requirements for the use of the Foreign Visits System. The sections require all DoN Components that are responsible for foreign personnel under their cognizance screen for terrorist and criminal associations prior to arrival, and that arrival and departure dates are documented in an automated system DoD OIG (b)(7)(E) [redacted]

(U) DIA (b)(3), 50 USC sec. 3024(i); [redacted]

~~(S//NF)~~ DIA: (b)(1), EO 13526, sec. 1.4(c); NAVAIR: (b)(1), EO 13526, sec. 1.4(a) [redacted]

(U) DIA (b)(3), 50 USC sec. 3024(i); [redacted]

(U//~~FOUO~~) DIA: (b)(3), 50 USC sec. 3024(i); [redacted]

- (U) DIA: (b)(3), 50 USC sec. 3024(i); [redacted]
- (U) DIA: (b)(3), 50 USC sec. 3024(i); [redacted]
- (U) DIA: (b)(3), 50 USC sec. 3024(i); [redacted]

(U) DIA (b)(3), 50 USC sec. 3024(i); [redacted]

(U) DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

(U//~~FOUO~~) DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

(U//~~FOUO~~) DIA: (b) (3), 50 USC sec. 3024(i). [redacted]

(U) Table – DIA: (b) (3), 50 USC sec. 3024(i), [redacted]

DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

(U) DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

(~~S//NF~~) DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); (b) (3), 50 USC sec. 3024(i); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c), 1.4(g), NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c), 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); 1.4(g), NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c), 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a); NCIS: (b) (1), EO 13526, sec. 1.4(c), 1.4(d) [redacted]

~~(C//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

(U) DIA: (b) (3), 50 USC sec. 3024(i) [redacted]

~~(S//NF)~~ DIA: (b) (1), EO 13526, secs. 1.4(a), 1.4(c); 1.4(g); NAVAIR: (b) (1), EO 13526, sec. 1.4(a) [redacted]

DIA: (b)(1), EO 13526, secs. 1.4(a), 1.4(c), 1.4(g); NAVAIR: (b)(1), EO 13526, sec. 1.4(a) [redacted]

(U) In order to ensure compliance with DoD requirements, it is imperative that short notice visits be held to a minimum. During initial coordination for a potential visit, it should be stressed to an official visitor the importance of meeting the DoD requirement of submitting a foreign visit request a minimum of 30 days in advance of any proposed visit.

(U) People we interviewed identified an incongruity in the implementation of the DoD Foreign Visit System policy and the conduct of DoN physical security arrangements. Discussions with NAVAIR foreign disclosure personnel and Naval Air Warfare Center-Aircraft Division security personnel pointed out that Navy "Regionalization" (grouping of support activities into a regional management structure) resulted in the change of control for physical security from Systems Command to the Commander, Navy Installations Command. The Navy established the Navy Installations Command in October 2003 to oversee 12 regional offices that are responsible for providing operations, quality of life, and facilities management support to Navy bases within a given region. The establishment of the Installations Command shifted responsibility for physical security from the Systems Commands to the Installation Command. In addition, the office of primary responsibility for current Navy physical security guidance is the Director of Materiel Readiness and Logistics.

(U) DoD OIG (b)(7)(E) [redacted]

(U) Conclusion

(U) The DoN policies highlight the different roles and responsibilities and provide a fairly integrated approach for security, intelligence, and counterintelligence support to acquisition programs with CPI. However, the DoD policy for foreign visits, although requiring components to use the Foreign Visits System – Confirmation Module, it has a "where practicable" caveat. The Under Secretary of Defense for Policy is in the process of revising the policy and we were told that the caveat will be removed. However, the policy has yet to be sent out for formal coordination. DoD OIG (b)(7)(E) [redacted] In addition, the need for training on foreign visitor processes and issues for physical security personnel should be determined and provided if needed.

(U) Recommendation, Management Comments, and Our Response

A1. (U//~~FOUO~~) We recommend that the Commander, Naval Installations Command revise the Navy physical security policy DODOIG (b)(7)(E) [redacted]

(U) Management Comments

(U) The Commander, Naval Installations Command, concurred, stating that the Navy Physical Security policy would be revised DODOIG (b)(7)(E) [redacted]

(U) Our Response

(U) The comments of the Commander, Naval Installations Command, are responsive and meet the intent of the recommendation.

(U) Recommendation, Management Comments, and Our Response

A2. (U) We recommended that the Under Secretary of Defense for Policy, in coordination with the Under Secretary of Defense for Intelligence

> **a (U) harmonize the requirements of their respective policies directing the use of the Foreign Visits System – Confirmation Module to confirm the occurrence of official visits by foreign nationals to DoD component facilities where classified, controlled unclassified information, and critical program information are resident.**
>
> **b ~~(S//NF)~~** DIA: (b)(1), EO 13526, secs. 1.4(a), 1.4(c), 1.4(g), NAVAIR: (b)(1), EO 13526, sec. 1.4(a) [redacted]

(U) Management Comments

~~(S//NF)~~ NAVAIR: (b)(3), EO 13526, sec. 1.4(a) [redacted] 1.4(a), 1.4(c); 1.4(g); (b) (3), 50

(U) As an example of the collaboration, the Under Secretary of Defense for Intelligence published DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," on February 24, 2012, which requires the Heads of the DoD Components to establish procedures to accommodate visits to their Component facilities involving access to, or disclosure of, classified information. It further states that visits by foreign nationals to DoD components and facilities (except for activities or events that are open to the public) shall be handled in accordance with [the Under Secretary of Defense for Policy's] DoD Directive 5230.20, "Foreign Visits and Assignments of Foreign Nationals" and documented in the Foreign Visits System - Confirmation Module.

(U) Additionally, DoD Instruction 5200.08, "DoD Physical Security Program," incorporates language regarding the use of the Foreign Visits System - Confirmation Module from Directive Type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control." This instruction is pending formal coordination and is expected to be promulgated in December 2012.

(U) Our Response

(U) The comments of the Under Secretary of Defense for Intelligence and the Defense Technology Security Administration are responsive and meet the intent of the recommendation.

(U) Recommendation, Management Comments, and Our Response

A3. (U) We recommended that the Under Secretary of Defense for Policy review its policy to ensure that the use of the Foreign Visits System – Confirmation Module is mandatory for DoD components, as originally required by the Deputy Secretary of Defense.

(U) Management Comments

(U) The Defense Technology Security Administration concurred, stating that it plans to reissue DoD Directive 5230.20, "Foreign Visits and Assignments of Foreign Nationals," with language that clarifies mandatory use of the Foreign Visits System – Confirmation Module. The Defense Technology Security Agency expects to review and reissue this policy in FY 2013.

Our Response

The comments of the Defense Technology Security Administration are responsive and meet the intent of the recommendation.

(U) Finding B. The Navy's EA-18G Program Efforts to Protect Critical Program Information

(U) Using the DoN's EA-18G as a program of record case study, we assessed program protection efforts for standardization of CPI protection processes and their application, oversight of the CPI protection process and its implementation, and responsibility for the protection of CPI, within the framework of the following eight issue areas:

- (U) ability to identify CPI;
- (U) effectiveness in developing and implementing a program protection plan;
- (U) training efforts for the protection of CPI;
- (U) use of resources for the protection of CPI;
- (U) effectiveness of policies to protect CPI;
- (U) ability of counterintelligence, intelligence, and security to support the protection of CPI;
- (U) effectiveness of the foreign visit program; and
- (U) application of "horizontal protection" of CPI.

~~(S//NF)~~ NAVAIR: (b)(1), EO 13526, sec. 1.4(a) [redacted]

- (U) a program protection survey had not been conducted to ensure contractor implementation of countermeasures as articulated in the program protection plan, nor had implementation been tracked;

- (U) the Defense Security Service was not provided with a copy of the program protection plan and the program office's specific requirements for the cleared contractor and the related documents for the protection of CPI; and the DD Form 254 did not reflect the information needed to protect CPI;

- ~~(S//NF)~~ NAVAIR: (b)(1), EO 13526, sec 1.4(a) [redacted]

- (U) counterintelligence support for the protection of CPI was not tailored to Program Management Air-265, the Program Office for the EA-18G and F/A-18, within the Naval Air Station Patuxent River "umbrella" counterintelligence support plan.

(U) Issue Area One: Ability to Identify Critical Program Information

(U) We assessed this issue area to determine whether published guidance for the identification of CPI is relevant to and adhered to by program, security, intelligence, and counterintelligence personnel. We also sought to determine whether there was a working-level integrated product team to assist with and collaborate on the identification of CPI. If so, we wanted to assess how the mission, composition, and effectiveness of the working-level integrated product team contributed to the identification of CPI and whether the working-level integrated product team performed a functional decomposition of the program or system. We determined that the EA-18G program office had an effective process for identifying CPI.

(U) DoD Instruction 5200.39 states that the USD(AT&L) should:

- (U) lead the effort, in collaboration with the USD(I) and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, to establish a consistent process for the identification and protection of CPI that takes into account the role that research, development, acquisition, counterintelligence, intelligence, security, and systems engineering personnel perform;
- (U) provide direction and management oversight for the identification and protection of CPI for RDA programs under the cognizance or oversight of the USD(AT&L);

(U) One of the USD(AT&L) and the USD(I)-led working groups (see Appendix D) developed a standardized process for identifying CPI and associated countermeasures, to include anti-tamper. A CPI identification handbook that includes a CPI survey. A CPI identification tool is being distributed by the Military Services to their programs.

(U) The EA-18G program office was effective in identifying CPI primarily through implementation of "Standard Operating Procedures (SOP) for the Standardized Critical Program Information Identification Process in Department of Navy Acquisition Programs, Version 1.01, of 26 September 2007." The CPI identification process described within the standard operating procedures involves seven phases that guide program office personnel through the process, as follows:

- (U) Phase 1 – Request Validation: During this phase, it is determined if the program meets the necessary criteria for CPI evaluation, which employs the CPI Validation Tool which must be completed by RDA protection security representative.

- (U) Phase 2 – Team Selection: During this phase, the PM with the assistance of RDA protection security representatives ensures that the appropriate personnel are included in the CPI integrated product team.

- (U) Phase 3 – Team Training: During this phase, the integrated product team participants receive training in the definition of CPI, potential indicators of CPI, and process tools.

- (U) Phase 4 – External Review: During this phase, the integrated product team reviews and evaluates program data and technology to determine if external information sources may affect Candidate CPI.
- (U) Phase 5 – Internal Review: During this phase, the information compiled during the previous External Review phase compares program data or technologies against specific CPI criteria in order to develop a list of Candidate CPI.
- (U) Phase 6 – Candidate CPI List: During this phase, the integrated product team, in conjunction with other interested parties, e.g., NCIS, the Foreign Disclosure Office, is tasked to reach agreement on the Candidate CPI, which in turn becomes the basis for the selection of the final list of CPI.
- (U) Phase 7 – Final CPI List: This final phase of the CPI identification process involves PM agreement and approval of the final CPI list. Should the PM not give an approval, the effort returns to Phase 6 for additional analysis of the Candidate CPI list; the updated CPI list is then returned to the PM for approval. Subsequent to PM approval, CPI is uploaded into the Acquisition Security Database.

(U) EA-18G Integrated Product Team

(U) The EA-18G Integrated Product Team was comprised of representatives from NAVAIR engineering, NAVAIR RDA protection offices (e.g. security, operations security, anti-tamper and threat/intelligence support personnel), NAVAIR foreign military sales/foreign disclosure office, NAVAIR STILO, and NCIS.

(U) The EA-18G PM ensured that the Integrated Product Team utilized the Navy's standard operating procedures for CPI identification and successfully used a cross-discipline integrated product team that included systems engineers in accordance with the DoD Instruction 5200.39 requirement for cross-discipline teams.

(U) One of the USD(AT&L) and the USD(I)-led working groups (see Appendix D) developed a standardized process for identifying CPI and associated countermeasures, to include anti-tamper. A CPI identification handbook that includes a CPI survey. A CPI identification tool is being distributed by the Military Services to their programs.

(U) Naval Air Systems Command Research, Development, and Acquisition Protection Efforts

(U) The NAVAIR RDA protection program developed tools for use in the CPI identification process that were incorporated into the "Standard Operating Procedures (SOP) for the Standardized Critical Program Information Identification Process in Department of Navy Acquisition Programs, Version 1.01, of 26 September 2007."

(U) The NAVAIR Security division utilized embedded security personnel within the EA-18G program office that were part of the CPI identification and protection process. Moreover, NAVAIR developed the Acquisition Security Database for horizontal protection of CPI, which has been adopted by the USD (AT&L) for the application of horizontal protection of CPI resident within all DoD programs. On July 22, 2010, the USD (AT&L) issued a memorandum designating the Acquisition Security Database as the horizontal protection database for the protection of DoD Component CPI across services and commands.

(U) EA-18G Anti-Tamper

(U) Within the DoN, the Anti-Tamper Technical Authority, located within NAVAIR developed tools that assist PMs, Systems Engineers, and integrated product team personnel in the application of anti-tamper processes and techniques, including the "Anti-Tamper Implementation Checklist for Program Managers," program security management requirements, and the validation and verification process. The CPI for the EA-18G included not only inherent CPI that was unique to the EA-18G, but also included CPI inherited from earlier variants. For anti-tamper purposes, CPI was identified as either "on board" (susceptible to reverse engineering) or "off board" (not susceptible to reverse engineering). Additionally, if the CPI will be included in an export configuration sold to foreign customers, the requirement for anti-tamper was noted.

(U) Conclusion

(U) EA-18G program office staff had an effective process for identifying CPI and anti-tamper requirements. The process used an integrated product team and the standard operating procedures. The Anti-Tamper Technical Authority, located within the NAVAIR developed tools that assist in the application of anti-tamper processes and techniques. The NAVAIR Security division utilized embedded security personnel within the EA-18G program. The USD(AT&L) and the USD(I) led a working group formed to improve the protection of CPI by, among other things, developing a standardized process for identifying CPI. A CPI identification handbook that includes a CPI survey and a CPI identification tool is being distributed by the Military Services to their programs. We make no recommendations for this issue area.

(U) Issue Area Two: Effectiveness in Developing and Implementing a Program Protection Plan

(U) We assessed this issue area to determine whether published guidance for the planning of program protection is relevant and adhered to by program, intelligence, counterintelligence, and security personnel and to ensure that program protection planning was in accordance with DoD Instruction 5200.39.

(U) At the time of this assessment, the EA-18G program office had a completed program protection plan which contained key elements. DoD OIG: (b)(7)(E) [redacted]

(U) Program Protection Plan Guidance

(U) DoD Instruction 5200.39 states that it is DoD policy to require that contracts supporting RDA programs where CPI has been identified contain language requiring the contractor to protect the CPI to DoD standards. DoD Instruction 5200.39 also states that the USD(AT&L) should:

- (U) require a program protection plan for all RDA programs with CPI within the purview of the USD(AT&L) and establish procedures outlining the program protection plan development and approval process in coordination with the Under Secretary of Defense (Intelligence), the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, the Under Secretary of Defense (Policy), and the DoD Components; and
- (U) lead the collaboration with the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer and the DoD Components for review of major Defense acquisition programs' program protection plans for sufficiency before their Defense Acquisition Board milestone decision reviews and at major acquisition strategy updates.

(U) The program protection plan is used to develop tailored protection guidance for dissemination and implementation throughout the program for which it is created. The layering and integration of the selected protection requirements documented in a program protection plan provide for the integration and synchronization of CPI protection activities. The following are considered key elements of a program protection plan and are tailored to meet the requirements of a RDA program:

- (U) technology and project description or system and program description, with an emphasis on what is unique, as the foundation for identifying CPI;
- (U) list of CPI to be protected in the program (this generally describes classified CPI in an unclassified manner and is not suitable for horizontal protection analysis or the preparation of a counterintelligence assessment);
- (U) threats to CPI;
- (U) foreign threats;
- (U) a summary of the counterintelligence assessment (the full report is an attachment to the plan);

- (U) vulnerabilities of CPI to identified threats;
- (U) countermeasures (all disciplines, as appropriate);
- (U) counterintelligence support plan;
- (U) anti-tamper annex;
- (U) operations security plan;
- (U) system assurance;
- (U) technology assessment/control plan;
- (U) classification guides;
- (U) protection costs; and
- (U) follow-on support.

(U) EA-18G Program Planning

(U) The EA-18G program is mature in its program protection planning. Milestone C for the EA-18G began April 4, 2007, with initial operating capability in September 2009. The current program protection plan dated March 14, 2007, incorporates the previous program protection plans for both the FA-18E/F and EA-18G, and includes multiple annexes, i.e., the security classification guide; the multidisciplinary counterintelligence threat assessment; an open source assessment; a classified anti-tamper plan; the technology assessment and control plan; and additional classified annexes.

(U) Also, the EA-18G contract required the implementation of an Acquisition Program Protection Program that is aligned with the EA-18G program protection plan. The contract required that a program protection implementation plan be developed and delivered as a contract data requirements list item by May 24, 2011. The plan would inform the EA-18G program management office how the contractor intended to protect CPI and implement the countermeasures articulated in the program protection plan; the contractor provided a draft version on May 24, 2011 and worked with the program office to complete the final version in December 2011.

(U) Of particular note, is that the program office has a comprehensive program protection implementation plan data item description that can be used repetitively for program protection implementation planning. The data item description is also located on the Acquisition Streamlining and Standardization Information System (also known as ASSIST) database.[9] The program protection implementation plan data item description is a result of the program protection requirements set forth in the statement of work, DoD contract, the program protection plan (including annexes), DD Form 254, the most current issuances, and applicable security classification guides. The data item description contains the format, content, and intended information for the data product resulting from the work task described in the contract statement of work.

(U) Security Support

(U) We found that the NAVAIR security division embedded security personnel within the EA-18G program office; however, this is not typical of DoN program's outside of NAVAIR. This EA-18G security arrangement provided direct support of the PM's

[9] ASSIST is a database system for DoD-wide standardization document information management. ASSIST-Online is a robust, comprehensive web site providing access to current information associated with military and federal specifications and standards in the management of the Defense Standardization Program. ASSIST is the official source of DoD specifications and standards.

implementation of the program protection plan and resulted in the assigned security personnel closely working with the contract management office and prime contractor security representatives in the development of a program protection implementation plan.

(U) We also found that while the EA-18G embedded security arrangement was beneficial in many ways, security personnel did not ensure that the program protection survey required by the program protection plan was conducted. A program representative stated that this was due to insufficient security personnel assigned to the program. According to the EA-18G program protection plan:

> (U) The PM, assisted by applicable security and CI [counterintelligence] activities, will assess the Program Protection Plan effectiveness, and Research and Technology Protection countermeasures prescribed herein, as part of the normal program review process. Security surveys will be the primary method used to perform these assessments. Such assessments shall be planned during each phase of an acquisition program considering the overall schedule, the time-phased arrival or development of system CPI at specific locations, and the schedule to revise the program protection plan.

(U) Defense Security Service Support

(U) A counterintelligence support plan existed between the NCIS and the NAVAIR that indicated coordination with the Defense Security Service[10] had occurred. However, Defense Security Service personnel responsible for coverage of the prime contractor's facilities were not informed of the existence of CPI for the EA-18G. Program management offices should notify the Defense Security Service office covering cleared contractor facilities holding CPI of the CPI and its presence, nature, and any special concerns (unique compromising characteristics).

(U) Defense Security Service personnel also reported that they were not provided the most recent multidisciplinary counterintelligence threat assessment from the NCIS; instead they were utilizing an older NCIS produced multidisciplinary counterintelligence threat assessment that identified threat information which was consistent with their local observations.

(U) Conclusion

(U) The EA-18G program protection plan was found to be complete. However, the EA-18G PM had not ensured contract requirements for CPI followed-up to discern if the countermeasures articulated in the program protection plan were being implemented and there were insufficient security personnel. Defense Security Service personnel were not informed that CPI resided within the prime contractor's and subcontractors' facilities because CPI was not identified in the DD Form 254.

[10] (U) The Defense Security Service assists DoD Component counterintelligence elements in coordinating the execution of a counterintelligence support plan at cleared Defense contractors with CPI; develops and conducts training for DoD and Defense contractor security personnel regarding CPI protection activities; publishes and disseminates unclassified and classified suspicious activity or equivalent reports, including those related to CPI, to the cognizant DoD Component CI element; and during the conduct of regularly scheduled security inspections at cleared Defense contractor facilities, determine if there are any contractually imposed protection measures for CPI related to classified contracts at these locations.

(U) Recommendation, Management Comments, and Our Response

B2. (U) We recommended that the EA-18G Program Manager

a. **(U) conduct a program protection survey to ensure that countermeasures articulated in the program protection plan are fully implemented and meeting specific milestone dates for their implementation; develop a tracking system for monitoring the implementation of the countermeasures; conduct site visits to assess the contractor's implementation of the countermeasures; and use the results of the site visits to evaluate the effectiveness of the countermeasures.**

b. **(U) provide the Defense Security Service with a copy of the program protection plan and the program office's specific requirements for the cleared contractor and the related documents for the protection of critical program information.**

c. **(U) ensure the DD Form 254 reflects the information needed to protect critical program information.**

(U) Management Comments

(U) The Assistant Secretary of the Navy for Research, Development, and Acquisition, and the EA-18G Program Manager concurred. The EA-18G Program Manager provided the following:

B2a. (U) Despite being understaffed, the Program Manager understands the importance of conducting program protection surveys and has begun to schedule the surveys, beginning in May 2012, and has requested the development of administrative aids from the Naval Air Systems Command Technology Protection Office, to conduct the surveys. They have also requested the establishment of a repository database of survey results to institutionalize best practices within Navy acquisition programs and defense industry partners.

B2b. (U) The EA-18G Program Manager has generated copies of the current program protection plan on a compact diskette, as well as developing a tracking system for deliveries of program protection plans to Defense Security Service representatives listed on the DD Form 254 of contracts that are currently in place. The first delivery was April 24, 2012.

B2c. (U) Naval Air Systems Command updated their DD Form 254 Manual, to include additional language on program protection implementation plan requirements to include referring to the program protection implementation plan contract data requirements list and the disposition of the program protection plan by the technical point of contact/contracting officer representative.

(U) Our Response

(U) The comments of the Assistant Secretary of the Navy for Research, Development, and Acquisition, and the EA-18G Program Manager are responsive and meet the intent of the recommendation.

(U) Issue Area Three: Training Efforts for the Protection of Critical Program Information

(U) We assessed this issue area to determine whether published guidance for training to identify and protect CPI is relevant and adhered to by program, intelligence, counterintelligence, and security personnel. We determined that training and education for the protection of CPI was not tailored to the specific roles that are involved in RDA protection. However, significant progress has been made since the first report in this series.

(U) DoD Instruction 5200.39 requires that appropriate training be available to RDA personnel regarding the identification and protection of CPI. Training should include the roles that RDA, sustainment (logistics, maintenance, repair, supply), testing, counterintelligence, intelligence, security, systems engineering, and information systems security engineering personnel perform to identify and protect CPI.

(U) While the amount of experience varied, the majority of the personnel interviewed about DoN and EA-18G program CPI protection efforts had many years of experience on major weapon system acquisition programs. However, the level of training related to CPI protection varied. There were personnel with no training, those with training acquired on the job, and others with training offered by the RDA program support organization.

(U) Available training varied significantly. The level 1 and 2 acquisition courses at the Defense Acquisition University minimally address counterintelligence, intelligence, and security support to RDA protection. The Joint Counterintelligence Training Academy offers counterintelligence support to RDA protection training and provides advanced counterintelligence training to Defense counterintelligence components. The Academy also provides training to other intelligence community personnel on a limited basis. However, the counterintelligence support to RDA protection training is not structured for non-counterintelligence personnel, who typically provide a large share of the RDA protection support to PMs.

(U) In DoD IG Report No. 10-INTEL-07, "DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network – Tactical," July 21, 2010, we recommended that the USD(AT&L), in collaboration with the USD(I) and the ASD(NII)/DoD CIO develop standardized guidance for training in CPI protection for use by the RDA protection community. In order to begin to address the void in the training of DoD and contractor security personnel in the protection of CPI, the Defense Security Service's Center for Development of Security Excellence developed computer-based and instructor-led courses that focus on DoD policy involving: the protection of CPI; the program protection planning process; threat and vulnerability analysis; risk management; the application of anti-tamper methods and security countermeasures to CPI; and key documents involved in the protection of CPI. After extensive beta-testing, the Center for Development of Security Excellence recently added a web-based course entitled "Introduction to Critical Program Information" to their training catalog.

(U) Additionally, the International Programs Security Requirements Course, offered through the Defense Institute of Security Assistance Management, was developed in response to a directive from the Deputy Secretary of Defense that every DoD employee who is involved in international programs would receive training in the security arrangements that protect sensitive and classified technology and military capabilities, including the laws, policies, and procedures that govern foreign involvement in DoD programs. This requirement was codified within DoD Directive 5230.20 "Visits and Assignments of Foreign Nationals," June 22, 2005. The Defense Institute of Security Assistance Management developed the International Programs Security Requirements course for delivery formats in both resident instructor-led courses, and computer-based courses.

(U) The International Programs Security Requirements course compliments the protection of CPI training found in Defense Acquisition University and Defense Security Service courses, but places emphasis on the acquisition process for international programs, National Disclosure Policy, U.S. export law, and procedures impacting DoD programs, visits, and assignments of foreign nationals, as well as Multinational Industrial Security Working Group procedures.

(U) Conclusion

(U) Training and education for the protection of CPI was not tailored to the specific roles that are involved in RDA protection. RDA program support organizations, the Defense Acquisition University, and the Defense Security Service should be considered delivery mechanisms for training. In response to a recommendation in a previous report in this series, the Defense Security Service's Center for Development of Security Excellence recently added a web-based course entitled "Introduction to Critical Program Information" to their training catalog. Other efforts are also being made. Therefore, we make no additional recommendations, but will follow up on implementation of the prior recommendations.

(U) Issue Area Four: Use of Resources for the Protection of Critical Program Information

(U) We assessed this issue area to determine whether program, intelligence, counterintelligence, and security personnel assigned to protect CPI are appropriately used.

(U) The F/A-18 E/F and EA-18G program protection plan included an estimate of costs for program protection from FY2006 to FY2009 of approximately $1.7 million annually. These estimated program protection costs were unique to Government functions that supported the F/A-18E/F and EA-18G programs. These costs included "personnel costs" that included Program Management Air-265 Government and contractor support labor for the management and implementation of the F/A-18E/F and EA-18G program protection plan; "product costs" associated with the development and update of the program protection plan; "service costs" for the conduct of program protection surveys, training, and related activities; "equipment costs" for procurement of items not available in the existing infrastructure where CPI was located; and "travel costs" for Program Management Air-265 Government and contractor support. These program protection costs do not include funding for standard facility overhead functions such as physical or operational security costs that were part of the prime contracts that supported the F/A-18E/F and EA-18G programs, specifically, costs associated with "Program Security" required under contract for the EA-18G. The contract required a program protection implementation plan as a deliverable contract data requirements list. The program security terms and conditions of the contract required the contractor to implement and maintain an Acquisition Program Protection program in accordance with the contract statement of work, DD Form 254, and EA-18G program protection plan.

(U) Program Security Support

(U) The program received security support from NAVAIR that was embedded with the EA-18G program. However, according to Navy security personnel this is not typical of DoN programs outside of NAVAIR. This security arrangement provided direct support of the PM's implementation of the program protection plan; and permitted the assigned security personnel to work closely with the contract management office and prime contractor security in the development of a program protection implementation plan. Security personnel assigned to the EA-18G program did not conduct the program protection survey required by the program protection plan. According to a program representative, there was insufficient security personnel to do the program protection survey. As a result, there was no measure of the implementation of countermeasures delineated by the EA-18G program protection plan.

(U) Threat Products

(U) The PM is required to obtain intelligence and counterintelligence threat products in order to make informed objective risk management decisions, and thereby employ the most cost effective countermeasures to the protection of the CPI in the program. The EA-18G program protection plan stated that the multidisciplinary counterintelligence threat assessment was based on the CPI list of August 2005 and would be updated every two (2) years.

(U) The multidisciplinary counterintelligence threat assessment that supported the EA-18G program protection plan was produced by the NCIS Multiple Threat Alert Center January 4, 2006. To date, the Multiple Threat Alert Center has not issued an updated multidisciplinary counterintelligence threat assessment that supports the EA-18G program protection plan.

(U) DoD policy requires that the multidisciplinary counterintelligence threat assessment be available to the PM no more than 120 days after CPI is identified. Both DoD and USN policies require the PM to develop a program protection plan based on the threat to CPI during the development and production of the weapons platform. The period of time between when CPI is identified in a program and the program protection plan is finalized is dependent on how quickly the servicing counterintelligence organization responds to the PM's request for counterintelligence threat products.

(U) The Multiple Threat Alert Center reported that NCIS analysts at the Multiple Threat Alert Center lacked engineering skill competencies that would assist in the analysis of science and technology matters. The NCIS analysts were primarily counterintelligence agents skilled in development of human intelligence reporting. The Multiple Threat Alert Center acknowledged this shortcoming and was working with the Office of Naval Intelligence to obtain science and technology expertise for its multidisciplinary counterintelligence threat assessment products.

(U) Defense Security Service

(U) The Defense Security Service is responsible for approximately 13,000 cleared facilities. According to the Defense Security Service, [redacted] industrial security representatives to cover cleared facilities and of counterintelligence personnel to provide support to the protection of CPI in cleared companies. In a January 15, 2009, memorandum, the Deputy Secretary of Defense directed that the resources necessary to implement recommendations from a 2008 Defense Security Service Future Options Study be added to the Defense Security Service program for FYs 2010-15.

(U) These resources include [redacted] full-time equivalents to strengthen the Defense Security Service and allow it to more effectively accomplish its mission: industrial security, education and training, counterintelligence, and information technology. Although the number of counterintelligence personnel supporting the CPI threat assessment process is increasing, [redacted] cleared defense facilities. However, even with increased resources, the Defense Security Service must be apprised of the existence of CPI and the protection plans. In Issue Area Two, we recommended that the EA-18G Program Manager give the Defense Security Service a DD Form 254, with CPI protection requirements and a copy of the program protection plan.

(U) Conclusion

(U) There was a lack of counterintelligence resources with the appropriate technical skills that support the protection of CPI. Moreover, the EA-18G program office attributed insufficient assigned security personnel to the program's failure to conduct the program protection survey required by the program protection plan. However, the required program protection implementation plan was not completed until December 2011. Without a completed and comprehensive program protection implementation plan, any survey would be incomplete and the Program Manager would have no measure of the implementation, much less the effectiveness, of countermeasures delineated by the EA-18G program protection plan.

(U) Similar findings related to personnel have been reported in the prior two reports in this series, DoD IG Report No. 10-INTEL-07, "DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network-Tactical," July 21, 2010, and Report No. 11-INTEL-08, "DoD Efforts to Protect Critical Program Information: The Air Force's Family of Advanced Beyond Line-of-Sight Terminals," April 15, 2011. Because of the many organizations we visited as part of this broad assessment and the upcoming budget cuts, we make no recommendations regarding the shortage of resources. However, DoD management at all levels needs to ensure that the correct skills are available, leverage existing resources, and identify and mitigate the risk associated when requirements are not or can not be met. Our report "DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network-Tactical," recommended that standardized guidance be developed for training in CPI protection for use by the research and technology protection community. The training should also encompass the new requirements to protect elements or components critical to network or mission effectiveness. In addition, the Defense Security Service has introduced a web-based course, "Introduction to Critical Program Information," as well as additional efforts being developed within the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Ensuring that acquisition staff, security personnel, and the intelligence/counterintelligence personnel understand the process and requirements can mitigate shortages in staff.

(U) Issue Area Five: DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

(U) DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

(U) DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

(U) DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

(U) DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

[11] (U) DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

(U) Conclusion

(U) DIA: (b) (3), 50 USC sec. 3024(i); [redacted]

(U) Issue Area Six: Ability of Counterintelligence, Intelligence, and Security to Support the Protection of Critical Program Information

(U) We assessed this issue area to determine whether published guidance to enable counterintelligence, intelligence, and security personnel and programs to support the protection of CPI is sufficient, relevant, and properly implemented. DoD Instruction 5200.39 requires the heads of DoD Components with counterintelligence elements and organizations to:

- (U) develop and implement tailored counterintelligence support plans for all RDA programs with CPI;
- (U) provide assessments regarding foreign intelligence requirements for and targeting of CPI;
- (U) provide Technology Targeting Risk Assessments[12] to assist RDA programs with mitigating the risk of CPI compromise; and
- (U) provide counterintelligence assessments for RDA programs with CPI.

(U) The NAVAIR STILO, NAVAIR security and foreign disclosure personnel, and assigned NCIS counterintelligence personnel were co-located, and had a close working relationship at NAVAIR headquarters. Additionally, the NAVAIR STILO served as a conduit to provide engineering, scientific, and technical support and foreign materiel intelligence collection activity, and tip-offs from NAVAIR to the Office of Naval Intelligence. Furthermore, it was noted that EA-18G program management personnel utilized support from each of these disciplines in their program protection planning.

(U) Although the NCIS had an overarching or "umbrella" counterintelligence support plan for NAVAIR, the overarching plan was not tailored for the EA-18G program. However, EA-18G program staff did request and were provided requisite counterintelligence and intelligence support and threat-related data. Also, counterintelligence personnel were known to EA-18G program staff, but Defense Security Service personnel were not. As a result, the Defense Security Service was not informed of the existence of EA-18G CPI. In addition, the existence of CPI or a program point of contact for reporting violations annotated on the DD Form 254 was not provided.

(U) Counterintelligence Support

(U) Counterintelligence personnel were known to EA-18G program management office personnel, participated in the CPI identification process, but did not provide a counterintelligence support plan tailored to the Program Management Air 265/EA-18G.

[12] Country-by-country assessments conducted by the Defense intelligence community that quantify risks to critical program information and related enabling technologies for weapons systems, advanced technologies or programs, and facilities such as laboratories, factories, research and development sites (test ranges, etc.), and military installations. The Technology Targeting Risk Assessment evaluates five independent risk factors, each of which contributes to an overall risk factor. The five areas evaluated are: technology competence, national level of interest, risk of technology diversion, ability to assimilate, and technology protection risk. The Technology Targeting Risk Assessment and counterintelligence assessment provide laboratory/technical directors and PMs with information required to establish a comprehensive security program for the protection of identified critical program information.

Therefore, program management staff was not aware of what to expect with regard to EA-18G specific counterintelligence support. Instead, staff relied on an umbrella counterintelligence support plan issued in June 2009 for all of NAVAIR. A counterintelligence support plan outlines the provision of counterintelligence support to be provided by NCIS to a specific program. The absence of a specific counterintelligence support plan focused on a RDA program with resident CPI may impact the level of counterintelligence resources dedicated to the protection of the RDA program's CPI.

(U) The NCIS agent assigned to NAVAIR informed us that the protection of CPI was one of a multitude of priorities. Though this assessment only represents one instance of NCIS support to RDA protection, the lack of an EA-18G specific counterintelligence support plan was not in harmony with SECNAV Instruction 5430.107, which states that:

> NCIS shall support Research and Technology Protection (RTP) by conducting counterintelligence activities that protect CPI, technologies, and systems. The focus of this support is on DoN research, development, technology, and evaluation (RDT&E) efforts, designated acquisition programs, and systems currently deployed. NCIS has exclusive jurisdiction within the DoN for providing CI support to RTP.

(U) A June 2009 "Security, Technology Protection, and Counterintelligence" inspection of NAVAIR conducted by the Naval Inspector General noted that NCIS was primarily focused on criminal investigations and that due to NCIS manning levels, "the task to provide consistent counterintelligence support (agent services and timely analytical products) to Naval Air Systems Command and its program managers is a challenging evolution." Similarly, the Naval Inspector General noted inadequate manning levels of NCIS agents for Naval Sea Systems Command for an umbrella counterintelligence support plan that covered "80-plus programs" and stated that "the quality of analysis and timeliness of the threat information requires additional resources to further complement the counterintelligence support plan."

(U) Thus, there was no counterintelligence support plan specifically agreed to with Program Management Air-265 – the NAVAIR program management organization responsible for the EA-18G and F/A-18E/F programs. Additionally, the "umbrella" counterintelligence support plan that existed for NAVAIR indicated liaison with Defense Security Service personnel located in proximity to Naval Air Station – Patuxent River, MD. However, we found little or no liaison between NCIS and the Defense Security Service representatives who were responsible for industrial security and counterintelligence at cleared Defense contractor facilities where EA-18G's CPI was located.

(U) Integrated Program Security Support

(U) NAVAIR security personnel were embedded in the EA-18G program management office and had submitted requirements for threat data via the servicing NCIS office. The Naval Inspector General identified that having security personnel embedded in the program was a best practice; we agree.

(U) Despite having security personnel embedded in the program, security surveys, the primary method used to assess the effectiveness of CPI measures, were not done. According to the EA-18G program protection plan, the PM, assisted by applicable security and counterintelligence activities, should assess program protection plan effectiveness, and research and technology protection countermeasures prescribed herein, as part of the normal program review process. Such assessments shall be planned during each phase of an acquisition program considering the overall schedule, the time-phased arrival or development of system CPI at specific locations, and the schedule to revise the program protection plan for the EA-18G. However, no program protection surveys had been accomplished. According to program representatives, there were not enough security personnel embedded to be able to conduct program protection surveys to assess the overall implementation of the EA-18G program protection plan countermeasures. The lack of surveys was previously addressed in Issue Area Four.

(U) Threat Products

(U) In accordance with DoD Instruction 5000.02 requirements and Navy Instruction 3880.6, the EA-18G PM requested the production of a System Threat Assessment Report through the NAVAIR STILO. The Office of Naval Intelligence responded to this request and produced a Defense Intelligence Agency validated Capstone System Threat Assessment. The Capstone System Threat Assessment for the EA-18G was produced as an "umbrella" System Threat Assessment Report by the Office of Naval Intelligence. The pertinent Capstone System Threat Assessment, "(U) Capstone System Threat Assessment: Naval Fixed-Wing Aircraft," June 30, 2007, addressed with specificity the EA-18G program.

(U) The NCIS Multiple Threat Assessment Center, which serves as a unique all-source fusion center that blends critical threat information from intelligence, counterintelligence, law enforcement, and security reporting, also responded to a request for a multidisciplinary counterintelligence threat assessment. In accordance with DoD Manual 5000.1-M requirements, the Multiple Threat Assessment Center produced a multidisciplinary counterintelligence threat assessment for the EA-18G program, "The Fighter/Attack-18E/F Supper Hornet (F/A-18E/F) and Electronic Attack-18G (EA-18G) (U)" on January 4, 2006. However, this multidisciplinary counterintelligence threat assessment provided no information regarding CPI located at cleared Defense contractors that were supporting the programs. The absence of this information may negatively impact the integration of Defense Security Service mission coverage in support of the protection of CPI in an industrial setting. NCIS did not provide updated threat briefings periodically. According to program management staff, NCIS would provide an updated multidisciplinary counterintelligence threat assessment if and when there was a specific threat to the program's CPI.

(U) Review of the January 3, 2006, NCIS multidisciplinary counterintelligence threat assessment for the F/A-18E/F and EA-18G depicted threat criterion for collection efforts targeting the F/A-18E/F and EA-18G critical technologies, e.g. AN/APG-79 Active Electronically Scanned Array (AESA) radar, as "Medium." However, the January 29, 2004, multidisciplinary counterintelligence threat assessment, for the same critical technology and involving the same country's collection efforts, was ascribed as "High." This different assessment was not addressed in the multidisciplinary counterintelligence threat assessment for the F/A-18E/F and EA-18G.

(U) The Defense Intelligence Agency Defense Warning Office also produced technology targeting risk assessments for the F/A-18E/F Super Hornet and "Technology Risks Incurred by the Export of U.S. Fighter Aircraft and Air Deliverable Weapons" that could have provided the PM enhanced threat perspectives for EA-18G program protection planning, since there was a commonality of CPI and critical technologies that the EA-18G program received from the FA-18E/F. These Technology Targeting Risk Assessments were produced in 2005 and available to the intelligence community.

(U) The NCIS Multiple Threat Assessment Center did not reference the Defense Intelligence Agency's tailored analysis contained in these technology targeting risk assessments in the EA-18G multidisciplinary counterintelligence threat assessment. Additionally, the technology targeting risk assessments were not given to the EA-18G program management as stand-alone threat products. Both DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008, and DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, require the integration of a Technology Targeting Risk Assessment with the appropriate counterintelligence analytical product to address foreign collection threats to RDA programs with CPI.

(U) Defense Security Service

(U) U.S. industry develops and produces the majority of our Nation's defense technology and thus plays a significant role in creating and protecting the information that is vital to our Nation's security. The National Industrial Security Program was established by Executive Order 12829, "National Industrial Security Program," January 6, 1993, to ensure that cleared U.S. defense facilities safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Defense Security Service administers the National Industrial Security Program on behalf of DoD and 23 other federal agencies. The Defense Security Service has responsibility for over 13,000 active, cleared facilities in the National Industrial Security Program.

(U) In accordance with DoD Instruction 5200.39, the Defense Security Service assists DoD counterintelligence elements in coordinating the execution of counterintelligence support plans at the facilities of cleared Defense contractors with classified CPI. The contract's DD Form 254, which includes security requirements and classification guidance for facilities with classified contracts, should indicate the existence of CPI so that the Defense Security Service will know what areas need enhanced levels of protection.

(U) The DD Form 254 also needs to identify cleared Defense contractors working on classified contracts with classified or unclassified CPI, as well as employees with access to the locations where classified contracts with classified or unclassified CPI reside. The Defense Security Service is developing procedures to centralize the receipt, analysis, and dissemination of such information in a manner that permits maximum control and use. Defense PMs must furnish the Defense Security Service with a copy of the program protection plan and counterintelligence support plan to adequately provide overlapping counterintelligence support to protect CPI. In addition, the identification of all subcontractors working on classified programs with classified or unclassified CPI as well as a program point of contact would further improve the protection of CPI.

(U) Defense Security Service personnel told us that specific to the EA-18G program, there was insufficient communication between the Defense Security Service and the prime contractor regarding subcontractors and the requirements established by program office staff for the protection of CPI.

(U) If the program's DD Form 254 had specified the existence of unclassified CPI and the requisite protection measures, the Defense Security Service could have incorporated CPI protection requirements into its facility inspections. The DD Form 254 could also have included a program point of contact for reporting violations and counterintelligence concerns. With this information, the Defense Security Service could better assist in efforts to safeguard CPI by reviewing the levels of CPI protection during the course of regular inspections of the cleared Defense facility.

(U) Conclusion

(U) In general, counterintelligence, intelligence, and security organizations provided the required threat and risk assessments. However, NCIS did not provide a counterintelligence support plan tailored specifically to Program Management Air-265 - the NAVAIR program management organization responsible for the EA-18G and F/A-18E/F programs. In accordance with both DoD Instructions 5200.39 and O-5240.24, a tailored counterintelligence support plan is required to be developed and implemented in support of RDA programs with CPI, DoD component-designated RDT&E facilities, and cleared defense contractors considered essential by a RDA PM and where CPI is present.

(U) Actions are being taken based on recommendations in our first two reports in this series, DoD IG Report No. 10-INTEL-07, "DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network-Tactical," July 21, 2010, and Report No. 11-INTEL-08, "DoD Efforts to Protect Critical Program Information: The Air Force's Family of Advanced Beyond Line-of-Sight Terminals," April 15, 2011. The Deputy Under Secretary of Defense for Intelligence and Security will include guidance in the forthcoming protection of CPI manual on what can and should be contained in the DD Form 254, including how program protection should be implemented at the level of subcontractors. Additionally, the USD(I) recently promulgated DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, which directs the integration of a technology targeting risk assessment with the appropriate CI analytical product to address foreign collection threats; provides for threat analysis to support supply chain risk management; and establishes the Counterintelligence Research, Development, and Acquisition Integrated Management Group.

(U) Recommendation, Management Comments, and Our Response

B6 (U) We recommended that the Director, Naval Criminal Investigative Service promulgate counterintelligence support specifically tailored to Program Management Air-265 within the Naval Air Station Patuxent River umbrella counterintelligence support plan.

(U) Management Comments

(U) The Director, Naval Criminal Investigative Service concurred, stating that although Appendix 2, Enclosure 3, paragraph 3.a. DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, authorizes use of an umbrella counterintelligence support plan to cover all research, development, and acquisition programs with critical program information under the cognizance of a research, development, test, and evaluation facility or Program Executive Office, Headquarters, Naval Criminal Investigative Service has directed a tailored counterintelligence support plan for Program Management Air-265 be developed. The Naval Criminal Investigative Service is working with Program Management Air -265 program personnel to develop a request for an updated threat assessment for Program Management Air-265. Once completed, the Naval Criminal Investigative Service will ensure a copy is provided to the Defense Security Service.

(U) Our Response

(U) The comments of the Director, Naval Criminal Investigative Service are responsive and meet the intent of the recommendation.

(U) Issue Area Seven: Effectiveness of the Foreign Visits Policy

(U) We assessed this issue area to determine whether published guidance for foreign visits is relevant and adhered to by program, intelligence, counterintelligence, and security personnel. Deputy Secretary of Defense policy letter, DoD OIG (b)(7)(E) [redacted] requires all Inspectors General to verify compliance with the sponsored foreign personnel policy through their inspection processes. We assessed this issue area in accordance with decisions to grant foreign nationals access to classified and controlled unclassified information during their visits to DoD Component and cleared contractor facilities are consistent with the security and foreign policy interests of the United States and DoD Directives 5230.11, 5230.20, and 5530.3.[13] If there is to be foreign involvement in any aspect of a program or foreign access to the system or its related information, the program protection plan should contain provisions to deny inadvertent or unauthorized access.[14]

(U//~~FOUO~~) We noted in Finding A that in spite of Deputy Secretary of Defense requirements and current DoD policy, DoD organizations DoD OIG (b)(7)(E) [redacted]. In fact, DoD OIG (b)(7)(E) [redacted]. Additionally, the Offices of the USD(P) and USD(I) had not harmonized their policies to ensure official foreign visits and visitors to DoD Components, to include RDT&E facilities were properly and effectively tracked and confirmed.

(U) Additionally, the EA-18G program protection plan and technology assessment/control plan did not address foreign visitor accountability procedures and processes as required by DoD Directive 5230.20 and the DoN Foreign Disclosure Manual.

[13] (U) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992; DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005; and DoD Directive 5530.3, "International Agreements," June 11, 1987.

[14] (U) Title 10 United States Code, Section 2350(a) "Cooperative Research and Development Agreements: NATO Organizations; Allied and Friendly Foreign Countries," requires an analysis of international cooperative opportunities at early decision points in the acquisition process. Additionally, DoD Directive 5000.01 requires coalition interoperability from DoD systems, units, and forces. As a result, a program proponent must consider foreign participation as part of its acquisition strategy. Therefore, foreign involvement in an acquisition program may require information and technology to be shared and/or transferred from one country to another. Consequently, two fundamental considerations must be addressed early in the acquisition process and prior to international participation: access to unclassified and classified data, and system capabilities protection.

(U) Background

(U) In a DODOIG (b)(7)(E) [redacted], letter concerning DoD OIG (b)(7)(E) [redacted] the Deputy Secretary of Defense stated:

> (U) DoD OIG: (b)(7)(E) [redacted]

(U) To that end, the Deputy Secretary of Defense directed that all DoD Components:

- (U) DIA: (b)(3), 50 USC sec. 3024(i) [redacted]
- (U) DIA: (b)(3), 50 USC sec. 3024(i) [redacted]
- (U) DIA: (b)(3), 50 USC sec. 3024(i) [redacted]
- (U) All DoD Components were to incorporate these policies into their relevant directives, and all Inspectors General were to verify compliance with these policies through their inspection processes.

(U) Foreign Visits and Program Protection Planning

(U) The program protection plan for the F/A-18E/F and the EA-18G reflects the presence of foreign interest as well as foreign components. The procedures for protection are addressed in the program protection plan and its annexes. The EA-18G program has foreign government or international organization involvement in its program development because it is a variant of the F/A-18E/F which incorporates foreign military sales technology.

(U) A variant of the F/A-18E/F is being produced under the auspices of foreign military sales for the government of Australia. Program Management Air-265 personnel told us that Australian Foreign Liaison Officers were involved with the F/A-18E/F and EA-18G programs; and that a number of the Australian variant F/A-18E/Fs were being wired for potential conversion to EA-18G capabilities at some future date. Additionally, the program protection plan for the F/A-18E/F and EA-18G included an annex for a technology assessment/control plan and delegation of disclosure authority letter due to the international aspects. The technology assessment/control plan provided detailed guidance of the countermeasures necessary to protect CPI and critical technology; while the delegation of disclosure authority letter addressed the terms under which foreign nationals could access classified and controlled unclassified program information.

(U) With respect to "international briefs" the program protection plan for the F/A-18E/G and EA-18G states that all briefings presented to foreign representatives must be approved by the Program Management Air-265 Security Manager prior to release. Moreover, with respect to "public release" it states:

> (U) Requests for F/A-18E/F/G information or material will be forwarded to the Program Executive Office, Tactical Aircraft Program (PEO(T) Public Affairs Officer (PAO) with concurrence of the Program Office and the Program Management Air-265 Security Manager for releasability determination . . . Contractors, subcontractors and vendors are not authorized to deliver public releases . . . concerning these systems without the prior written consent of the Program Management Air-265 PAO, and with the concurrence of the Program Office and the Program Management Air-265 Security Manager as spelled out in the DD From 254 and the Federal Acquisition Regulation (FAR). At this time the EA-18G is not authorized for foreign release.

(U) The program protection plan for the F/A-18E/F and EA-18G stated that the technology assessment/control plan (Annex 5):

> (U)...identifies and describes sensitive program information; the risks involved in foreign access to the information; the participation in the program or foreign sales of the resulting system; and the development of access controls and measures necessary to protect the U.S. technological or operational advantage of the system, as prescribed in DoDD 5230.11, DoDD 5230.20, and DoDD 5530.3.

(U) However, a review of the technology assessment/control plan regarding the implementation of DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," provided only a section entitled "Foreign National Access" wherein it was stated "controls of foreign nationals at U.S. Government facilities are covered under DoD/Navy operations security instructions." Other than this statement, there was no other discussion of pertinent foreign visitor accountability procedures and processes that are required by DoD Directive 5230.20 and the DoN Foreign Disclosure Manual.

(U) Conclusion

(U//~~FOUO~~) DoD OIG (b)(7)(E) [redacted] The U.S. system is controlled for export; however, a number of the international variants are wired for conversion to EA-18G functionality and incorporate foreign military sales technology. DoD OIG (b)(7)(E) [redacted] The technology assessment/control plan should address these concerns to mitigate the threat of potential foreign technology targeting.

(U) Recommendation, Management Comments, and Our Response

(U) B7 We recommended that the EA-18G Program Manager update the EA-18G program protection plan and technology assessment/control plan to better align protection efforts with DoD and Navy policy regarding foreign visits and foreign disclosure.

(U) Management Comments

(U) The Assistant Secretary of the Navy for Research, Development, and Acquisition, and the EA-18G Program Manager concurred. The F/A-18 E/F and EA-18G Program Executive Office and the EA-18G Program Manager will be updating the current program protection plan during FY 2013, and will more clearly annotate the process for foreign visits and foreign disclosures within the program protection plan and technology assessment/control plan.

(U) Our Response

(U) The comments of the Assistant Secretary of the Navy for Research, Development, and Acquisition, and the EA-18G Program Manager are responsive and meet the intent of the recommendation.

(U) Issue Area Eight: Application of Horizontal Protection of Critical Program Information

(U) We assessed this issue area to determine whether published guidance for horizontal protection is relevant to and adhered to by program, security, intelligence, and counterintelligence personnel. We assessed this issue area to ensure that critical Defense technologies, to include CPI, associated with more than one RDA program are protected to the same degree by all involved DoD activities. DoD Instruction 5200.39 states that it is DoD policy to conduct comparative analysis of defense systems technologies and align CPI protection activities horizontally throughout DoD.

(U) The DoD Instruction 5200.39 requirement that a horizontal protection database be used in support of the identification of CPI was further solidified on July 22, 2010, when the USD(AT&L) issued a memorandum designating the Acquisition Security Database as the horizontal protection database for the Department. The Acquisition Security Database is now under the control, oversight, and management of the Director, Defense Research and Engineering, and currently tracks 728 programs. In the memorandum, the USD(AT&L) states that the Heads of DoD Components use the Acquisition Security Database to execute mission requirements for the horizontal protection of DoD Component CPI. The memorandum also states that within 90 days, the Heads of DoD Components shall submit their respective plans for entering current, future, and legacy RDA programs/projects into the Acquisition Security Database and for updating these records at each milestone.

(U) The Acquisition Security Database, a horizontal protection database originally developed by the DoN, provides the RDA community with greater visibility of CPI. Use of DoD OIG (b)(7)(F) [redacted] horizontal protection database by the RDA community would represent an important step toward greater protection of DoD's CPI. Once the RDA community is populating DoD OIG (b)(7)(F) [redacted] horizontal protection database, RDA protection practitioners will be able to view all programs with similar CPI to help ensure consistent RDA protection support and decrease the mishandling or inadvertent compromise of CPI, especially with respect to CPI that is inherited from other RDA programs.

(U) All DoN acquisition commands and selected RDT&E facilities provide information to and utilize information within the Acquisition Security Database. DoN participation is across multiple acquisition support areas, to include RDA protection, counterintelligence, anti-tamper, operations security, and other security disciplines, as well as acquisition personnel. The focus is on the protection of critical technology and CPI from foreign intelligence collection and inadvertent or unauthorized disclosure. The DoN is fully represented on the Acquisition Security Database Configuration Control Board by three personnel, each representing a different area of Acquisition Security Database interest: Anti-tamper, counterintelligence, and acquisition/RDA protection.

(U) EA-18G program management personnel advised that they were aware of horizontal protection being applied to the EA-18G program. They briefed the PM routinely on horizontal protection. Moreover, the EA-18G program protection plan addressed horizontal protection and indicated that the Acquisition Security Database was to be used to see what other programs with similar technologies have identified as CPI.

(U) Additionally, the program protection implementation plan addressed horizontal protection, and utilizing Navy databases to make informed decisions concerning CPI that was present in the EA-18G, and was also being used by other programs and weapons platforms.

(U) Conclusion

(U) The EA-18G program office staff did use the Acquisition Security Database to see what other programs with similar technologies have identified as CPI. The DoD Instruction 5200.39 requirement that a horizontal protection database should be used in support of the identification of CPI appears to be effective for the EA-18G program; therefore we make no recommendations for this issue area.

(U) Appendix A. Scope and Methodology

(U) This assessment was conducted in accordance with Quality Standards for Inspections.[15] Those standards require that we plan and perform the assessment to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our assessment objectives. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations. We began our site visits and interviews for this assessment in June 2009, with additional clarifying interviews of both Navy and Office of the Secretary of Defense officials extending to the publication of this draft report.

(U) The overall assessment scope was broad, encompassing DoD counterintelligence, intelligence, security, and program personnel to protect CPI. We looked at programs that had identified CPI. Our scope did not include Section 254 of the FY 2009 National Defense Authorization Act, "Trusted Defense Systems." Section 254 requires the Office of the Secretary of Defense to conduct assessments of selected acquisition programs to identify vulnerabilities in the supply chain of each program's electronics and information processing systems that potentially compromise the level of trust in the systems. The Offices of the USD(AT&L) and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer led a detailed effort, in conjunction with other DoD elements, to conduct those vulnerability assessments and reported to Congress as required.

(U) For our methodology, we focused on the eight issue areas related to CPI identification and program protection planning that evolved from a series of inspections conducted by the Service Inspectors General and an overarching integrated process team chartered by the Deputy Secretary of Defense in 2000. The overarching integrated process team identified 27 tasks that would enhance the Department's ability to identify and protect CPI, the effectiveness of the foreign visitor program, and the effectiveness of counterintelligence and security support to RDT&E facilities and the acquisition process. We categorized these 27 tasks into the eight key issue areas. Within the framework of these eight issue areas, we specifically focused on and assessed standardization of protection processes and their application, oversight of the protection process and its implementation, and responsibility for protection.

(U) We selected three programs, one from each Service. We reviewed DoD and Service policies, instructions, and procedures. We analyzed relevant program-specific documentation and interviewed appropriate individuals in the program offices, as well as individuals in the acquisition, counterintelligence, and security communities. This assessment addresses EA-18G and Navy policies and procedures.

[15] (U) The standards were published by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency, which the Inspector General Reform Act of 2008 combined in creating the Council of the Inspectors General on Integrity and Efficiency.

(U) Report No. 10-INTEL-07, "DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network – Tactical," addressed the Warfighter Information Network – Tactical and Army policies and procedures. Report No. 11-INTEL-08 "DoD Efforts to Protect Critical Program Information: The Air Force's Family of Advanced Beyond Line-of-Sight Terminals," addressed the Family of Advanced Beyond Line-of-Sight Terminals and Air Force policies and procedures.

(U) We planned and performed this assessment in coordination with subject matter experts from the Offices of the Under Secretaries of Defense for Acquisition, Technology, and Logistics, for Policy, and for Intelligence; the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer; and the Defense Security Service. Although the subject matter experts contributed to this project, the project results and recommendations are those of the DoD Office of Inspector General.

(U) We assessed a program of record from each Service at different stages in the acquisition cycle. One Service had a program that was in the early stage of program protection planning, another Service had a program that was almost at the conclusion of program protection planning, and the final Service had completed program protection planning. This methodology would provide us with an evolutionary perspective of program protection planning. EA-18G completed its program protection plan. The Army's Warfighter Information Network – Tactical – the first in the series – had almost completed its program protection plan; and the Air Force's Family of Advanced Beyond Line-of-Sight Terminals – the second in the series – was still developing its program protection plan and was nearing completion. Because EA-18G had completed its program protection plan, we could assess its effectiveness to implement and follow-up on countermeasures aimed at protecting CPI. We did not focus on whether EA-18G officials identified the correct CPI because the process for identifying CPI is very subjective.

(U) We assessed whether the published guidance on the protection of CPI in each issue area was relevant and whether program, intelligence, counterintelligence, and security personnel adhered to the guidance. In those instances where efforts to protect CPI could be strengthened, we made recommendations for improvements.

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this assessment.

(U) Appendix B. Prior Coverage

(U) During the last 10 years, the Government Accountability Office (GAO) and the Department of Defense Inspector General (DoD IG) have issued 15 reports discussing DoD and Navy efforts to protect critical program information. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/Ir/reports.

(U) GAO

(U) GAO Report No. GAO-11-354, "Improvements Needed to Prevent Unauthorized Technology Releases to Foreign Nationals in the United States," February 2011

(U) GAO Report No. GAO-09-271, "GAO High-Risk Series – An Update," January 2009

(U) GAO Report No. GAO-08-467SP, "Assessments of Selected Weapons Programs," March 2008

(U) DoD IG

(U) DoD IG Report No. DoDIG-2012-001, "Assessment of Security Within the Department of Defense – Training, Certification, and Professionalization," October 6, 2011

(U) DoD IG Report No. 11-INTEL-11, "Summary Report of FY 2010 Inspections on Security, Intelligence, Counterintelligence, and Technology Protection Practices at DoD Research, Development, Test, and Evaluation Facilities," June 27, 2011

(U) DoD IG Report No. 11-INTEL-08, "DoD Efforts to Protect Critical Program Information: The Air Force's Family of Advanced Beyond Line-of-Sight Terminals," April 15, 2011

(U) DoD IG Report No. 10-INTEL-09, "Assessment of Security Within the Department of Defense – Tracking and Measuring Security Costs," August 6, 2010

(U) DoD IG Report No. 10-INTEL-08, "Inspection Guidelines for DoD Security, Intelligence, and Counterintelligence Support to Research, Development, and Acquisition Protection for 2010," August 6, 2010

(U) DoD IG Report No. 10-INTEL-07, "DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network – Tactical," July 21, 2010

(U) DoD IG Report No. 10-INTEL-06, "Summary Report of FY 2009 Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test, and Evaluation Facilities," May 21, 2010

(U) DoD IG Report No. 09-INTEL-15, "Summary Report of FY 2008 Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test and Evaluation Facilities," September 30, 2009

(U) DoD IG Report No. 08-INTEL-09, "Report on FY 2007 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test and Evaluation Facilities," June 23, 2008

(U) DoD IG Report No. 08-INTEL-04, "Inspection Guidelines for DoD Research and Technology Protection, Security and Counterintelligence for 2008," April 18, 2008

(U) DoD IG Report No. 07-INTEL-11, "FY 2006 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test and Evaluation Facilities," August 31, 2007

(U) DoD IG Report No. 06-INTEL-14, "FY 2005 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test and Evaluation Facilities," September 20, 2006

(U) DoD IG Report No. 06-INTEL-03, "Inspection Guidelines for DoD Research and Technology Protection, Security and Counterintelligence for 2006," February 28, 2006

(U) DoD IG Report No. 05-INTEL-14, "FY 2004 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test and Evaluation Facilities," May 27, 2005

(U) DoD IG Report No. 00-OIR-05, "Measures to Protect Against the Illicit Transfer of Sensitive Technology," March 27, 2000

(U) Appendix C. Additional Background Information

(U) Historical Perspective. In early 1999, the Deputy Secretary of Defense directed the Service Inspectors General to survey the counterintelligence and security programs at more than 60 RDT&E facilities. The teams identified a number of recommendations related to the specific sites. As a result of these efforts, the Deputy Secretary of Defense chartered an Overarching Integrated Process Team to better frame the recommendations and to oversee their implementation. From February 12 to May 12, 2000, the Deputy Secretary of Defense signed a total of 7 memoranda containing 27 tasks aimed at enhancing the Department's ability to identify and protect CPI, implement an effective foreign visitor program, and provide effective counterintelligence and security support to RDT&E facilities and the acquisition process. On February 17, 2000, the Deputy Secretary of Defense signed a memorandum requesting the DoD Inspector General to ensure that DoD Components implement a uniform system of periodic reviews through their existing agency and Service inspection processes for compliance with directives concerning security, technology protection, and counterintelligence practices. These reviews were to assist with the protection of the cutting edge technology of U.S. weapon systems. The February 17, 2000, memorandum also requested that the DoD Inspector General develop inspection list guidelines for all Department Inspectors General to enhance consistency.

(U) On May 8, 2002, the Inspector General, DoD; the Deputy Under Secretary of Defense for Laboratories and Basic Sciences; the Director, Operational Test and Evaluation; the Service Inspectors General; and the Director, Program Integration, Internal Management Review (formerly Internal Assessments), Missile Defense Agency, signed a memorandum of understanding on security, technology protection, and counterintelligence inspections. The memorandum of understanding requires participating Inspectors General to prepare and forward to the DoD Office of Inspector General any significant findings and recommendations at the end of each inspection. The DoD Office of Inspector General[16] issues a summary report on inspections of security, RDA protection, and counterintelligence practices at DoD RDT&E facilities.

[16] (U) Since the original request by the Deputy Secretary of Defense, the Office of the Deputy Inspector General for Intelligence and Special Program Assessments, in the DoD Office of the Inspector General, has published the annual summary report, highlighting Service and milestone decision authority inspections and best practices. We also publish the guidelines biennially, with input from Department and Component RDA, counterintelligence, intelligence, security, and Inspectors General elements.

(U) Appendix D. DoD Organizations and Efforts to Protect Critical Program Information

(U) Establishing a consistent process for identifying CPI and conducting program protection planning, a process that takes into account the role RDA, counterintelligence, intelligence, security, and systems engineering personnel perform, is critical for ensuring that DoD can protect CPI. As part of making this process consistent, beginning in December 2008, DoD established working groups to address CPI identification and program protection planning. The working group process is co-led by the offices of the USD(AT&L) and the Under Secretary of Defense Intelligence. Each working group is chaired by either an Office of the Secretary of Defense-level or Service representative with expertise in the protection of CPI. All working groups operate under an agreement that there should be an overarching set of program protection products (for example, process, guidance, tools) and that these standards would be extended and amplified by the Services and agencies to serve their needs. In some cases, the working group met its goal and was disestablished. The USD(I) and the Defense Intelligence Agency also contribute to the Department's efforts to protect CPI.

(U) Program Protection Working Groups

(U) Definitions Working Group. This working group was established in December 2008 to affirm and document the CPI, program protection, systems assurance, and software assurance terms and associated hierarchy of relationships. Completion of this working group was described as being necessary to initiate the other working groups. Four weeks later, this working group presented a briefing of the group's product that defined the terms and relationships per their objective to the Program Protection Executive Committee.[17] Having met the goal, the working group was disestablished.

(U) CPI Identification Process Working Group. This working group was formed in August 2009 to establish the minimum standards for the process used by DoD to identify CPI. Services and agencies will be allowed to extend and amplify the standard to suit their Service or agency needs. A second product will be a method of assessing the tools used by various Services and agencies to identify CPI. The working group will use, as appropriate, the results from other groups. In December 2009, this working group developed a CPI identification survey and a CPI identification tool, which were combined with a more detailed explanation on how to use each of these tools into a CPI Identification Handbook. This Handbook is now being distributed by the Services to their programs to assist in the identification of CPI and to facilitate consistency in identifying CPI across the Services. Having met the goal, the group was disestablished.

[17] (U) The purpose of the Program Protection Executive Committee is to further develop the products started by these working groups, under the guidance and review of senior executive members. The Program Protection Executive Committee is composed of OUSD(AT&L), Office of the USD(I), Service executives, and Service cross-working group coordination points of contact.

(U) Manpower Studies Working Group. Formation of this working group will depend on each Service making a determination whether or not to act on the proposal of the Program Protection Working Group to conduct manpower studies to assess the sufficiency and availability of resources to support the program protection process.

(U) Program Protection Planning Content, Format, and Review Working Group. This working group was established in June 2008 to develop two products. The first product was guidance on preparing program protection plans. The second product will document the program protection plan review process and stakeholders. The program protection plan review process will detail milestone requirements (with checklists) for development, review, and approval; stakeholders include Service components, the USD(AT&L), the USD(I), and subject matter experts for applicable countermeasures such as anti-tamper measures, and Defense trusted integrated circuits. The first draft of the program protection plan review process issued was based on the systems engineering plan[18] process and will be revised in a Six Sigma working group. This working group completed a Six Sigma project to define the program protection plan review process, and developed a Program Protection Plan Preparation Guide. The program protection plan review process is in place and the USD(AT&L) signed out the first program protection plan on June 17, 2010. The Services are in the process of introducing and piloting the Program Protection Plan Preparation Guide on their programs. Having met the goal, the group was disestablished.

(U) Training and Transition Working Group. This group, which had been slated to start 60 days after DoD Manual 5200.39 is published (December 2011), will develop a competency model for program protection roles. Based on preliminary work completed, this working group identify the required skills, define the course content to serve the needs of the various functional areas (acquisition, engineering, counterintelligence, criminal investigative service, and the like), and estimate the number of courses required per year to accommodate the training of the workforce. This working group will also develop and implement a plan to train Service personnel and transition to the revised program protection process and policy.

(U) Criticality Assessment Working Group. This working group was established in June 2008 to develop the process required to implement system security engineering in program protection planning. Membership includes primarily systems engineers and individuals familiar with program risk mitigation as currently implemented by programs. This working group will develop a document defining the criticality analysis process and will modify the CPI Identification Handbook as necessary to support the criticality analysis process. The products developed by this working group will be incorporated into the program protection plan review process, the Program Protection Plan Preparation Guide, and the CPI Identification Handbook.

[18] (U) The systems engineering plan is the blueprint for the execution, management, and control of the technical aspects of an acquisition program from conception to disposal. Systems engineering translates operational requirements into configured systems, integrates technical inputs of the entire design team, manages interfaces, characterizes and manages technical risk, transitions technology from the technology base into program specific efforts, and verifies that designs meet operational needs. The systems engineering plan is a "living" document that captures a program's current and evolving systems engineering strategy and its relationship with the overall program management effort.

(U) Threats, Vulnerabilities, and Countermeasures Working Group. This working group was established in February 2008 to define the process and criteria for the vulnerability assessment step in the program protection process. The scope of the vulnerabilities assessment will include the acquisition development and manufacturing environments, supply chain, operational environment, and system design. This working group developed an Anti-Tamper Exposure Chart, an Anti-Tamper Consequence Chart, and an Anti-Tamper Criteria spreadsheet. These products were developed based on existing open Anti-Tamper products developed by the Anti-Tamper Executive Agency. The tools developed by this working group will be used to ensure consistency in applying the Anti-Tamper countermeasure. DoD OIG (b)(5) [redacted] This working group was merged with the Criticality Assessment Working Group in June 2008.

(U) Horizontal Protection Process Working Group. This working group was started for the first time in 2009 for three months to define the process flow, roles, responsibilities, and policy to execute horizontal protection from before milestone A through sustainment. The first task to determine the need for a standardized security classification guide for program protection was completed; the group determined that a standardized security classification guide was not required. This group will provide input to the Acquisition Security Database Configuration Control Board and to incorporate the Acquisition Security Database within Service policy and processes. This working group defined the horizontal protection process and data read/write/modify requirements for the Acquisition Security Database. This group is no longer meeting, but has not been officially disestablished.

(U) Acquisition Policy and Guidance for Program Protection Working Group. This working group was established in February 2008 to aid in the development of program protection guidance to be documented in the DoD Instruction 5200.39 and the upcoming DoD 5200.39 Manual. The working group will build on all other working group outputs and ensure consistency with the DoD Instruction 5000.02. The updates to these policies are intended to rectify deficiencies in the initial versions of the policies (such as no process for reviewing program protection plans at the Office of the Secretary of Defense level, and no horizontal protection process) and to provide guidance for the application of designing-in security and supply chain risk mitigation for the protection of CPI. Based on the work of the Criticality Assessment Working Group, in January 2011, it was decided to shift the systems engineering half of the scope that was planned for the DoD Manual 5200.39 to the DoD Instruction 5000.02. The DoD Manual 5200.39 scope that remains will be completely within the purview of the USD(I) and implement the requirements outlined in DoD Instruction 5200.39.

(U) Under Secretary of Defense (Intelligence)

(U) The USD(I) recently published DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011. The policy implements the relevant sections of policy established in DoD Instruction 5200.39 for counterintelligence support to the protection of CPI; DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," July 10, 2008, for counterintelligence support to international transfers of technology, articles, and services; and Deputy Secretary of Defense Directive-Type Memorandum 09-016, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems," March 25, 2010, for counterintelligence support to supply-chain risk management. The new policy established a requirement for an intelligence assessment of DoD RDA programs to provide baseline security requirements against foreign intelligence collection. It also integrated a technology targeting risk assessment with the appropriate counterintelligence analytical product to inform RDA programs of threats to CPI from foreign intelligence entities.

(U) The USD(I) is also in the process of finalizing DoD Manual 5200.39, "Procedures for Critical Program Information (CPI) Protection Within the Department of Defense," which will provide the guidance for the implementation of program protection measures. It is currently in the formal coordination process.

(U) Defense Intelligence Agency

(U) DIA: (b)(3), 10 USC sec. 424, 50 USC sec. 3024(i) [redacted]

(U) Appendix E – Best Practices

(U) This assessment noted examples of best practices employed by the Navy. This information identifies practices which increase efficiencies and productivity and are included to encourage the recognition of best practices across the RDA protection enterprise, and integrate and synchronize RDA efforts that furnish protection to CPI. These best practices include:

- (U) ASN/RDA required standard operating procedures for CPI identification for DoN acquisition programs.

- (U) Employment of robust and disciplined systems engineering and anti-tamper processes.

- (U) Utilization of the STILO program for providing timely and continuous intelligence support to the DoN acquisition process.

- (U) Systems Command focused RDA protection efforts with embedded security personnel within the program offices, and the integration of security working group personnel in the Procurement Planning Conference process.

- (U) Implementation of contract terms and conditions for contractor development of a program protection implementation plan that compliments the program protection plan.

- (U) NAVAIR development of horizontal protection and institutionalized use of the Acquisition Security Database, which has been adopted as the DoD standard.

- (U) Program office staff crafted a comprehensive program protection implementation plan data item description that can be used repetitively for program protection implementation planning. The data item description is also located in the Acquisition Streamlining and Standardization Information System (also known as ASSIST) database.

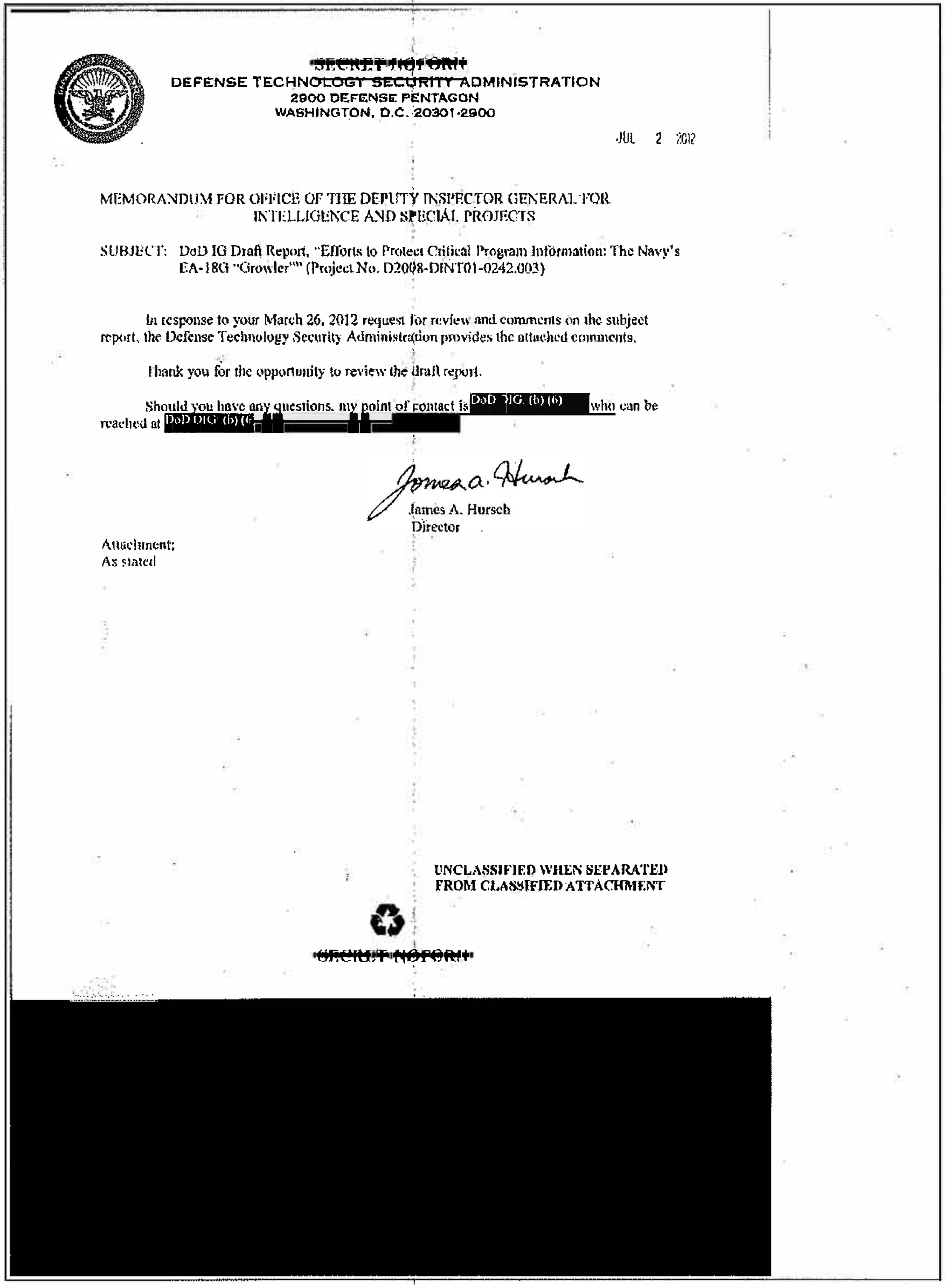
(U///~~FOUO~~) Appendix F. [redacted]

DIA: (b)(3), 10 USC sec. 424, 50 USC sec. 3024(i)

DIA: (b)(1), EO 13526, secs 1.4(a), 1.4(c), (b)(3), 10 USC sec. 424, 50 USC sec. 3024(i)

[redacted]

Office of the Under Secretary of Defense for Policy Comments



~~SECRET//NOFORN~~

DEFENSE TECHNOLOGY SECURITY ADMINISTRATION
2900 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2900

JUL 2 2012

MEMORANDUM FOR OFFICE OF THE DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE AND SPECIAL PROJECTS

SUBJECT: DoD IG Draft Report, "Efforts to Protect Critical Program Information: The Navy's EA-18G "Growler"" (Project No. D2008-DINT01-0242.003)

In response to your March 26, 2012 request for review and comments on the subject report, the Defense Technology Security Administration provides the attached comments.

Thank you for the opportunity to review the draft report.

Should you have any questions, my point of contact is DoD OIG (b)(6) who can be reached at DoD OIG (b)(6) [redacted]

James a. Hursch

James A. Hursch
Director

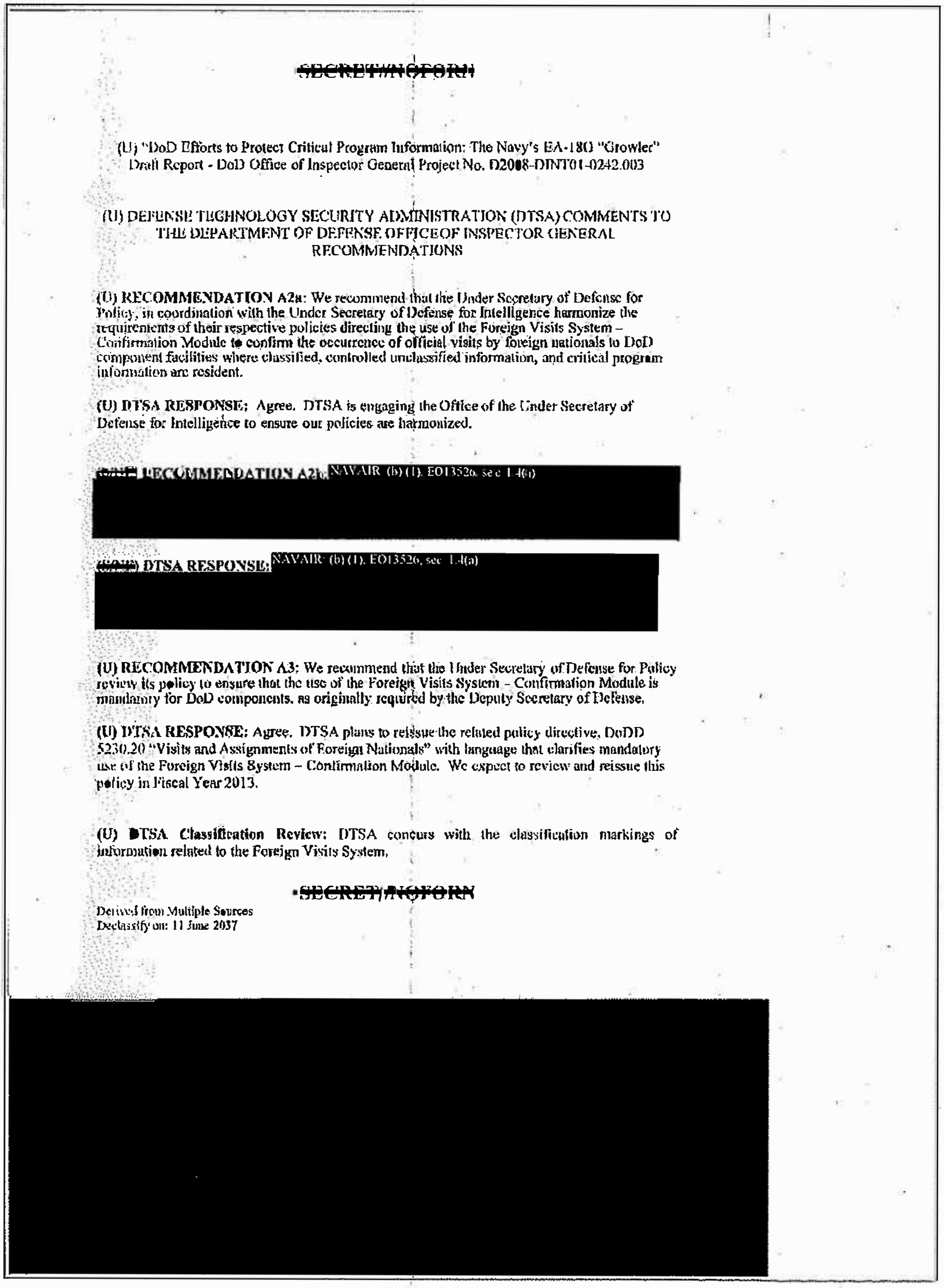
Attachment:
As stated

UNCLASSIFIED WHEN SEPARATED
FROM CLASSIFIED ATTACHMENT

~~SECRET//NOFORN~~

[redacted]

Office of the Under Secretary of Defense for Policy Comments



~~SECRET//NOFORN~~

(U) "DoD Efforts to Protect Critical Program Information: The Navy's EA-18G "Growler"
Draft Report - DoD Office of Inspector General Project No. D2008-DINT01-0242.003

(U) DEFENSE TECHNOLOGY SECURITY ADMINISTRATION (DTSA) COMMENTS TO
THE DEPARTMENT OF DEFENSE OFFICEOF INSPECTOR GENERAL
RECOMMENDATIONS

(U) RECOMMENDATION A2a: We recommend that the Under Secretary of Defense for Policy, in coordination with the Under Secretary of Defense for Intelligence harmonize the requirements of their respective policies directing the use of the Foreign Visits System – Confirmation Module to confirm the occurrence of official visits by foreign nationals to DoD component facilities where classified, controlled unclassified information, and critical program information are resident.

(U) DTSA RESPONSE: Agree. DTSA is engaging the Office of the Under Secretary of Defense for Intelligence to ensure our policies are harmonized.

RECOMMEDATION A2b: NAVAIR (b)(1), EO13526, sec 1.4(a) [redacted]

DTSA RESPONSE: NAVAIR (b)(1), EO13526, sec 1.4(a) [redacted]

(U) RECOMMENDATION A3: We recommend that the Under Secretary of Defense for Policy review its policy to ensure that the use of the Foreign Visits System – Confirmation Module is mandatory for DoD components, as originally required by the Deputy Secretary of Defense.

(U) DTSA RESPONSE: Agree. DTSA plans to reissue the related policy directive, DoDD 5230.20 "Visits and Assignments of Foreign Nationals" with language that clarifies mandatory use of the Foreign Visits System – Confirmation Module. We expect to review and reissue this policy in Fiscal Year 2013.

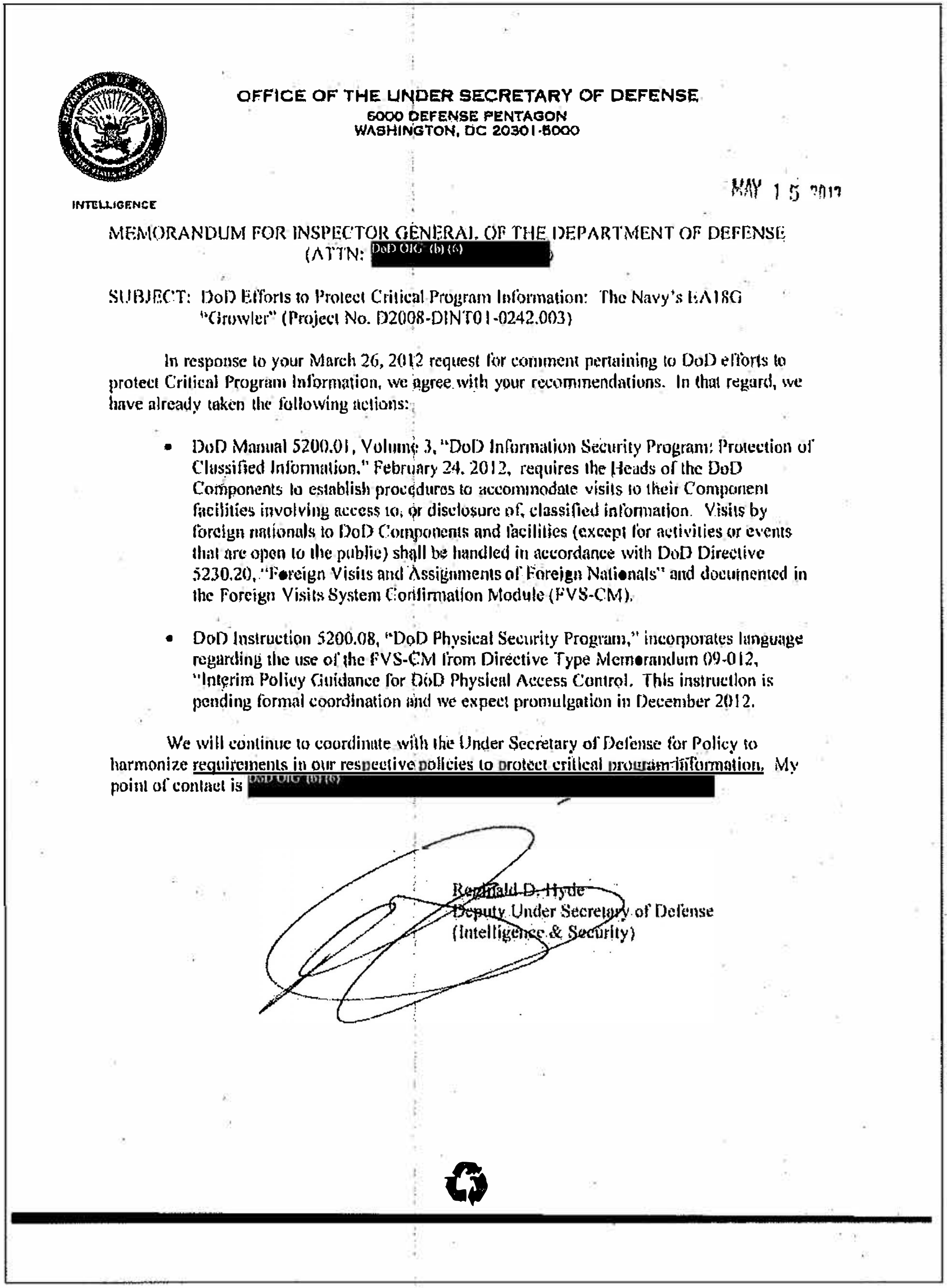
(U) DTSA Classification Review: DTSA concurs with the classification markings of information related to the Foreign Visits System.

~~SECRET//NOFORN~~

Derived from Multiple Sources
Declassify on: 11 June 2037

[redacted]

Office of the Under Secretary of Defense for Intelligence Comments



OFFICE OF THE UNDER SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

MAY 1 5 2012

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
(ATTN: DoD OIG (b)(6))

SUBJECT: DoD Efforts to Protect Critical Program Information: The Navy's EA18G "Growler" (Project No. D2008-DINT01-0242.003)

In response to your March 26, 2012 request for comment pertaining to DoD efforts to protect Critical Program Information, we agree with your recommendations. In that regard, we have already taken the following actions:

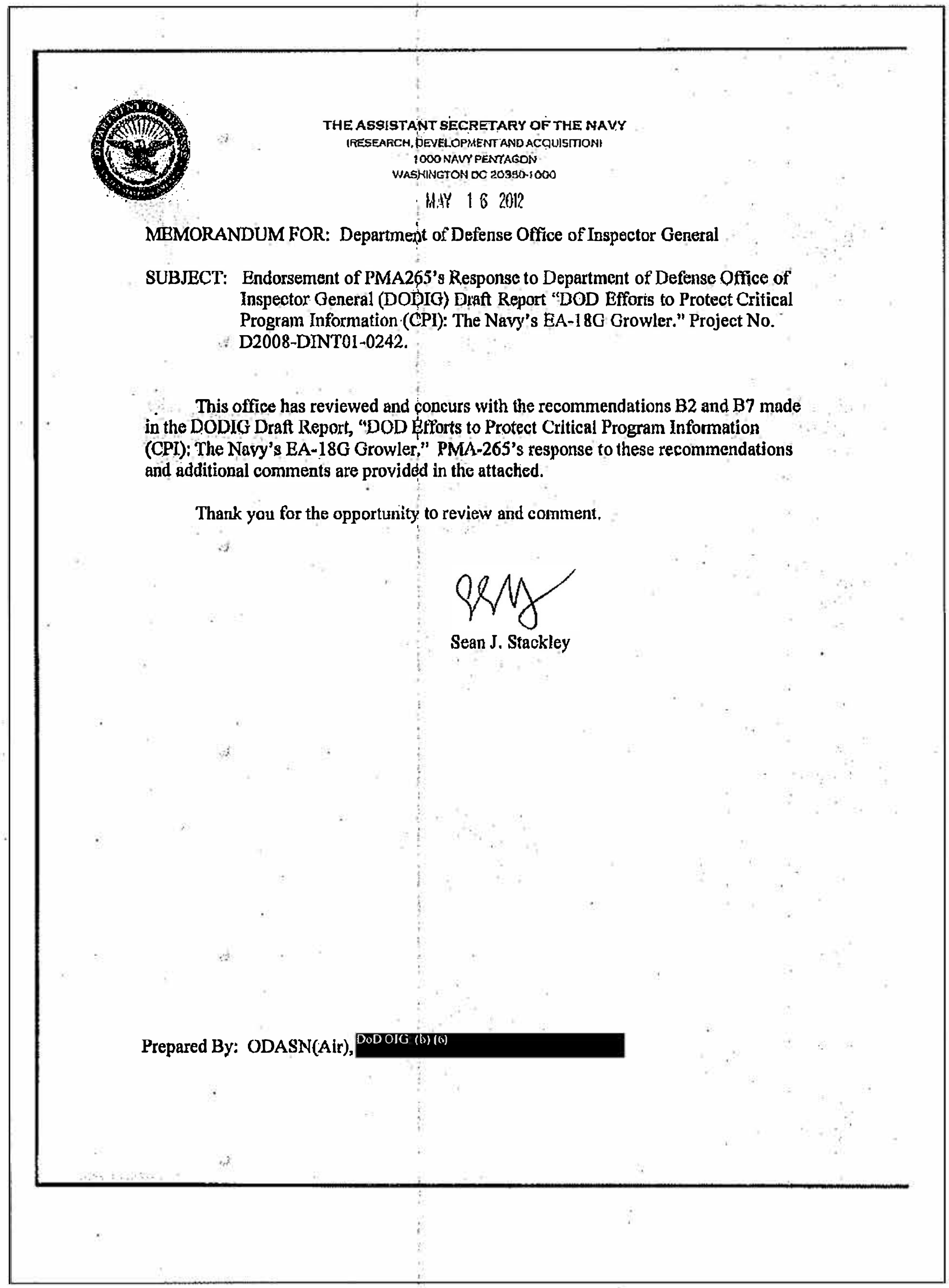
- DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, requires the Heads of the DoD Components to establish procedures to accommodate visits to their Component facilities involving access to, or disclosure of, classified information. Visits by foreign nationals to DoD Components and facilities (except for activities or events that are open to the public) shall be handled in accordance with DoD Directive 5230.20, "Foreign Visits and Assignments of Foreign Nationals" and documented in the Foreign Visits System Confirmation Module (FVS-CM).

- DoD Instruction 5200.08, "DoD Physical Security Program," incorporates language regarding the use of the FVS-CM from Directive Type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control. This instruction is pending formal coordination and we expect promulgation in December 2012.

We will continue to coordinate with the Under Secretary of Defense for Policy to harmonize requirements in our respective policies to protect critical program information. My point of contact is DoD OIG (b)(6)

Reginald D. Hyde
Deputy Under Secretary of Defense
(Intelligence & Security)

Assistant Secretary of the Navy for Research, Development and Acquisition and Program Manager, EA-18G Comments



THE ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

MAY 16 2012

MEMORANDUM FOR: Department of Defense Office of Inspector General

SUBJECT: Endorsement of PMA265's Response to Department of Defense Office of Inspector General (DODIG) Draft Report "DOD Efforts to Protect Critical Program Information (CPI): The Navy's EA-18G Growler." Project No. D2008-DINT01-0242.

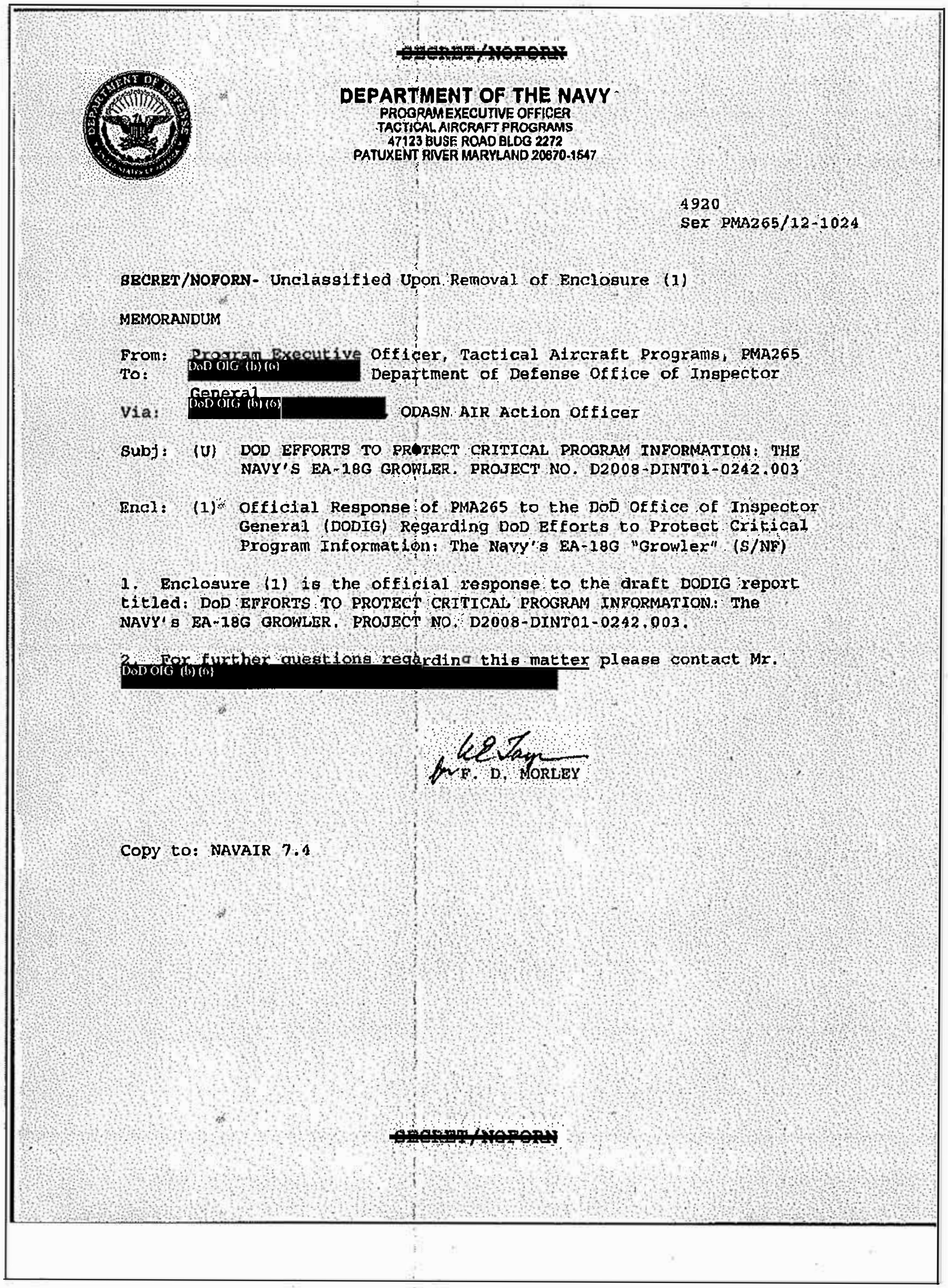
This office has reviewed and concurs with the recommendations B2 and B7 made in the DODIG Draft Report, "DOD Efforts to Protect Critical Program Information (CPI): The Navy's EA-18G Growler," PMA-265's response to these recommendations and additional comments are provided in the attached.

Thank you for the opportunity to review and comment.

Sean J. Stackley

Prepared By: ODASN(Air), DoD OIG (b) (6)

Assistant Secretary of the Navy for Research, Development and Acquisition and Program Manager, EA-18G Comments



~~SECRET/NOFORN~~

DEPARTMENT OF THE NAVY
PROGRAM EXECUTIVE OFFICER
TACTICAL AIRCRAFT PROGRAMS
47123 BUSE ROAD BLDG 2272
PATUXENT RIVER MARYLAND 20670-1547

4920
Ser PMA265/12-1024

SECRET/NOFORN- Unclassified Upon Removal of Enclosure (1)

MEMORANDUM

From: Program Executive Officer, Tactical Aircraft Programs, PMA265
To: DoD OIG (b)(6) Department of Defense Office of Inspector General
Via: DoD OIG (b)(6), ODASN AIR Action Officer

Subj: (U) DOD EFFORTS TO PROTECT CRITICAL PROGRAM INFORMATION: THE NAVY'S EA-18G GROWLER. PROJECT NO. D2008-DINT01-0242.003

Encl: (1) Official Response of PMA265 to the DoD Office of Inspector General (DODIG) Regarding DoD Efforts to Protect Critical Program Information: The Navy's EA-18G "Growler" (S/NF)

1. Enclosure (1) is the official response to the draft DODIG report titled: DoD EFFORTS TO PROTECT CRITICAL PROGRAM INFORMATION: The NAVY's EA-18G GROWLER. PROJECT NO. D2008-DINT01-0242.003.

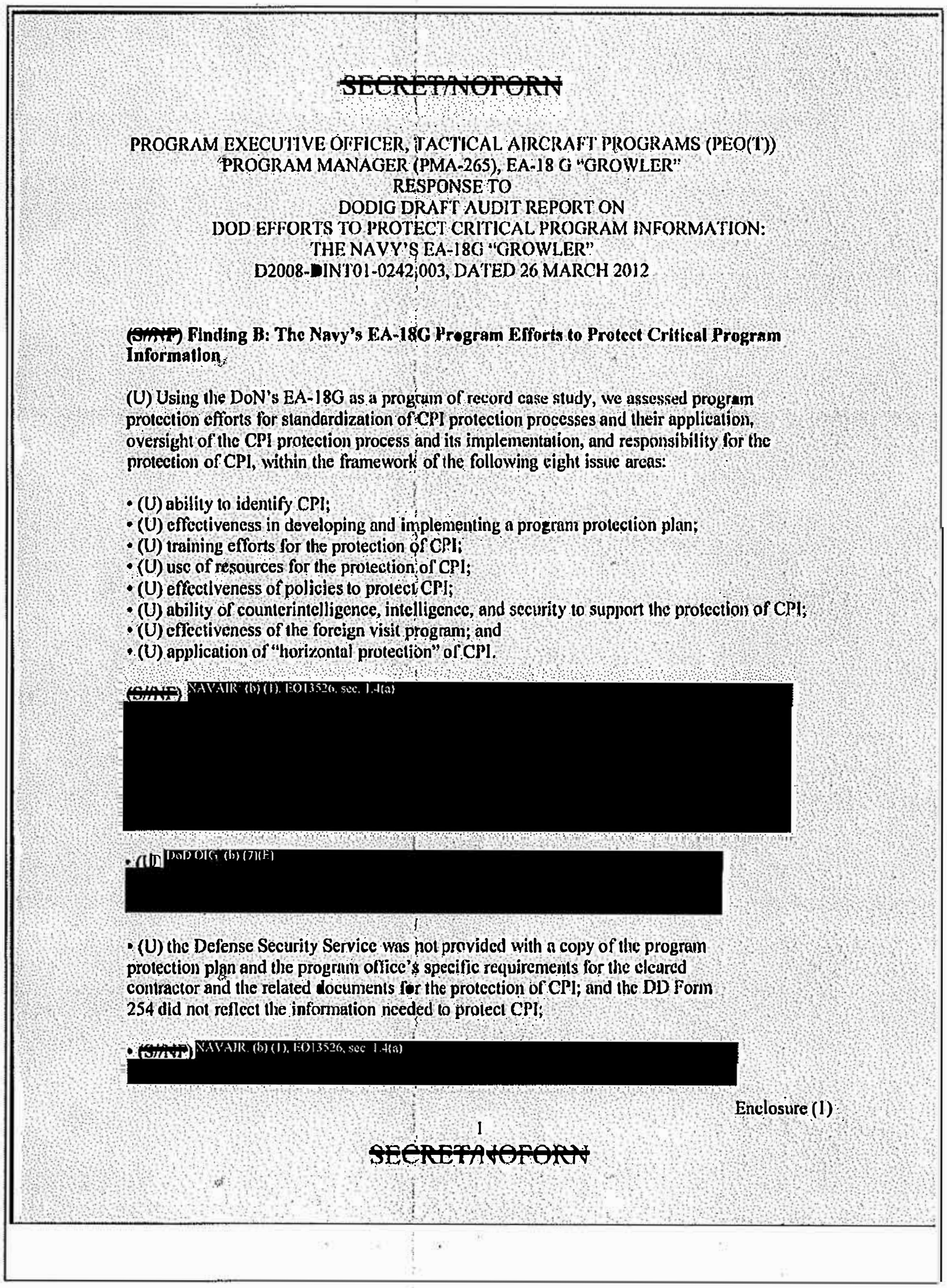
2. For further questions regarding this matter please contact Mr. DoD OIG (b)(6)

F. D. MORLEY

Copy to: NAVAIR 7.4

~~SECRET/NOFORN~~

Assistant Secretary of the Navy for Research, Development and Acquisition and Program Manager, EA-18G Comments



~~SECRET//NOFORN~~

PROGRAM EXECUTIVE OFFICER, TACTICAL AIRCRAFT PROGRAMS (PEO(T))
PROGRAM MANAGER (PMA-265), EA-18 G "GROWLER"
RESPONSE TO
DODIG DRAFT AUDIT REPORT ON
DOD EFFORTS TO PROTECT CRITICAL PROGRAM INFORMATION:
THE NAVY'S EA-18G "GROWLER"
D2008-DINT01-0242.003, DATED 26 MARCH 2012

~~(S//NF)~~ Finding B: The Navy's EA-18G Program Efforts to Protect Critical Program Information.

(U) Using the DoN's EA-18G as a program of record case study, we assessed program protection efforts for standardization of CPI protection processes and their application, oversight of the CPI protection process and its implementation, and responsibility for the protection of CPI, within the framework of the following eight issue areas:

- (U) ability to identify CPI;
- (U) effectiveness in developing and implementing a program protection plan;
- (U) training efforts for the protection of CPI;
- (U) use of resources for the protection of CPI;
- (U) effectiveness of policies to protect CPI;
- (U) ability of counterintelligence, intelligence, and security to support the protection of CPI;
- (U) effectiveness of the foreign visit program; and
- (U) application of "horizontal protection" of CPI.

~~(S//NF)~~ NAVAIR (b)(1), EO13526, sec. 1.4(a) [redacted]

- (U) DoD OIG (b)(7)(E) [redacted]

- (U) the Defense Security Service was not provided with a copy of the program protection plan and the program office's specific requirements for the cleared contractor and the related documents for the protection of CPI; and the DD Form 254 did not reflect the information needed to protect CPI;

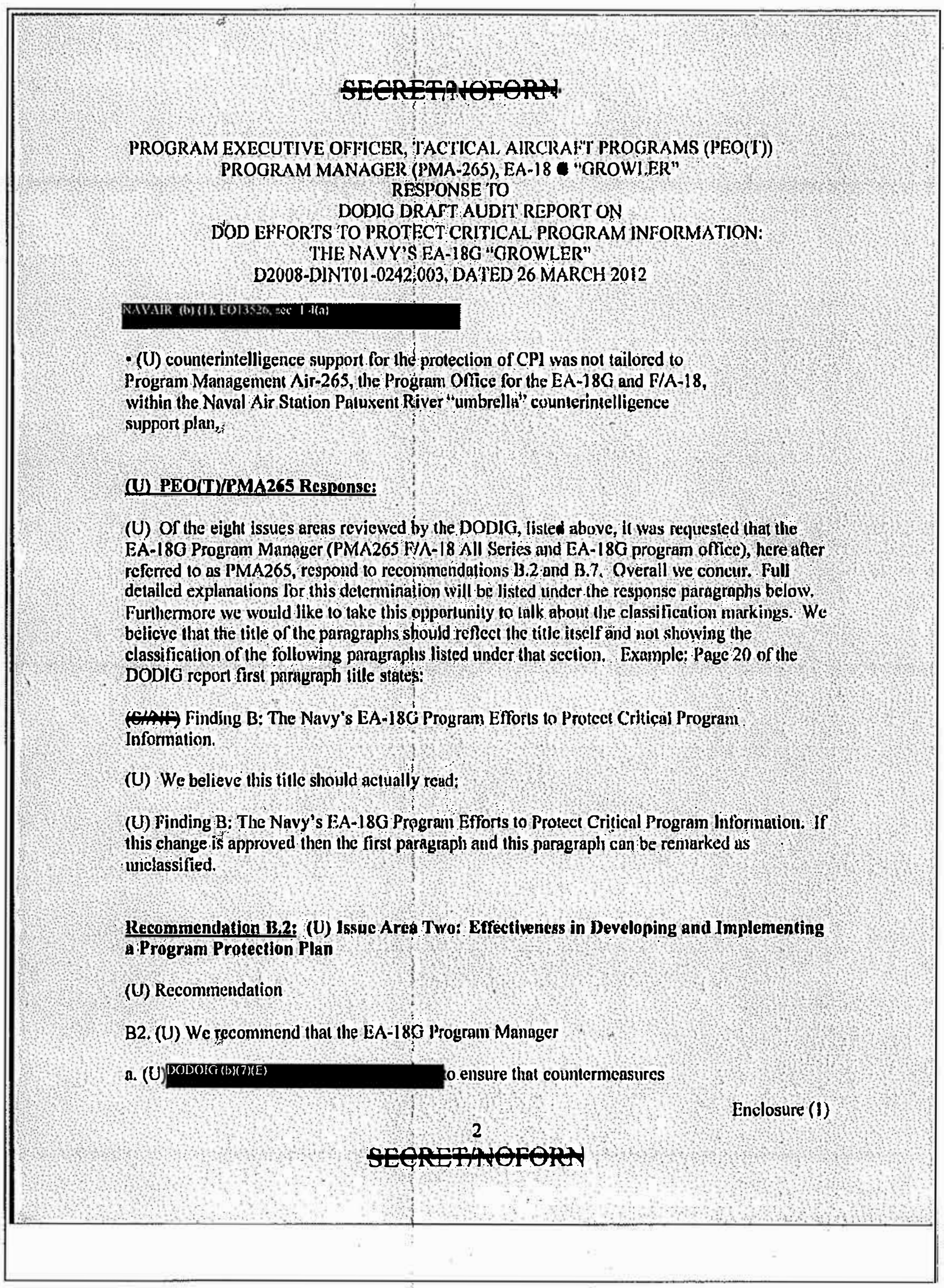
- ~~(S//NF)~~ NAVAIR (b)(1), EO13526, sec. 1.4(a) [redacted]

Enclosure (1)

1

~~SECRET//NOFORN~~

Assistant Secretary of the Navy for Research, Development and Acquisition and Program Manager, EA-18G Comments



~~SECRET/NOFORN~~

PROGRAM EXECUTIVE OFFICER, TACTICAL AIRCRAFT PROGRAMS (PEO(T))
PROGRAM MANAGER (PMA-265), EA-18 ● "GROWLER"
RESPONSE TO
DODIG DRAFT AUDIT REPORT ON
DOD EFFORTS TO PROTECT CRITICAL PROGRAM INFORMATION:
THE NAVY'S EA-18G "GROWLER"
D2008-DINT01-0242.003, DATED 26 MARCH 2012

NAVAIR (b)(1), EO13526, sec 1.4(a) [redacted]

- (U) counterintelligence support for the protection of CPI was not tailored to Program Management Air-265, the Program Office for the EA-18G and F/A-18, within the Naval Air Station Patuxent River "umbrella" counterintelligence support plan.,

(U) PEO(T)/PMA265 Response:

(U) Of the eight issues areas reviewed by the DODIG, listed above, it was requested that the EA-18G Program Manager (PMA265 F/A-18 All Series and EA-18G program office), here after referred to as PMA265, respond to recommendations B.2 and B.7. Overall we concur. Full detailed explanations for this determination will be listed under the response paragraphs below. Furthermore we would like to take this opportunity to talk about the classification markings. We believe that the title of the paragraphs should reflect the title itself and not showing the classification of the following paragraphs listed under that section. Example: Page 20 of the DODIG report first paragraph title states:

~~(S//NF)~~ Finding B: The Navy's EA-18G Program Efforts to Protect Critical Program Information.

(U) We believe this title should actually read:

(U) Finding B: The Navy's EA-18G Program Efforts to Protect Critical Program Information. If this change is approved then the first paragraph and this paragraph can be remarked as unclassified.

Recommendation B.2: (U) Issue Area Two: Effectiveness in Developing and Implementing a Program Protection Plan

(U) Recommendation

B2. (U) We recommend that the EA-18G Program Manager

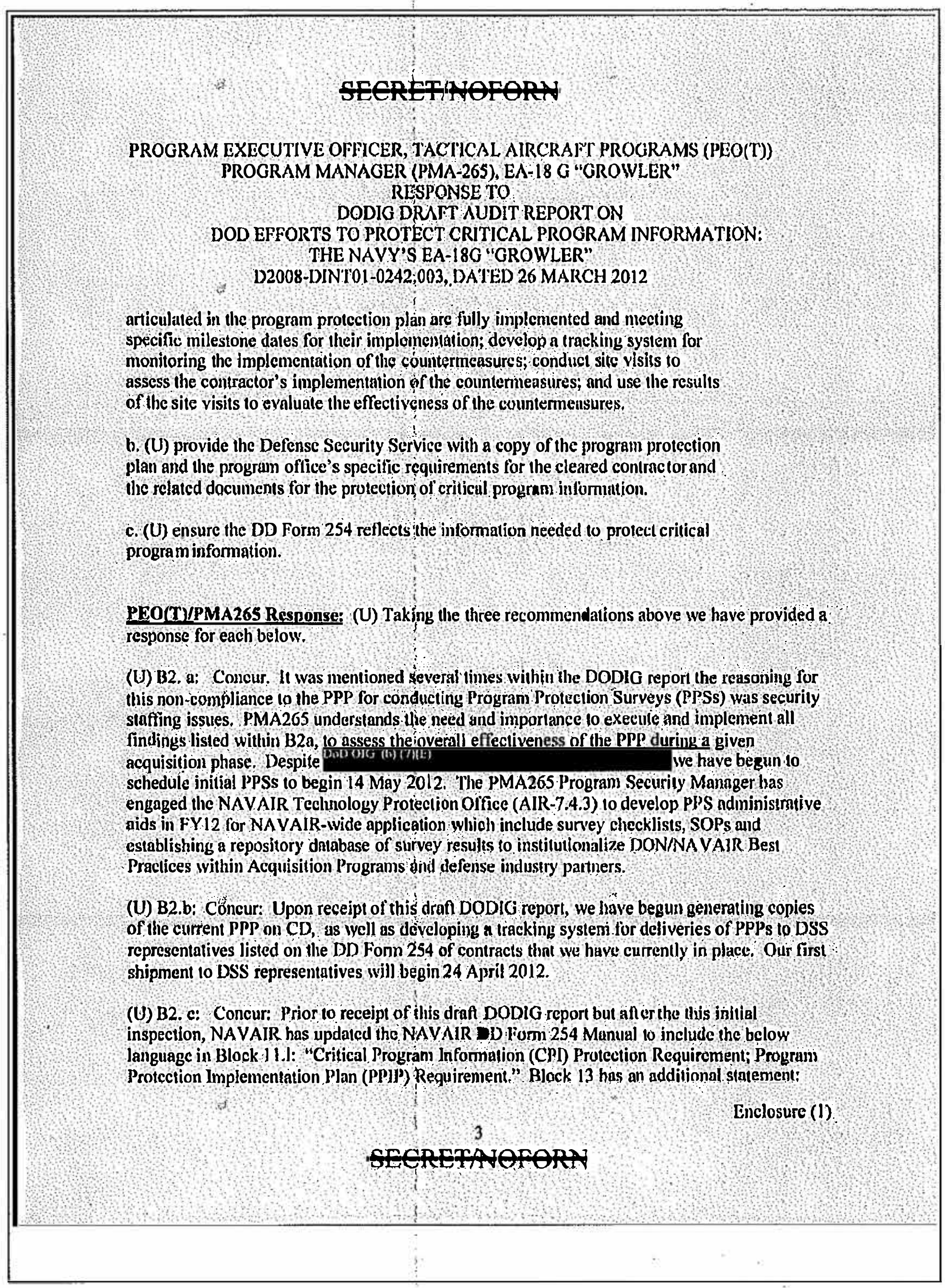
a. (U) DODOIG (b)(7)(E) [redacted] o ensure that countermeasures

Enclosure (1)

2

~~SECRET/NOFORN~~

Assistant Secretary of the Navy for Research, Development and Acquisition and Program Manager, EA-18G Comments



~~SECRET/NOFORN~~

PROGRAM EXECUTIVE OFFICER, TACTICAL AIRCRAFT PROGRAMS (PEO(T))
PROGRAM MANAGER (PMA-265), EA-18 G "GROWLER"
RESPONSE TO
DODIG DRAFT AUDIT REPORT ON
DOD EFFORTS TO PROTECT CRITICAL PROGRAM INFORMATION:
THE NAVY'S EA-18G "GROWLER"
D2008-DINT01-0242.003, DATED 26 MARCH 2012

articulated in the program protection plan are fully implemented and meeting specific milestone dates for their implementation; develop a tracking system for monitoring the implementation of the countermeasures; conduct site visits to assess the contractor's implementation of the countermeasures; and use the results of the site visits to evaluate the effectiveness of the countermeasures.

b. (U) provide the Defense Security Service with a copy of the program protection plan and the program office's specific requirements for the cleared contractor and the related documents for the protection of critical program information.

c. (U) ensure the DD Form 254 reflects the information needed to protect critical program information.

PEO(T)/PMA265 Response: (U) Taking the three recommendations above we have provided a response for each below.

(U) B2. a: Concur. It was mentioned several times within the DODIG report the reasoning for this non-compliance to the PPP for conducting Program Protection Surveys (PPSs) was security staffing issues. PMA265 understands the need and importance to execute and implement all findings listed within B2a, to assess the overall effectiveness of the PPP during a given acquisition phase. Despite DoD OIG (b)(7)(E) we have begun to schedule initial PPSs to begin 14 May 2012. The PMA265 Program Security Manager has engaged the NAVAIR Technology Protection Office (AIR-7.4.3) to develop PPS administrative aids in FY12 for NAVAIR-wide application which include survey checklists, SOPs and establishing a repository database of survey results to institutionalize DON/NAVAIR Best Practices within Acquisition Programs and defense industry partners.

(U) B2.b: Concur: Upon receipt of this draft DODIG report, we have begun generating copies of the current PPP on CD, as well as developing a tracking system for deliveries of PPPs to DSS representatives listed on the DD Form 254 of contracts that we have currently in place. Our first shipment to DSS representatives will begin 24 April 2012.

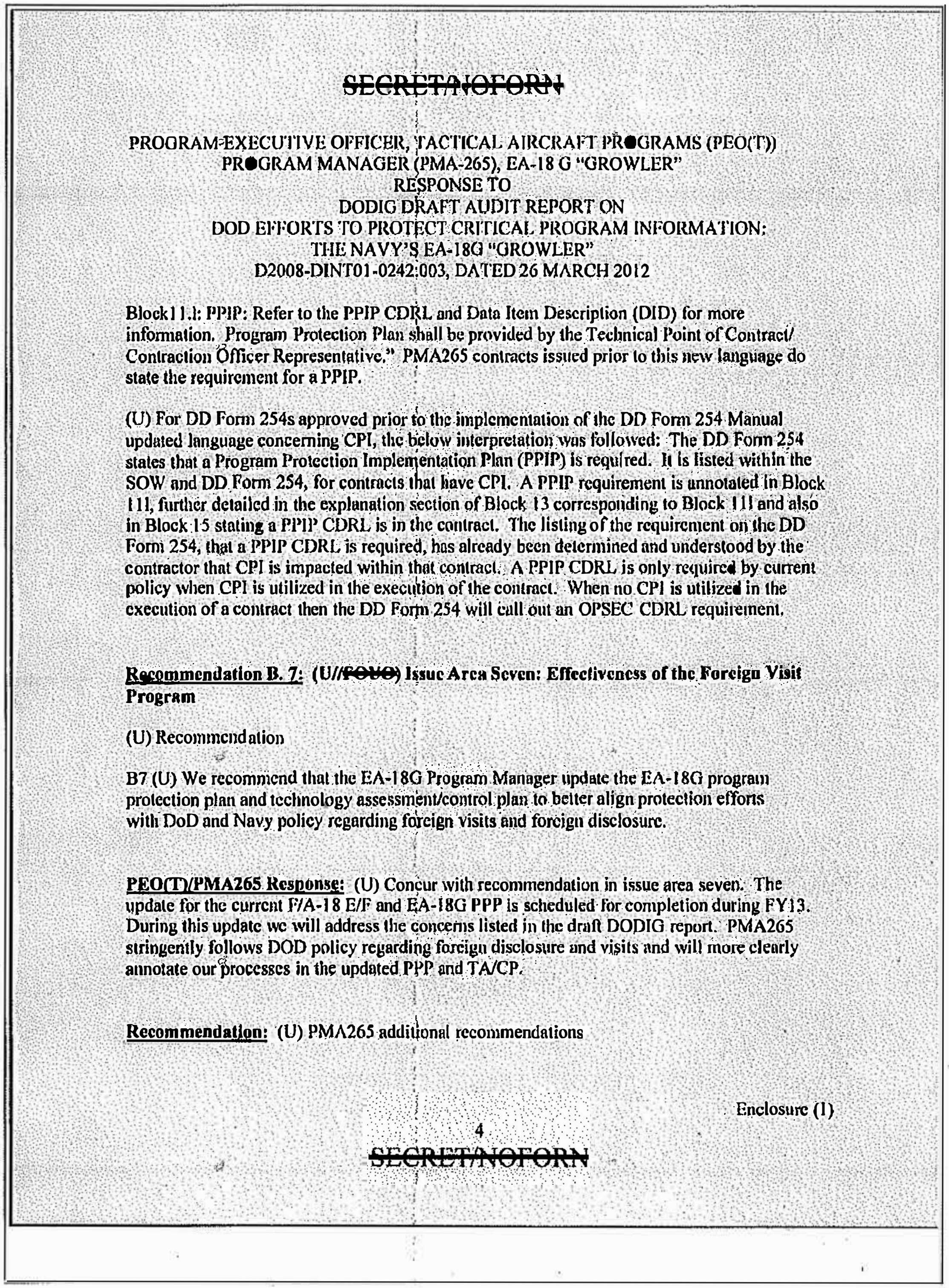
(U) B2. c: Concur: Prior to receipt of this draft DODIG report but after the this initial inspection, NAVAIR has updated the NAVAIR DD Form 254 Manual to include the below language in Block 11.l: "Critical Program Information (CPI) Protection Requirement; Program Protection Implementation Plan (PPIP) Requirement." Block 13 has an additional statement:

Enclosure (1)

3

~~SECRET/NOFORN~~

Assistant Secretary of the Navy for Research, Development and Acquisition and Program Manager, EA-18G Comments



~~SECRET//NOFORN~~

PROGRAM EXECUTIVE OFFICER, TACTICAL AIRCRAFT PROGRAMS (PEO(T))
PROGRAM MANAGER (PMA-265), EA-18 G "GROWLER"
RESPONSE TO
DODIG DRAFT AUDIT REPORT ON
DOD EFFORTS TO PROTECT CRITICAL PROGRAM INFORMATION:
THE NAVY'S EA-18G "GROWLER"
D2008-DINT01-0242.003, DATED 26 MARCH 2012

Block11.1: PPIP: Refer to the PPIP CDRL and Data Item Description (DID) for more information. Program Protection Plan shall be provided by the Technical Point of Contract/ Contraction Officer Representative." PMA265 contracts issued prior to this new language do state the requirement for a PPIP.

(U) For DD Form 254s approved prior to the implementation of the DD Form 254 Manual updated language concerning CPI, the below interpretation was followed: The DD Form 254 states that a Program Protection Implementation Plan (PPIP) is required. It is listed within the SOW and DD Form 254, for contracts that have CPI. A PPIP requirement is annotated in Block 11l, further detailed in the explanation section of Block 13 corresponding to Block 11l and also in Block 15 stating a PPIP CDRL is in the contract. The listing of the requirement on the DD Form 254, that a PPIP CDRL is required, has already been determined and understood by the contractor that CPI is impacted within that contract. A PPIP CDRL is only required by current policy when CPI is utilized in the execution of the contract. When no CPI is utilized in the execution of a contract then the DD Form 254 will call out an OPSEC CDRL requirement.

Recommendation B. 7: (U//~~FOUO~~) Issue Area Seven: Effectiveness of the Foreign Visit Program

(U) Recommendation

B7 (U) We recommend that the EA-18G Program Manager update the EA-18G program protection plan and technology assessment/control plan to better align protection efforts with DoD and Navy policy regarding foreign visits and foreign disclosure.

PEO(T)/PMA265 Response: (U) Concur with recommendation in issue area seven. The update for the current F/A-18 E/F and EA-18G PPP is scheduled for completion during FY13. During this update we will address the concerns listed in the draft DODIG report. PMA265 stringently follows DOD policy regarding foreign disclosure and visits and will more clearly annotate our processes in the updated PPP and TA/CP.

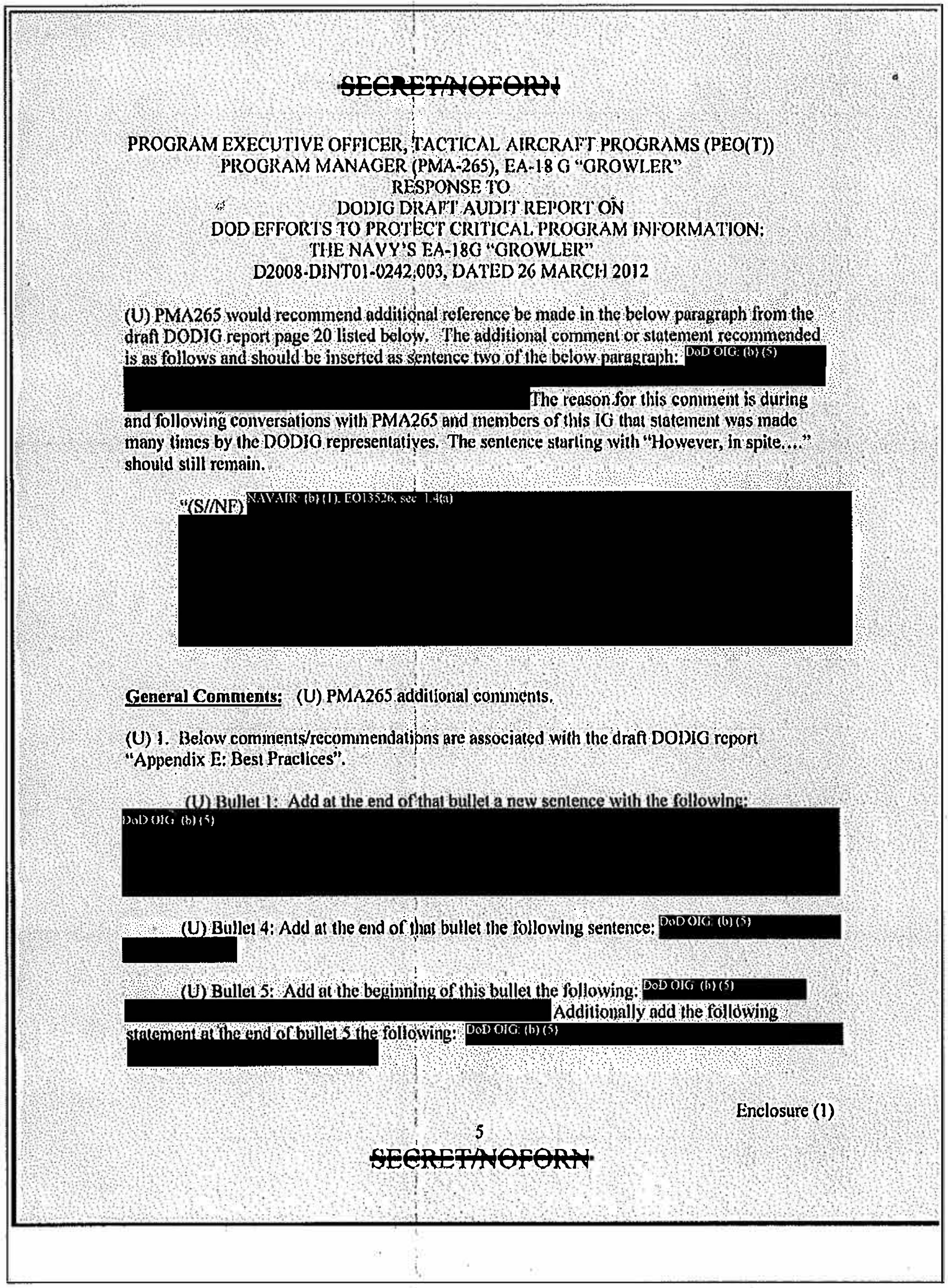
Recommendation: (U) PMA265 additional recommendations

Enclosure (1)

4

~~SECRET//NOFORN~~

Assistant Secretary of the Navy for Research, Development and Acquisition and Program Manager, EA-18G Comments



~~SECRET/NOFORN~~

PROGRAM EXECUTIVE OFFICER, TACTICAL AIRCRAFT PROGRAMS (PEO(T))
PROGRAM MANAGER (PMA-265), EA-18 G "GROWLER"
RESPONSE TO
DODIG DRAFT AUDIT REPORT ON
DOD EFFORTS TO PROTECT CRITICAL PROGRAM INFORMATION:
THE NAVY'S EA-18G "GROWLER"
D2008-DINT01-0242.003, DATED 26 MARCH 2012

(U) PMA265 would recommend additional reference be made in the below paragraph from the draft DODIG report page 20 listed below. The additional comment or statement recommended is as follows and should be inserted as sentence two of the below paragraph: DoD OIG: (b)(5) [redacted] The reason for this comment is during and following conversations with PMA265 and members of this IG that statement was made many times by the DODIG representatives. The sentence starting with "However, in spite...." should still remain.

"(S//NF) NAVAIR: (b)(1), EO13526, sec 1.4(a) [redacted]

General Comments: (U) PMA265 additional comments.

(U) 1. Below comments/recommendations are associated with the draft DODIG report "Appendix E: Best Practices".

(U) Bullet 1: Add at the end of that bullet a new sentence with the following: DoD OIG: (b)(5) [redacted]

(U) Bullet 4: Add at the end of that bullet the following sentence: DoD OIG: (b)(5) [redacted]

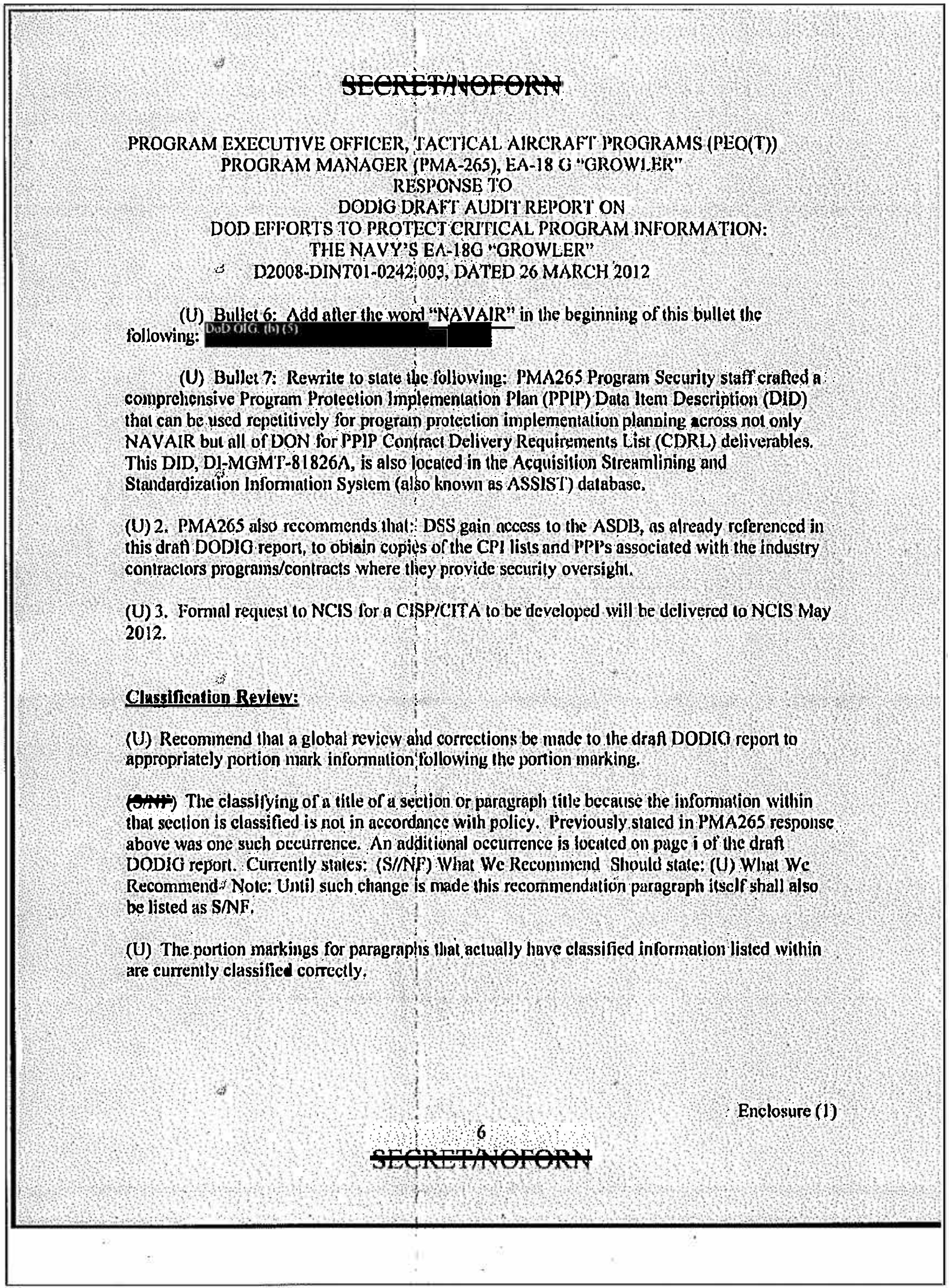
(U) Bullet 5: Add at the beginning of this bullet the following: DoD OIG: (b)(5) [redacted] Additionally add the following statement at the end of bullet 5 the following: DoD OIG: (b)(5) [redacted]

Enclosure (1)

5

~~SECRET/NOFORN~~

Assistant Secretary of the Navy for Research, Development and Acquisition and Program Manager, EA-18G Comments



~~SECRET//NOFORN~~

PROGRAM EXECUTIVE OFFICER, TACTICAL AIRCRAFT PROGRAMS (PEO(T))
PROGRAM MANAGER (PMA-265), EA-18 G "GROWLER"
RESPONSE TO
DODIG DRAFT AUDIT REPORT ON
DOD EFFORTS TO PROTECT CRITICAL PROGRAM INFORMATION:
THE NAVY'S EA-18G "GROWLER"
D2008-DINT01-0242.003, DATED 26 MARCH 2012

(U) Bullet 6: Add after the word "NAVAIR" in the beginning of this bullet the following: DoD OIG (b)(5) [redacted]

(U) Bullet 7: Rewrite to state the following: PMA265 Program Security staff crafted a comprehensive Program Protection Implementation Plan (PPIP) Data Item Description (DID) that can be used repetitively for program protection implementation planning across not only NAVAIR but all of DON for PPIP Contract Delivery Requirements List (CDRL) deliverables. This DID, DI-MGMT-81826A, is also located in the Acquisition Streamlining and Standardization Information System (also known as ASSIST) database.

(U) 2. PMA265 also recommends that: DSS gain access to the ASDB, as already referenced in this draft DODIG report, to obtain copies of the CPI lists and PPPs associated with the industry contractors programs/contracts where they provide security oversight.

(U) 3. Formal request to NCIS for a CISP/CITA to be developed will be delivered to NCIS May 2012.

Classification Review:

(U) Recommend that a global review and corrections be made to the draft DODIG report to appropriately portion mark information following the portion marking.

~~(S/NF)~~ The classifying of a title of a section or paragraph title because the information within that section is classified is not in accordance with policy. Previously stated in PMA265 response above was one such occurrence. An additional occurrence is located on page i of the draft DODIG report. Currently states: (S//NF) What We Recommend Should state: (U) What We Recommend. Note: Until such change is made this recommendation paragraph itself shall also be listed as S/NF.

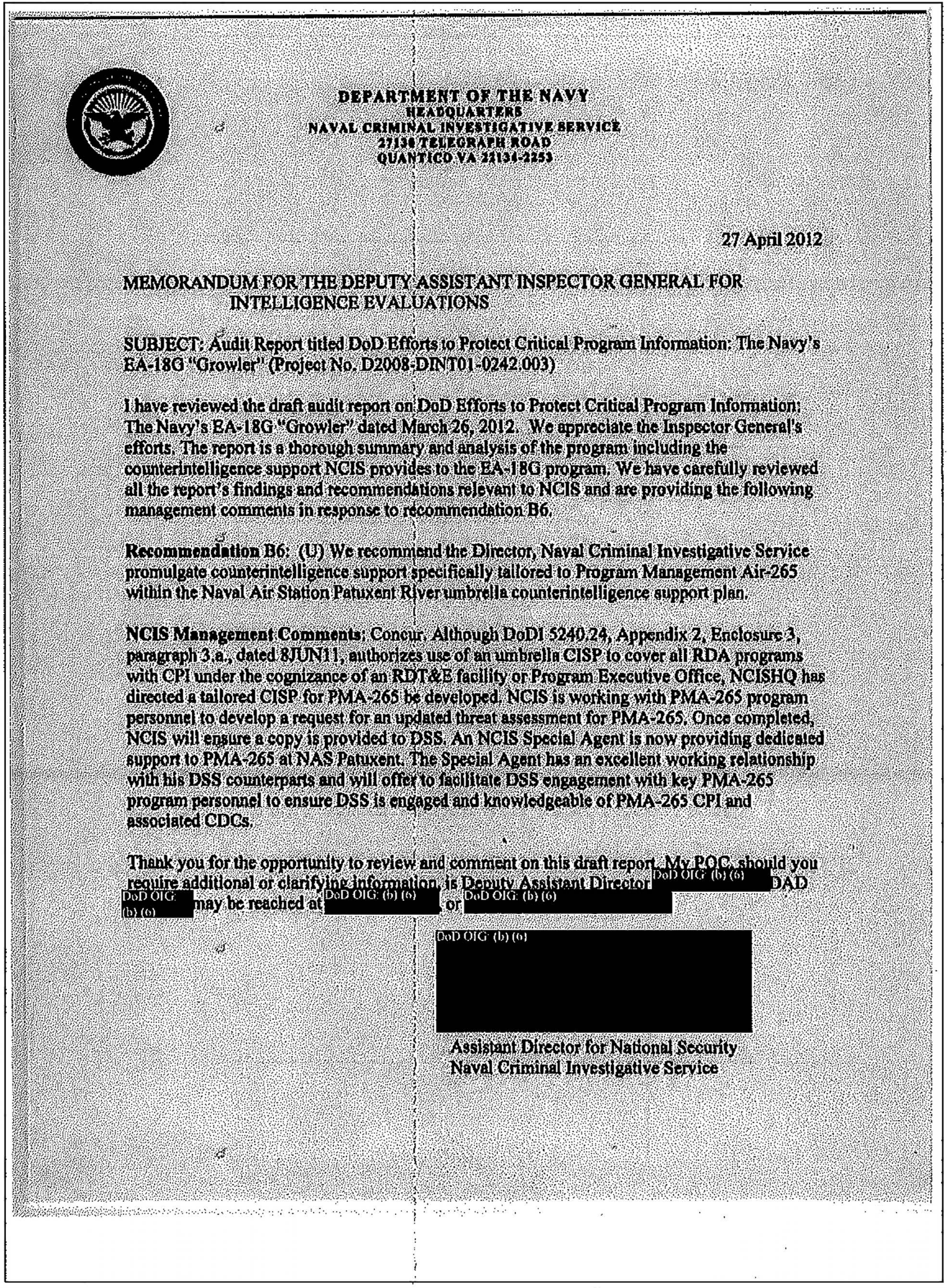
(U) The portion markings for paragraphs that actually have classified information listed within are currently classified correctly.

Enclosure (1)

6

~~SECRET//NOFORN~~

Naval Criminal Investigative Service Comments



DEPARTMENT OF THE NAVY
HEADQUARTERS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
27130 TELEGRAPH ROAD
QUANTICO VA 22134-2253

27 April 2012

MEMORANDUM FOR THE DEPUTY ASSISTANT INSPECTOR GENERAL FOR INTELLIGENCE EVALUATIONS

SUBJECT: Audit Report titled DoD Efforts to Protect Critical Program Information: The Navy's EA-18G "Growler" (Project No. D2008-DINT01-0242.003)

I have reviewed the draft audit report on DoD Efforts to Protect Critical Program Information: The Navy's EA-18G "Growler" dated March 26, 2012. We appreciate the Inspector General's efforts. The report is a thorough summary and analysis of the program including the counterintelligence support NCIS provides to the EA-18G program. We have carefully reviewed all the report's findings and recommendations relevant to NCIS and are providing the following management comments in response to recommendation B6.

Recommendation B6: (U) We recommend the Director, Naval Criminal Investigative Service promulgate counterintelligence support specifically tailored to Program Management Air-265 within the Naval Air Station Patuxent River umbrella counterintelligence support plan.

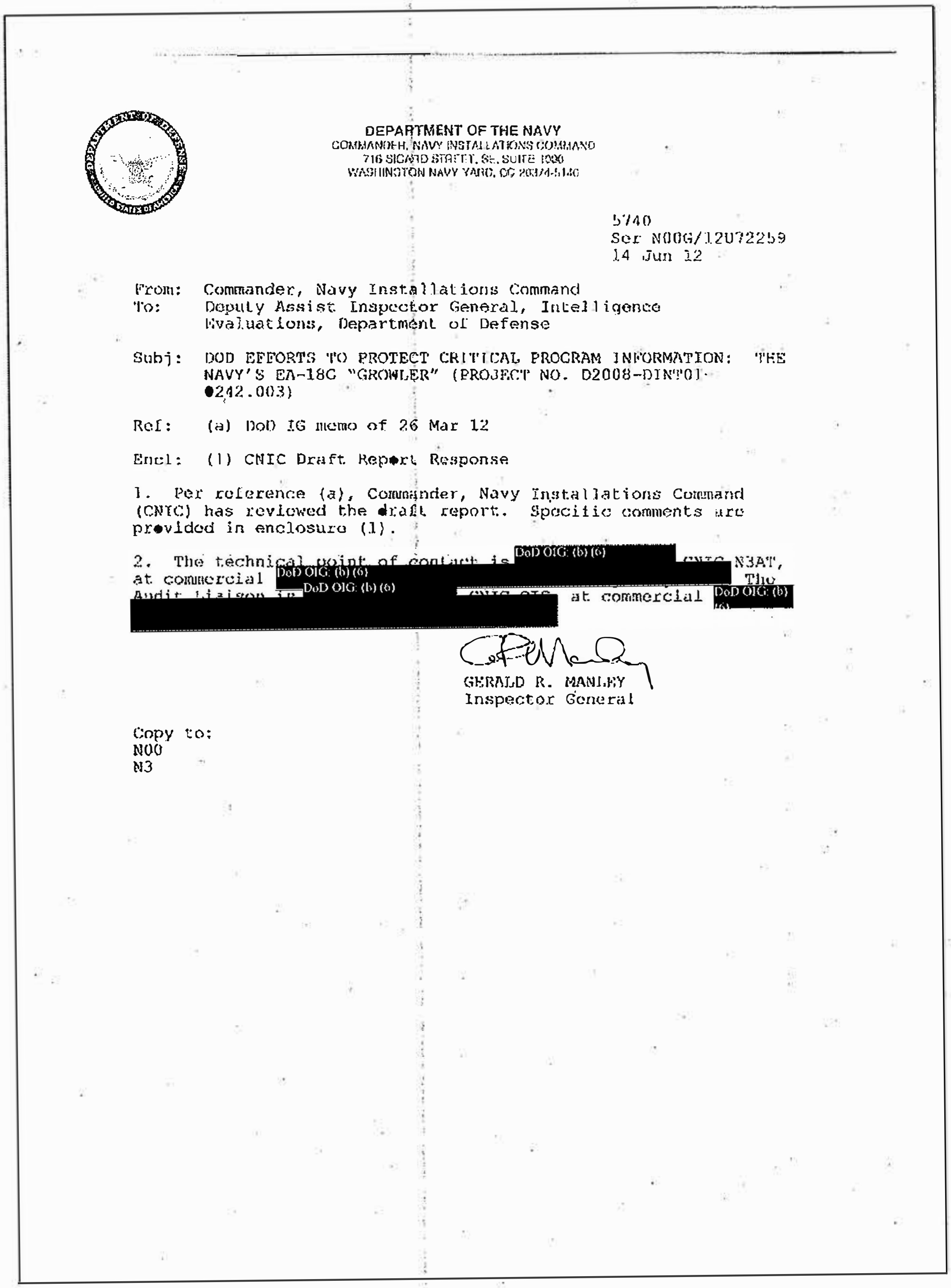
NCIS Management Comments: Concur. Although DoDI 5240.24, Appendix 2, Enclosure 3, paragraph 3.a., dated 8JUN11, authorizes use of an umbrella CISP to cover all RDA programs with CPI under the cognizance of an RDT&E facility or Program Executive Office, NCISHQ has directed a tailored CISP for PMA-265 be developed. NCIS is working with PMA-265 program personnel to develop a request for an updated threat assessment for PMA-265. Once completed, NCIS will ensure a copy is provided to DSS. An NCIS Special Agent is now providing dedicated support to PMA-265 at NAS Patuxent. The Special Agent has an excellent working relationship with his DSS counterparts and will offer to facilitate DSS engagement with key PMA-265 program personnel to ensure DSS is engaged and knowledgeable of PMA-265 CPI and associated CDCs.

Thank you for the opportunity to review and comment on this draft report. My POC, should you require additional or clarifying information, is Deputy Assistant Director DoD OIG: (b) (6) DAD DoD OIG: (b) (6) may be reached at DoD OIG: (b) (6), or DoD OIG: (b) (6).

DoD OIG: (b) (6)

Assistant Director for National Security
Naval Criminal Investigative Service

Commander, Navy Installations Command Comments



DEPARTMENT OF THE NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
716 SICARD STREET, SE, SUITE 1000
WASHINGTON NAVY YARD, DC 20374-5140

5740
Ser N00G/12U72259
14 Jun 12

From: Commander, Navy Installations Command
To: Deputy Assist Inspector General, Intelligence Evaluations, Department of Defense

Subj: DOD EFFORTS TO PROTECT CRITICAL PROGRAM INFORMATION: THE NAVY'S EA-18G "GROWLER" (PROJECT NO. D2008-DINT01-0242.003)

Ref: (a) DoD IG memo of 26 Mar 12

Encl: (1) CNIC Draft Report Response

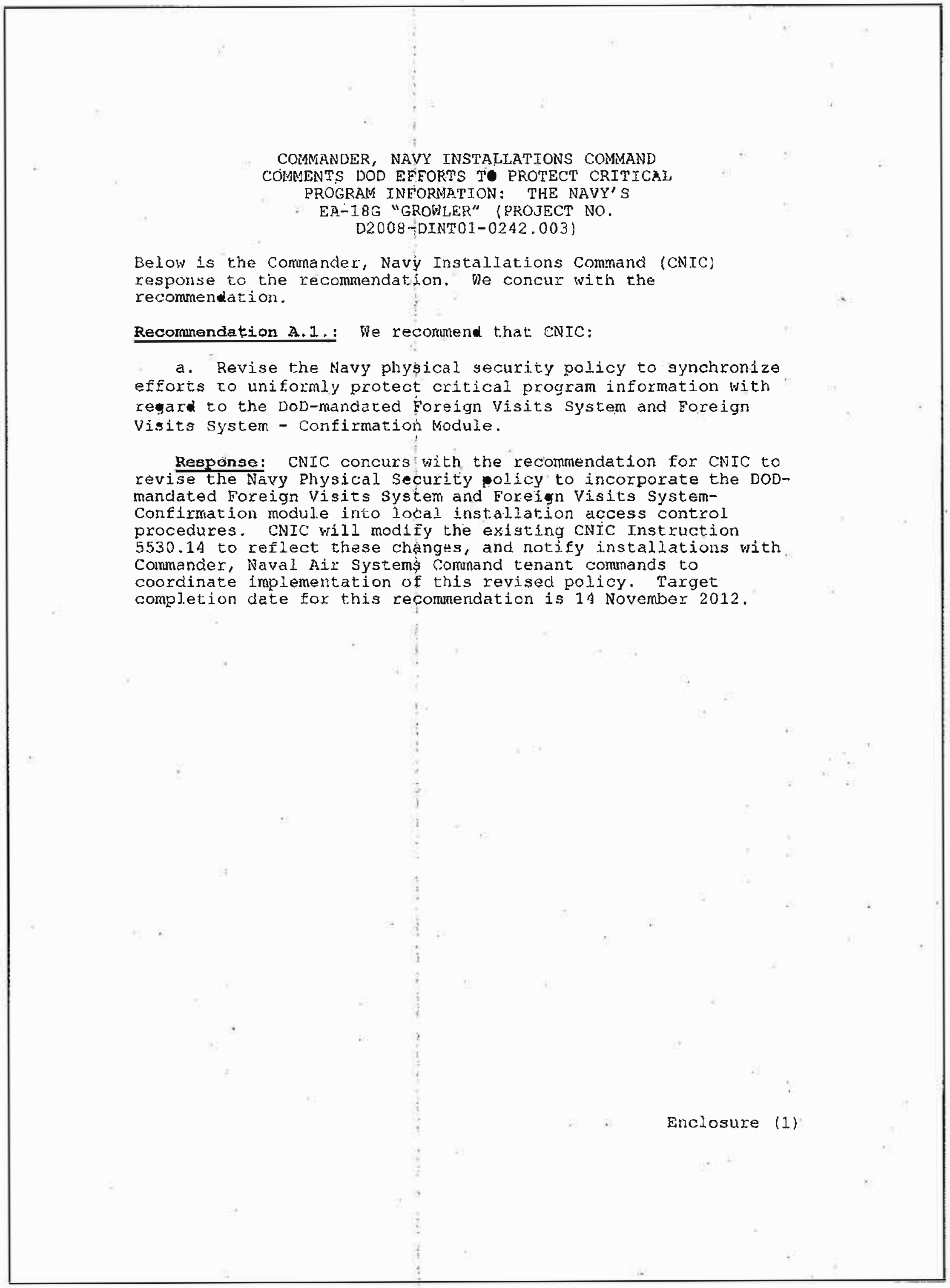
1. Per reference (a), Commander, Navy Installations Command (CNIC) has reviewed the draft report. Specific comments are provided in enclosure (1).

2. The technical point of contact is DoD OIG: (b)(6) N3AT, at commercial DoD OIG: (b)(6) The DoD OIG: (b)(6) CNIC OIG, at commercial DoD OIG: (b)(6) [redacted]

GERALD R. MANLEY
Inspector General

Copy to:
N00
N3

Commander, Navy Installations Command Comments



COMMANDER, NAVY INSTALLATIONS COMMAND
COMMENTS DOD EFFORTS TO PROTECT CRITICAL
PROGRAM INFORMATION: THE NAVY'S
EA-18G "GROWLER" (PROJECT NO.
D2008-DINT01-0242.003)

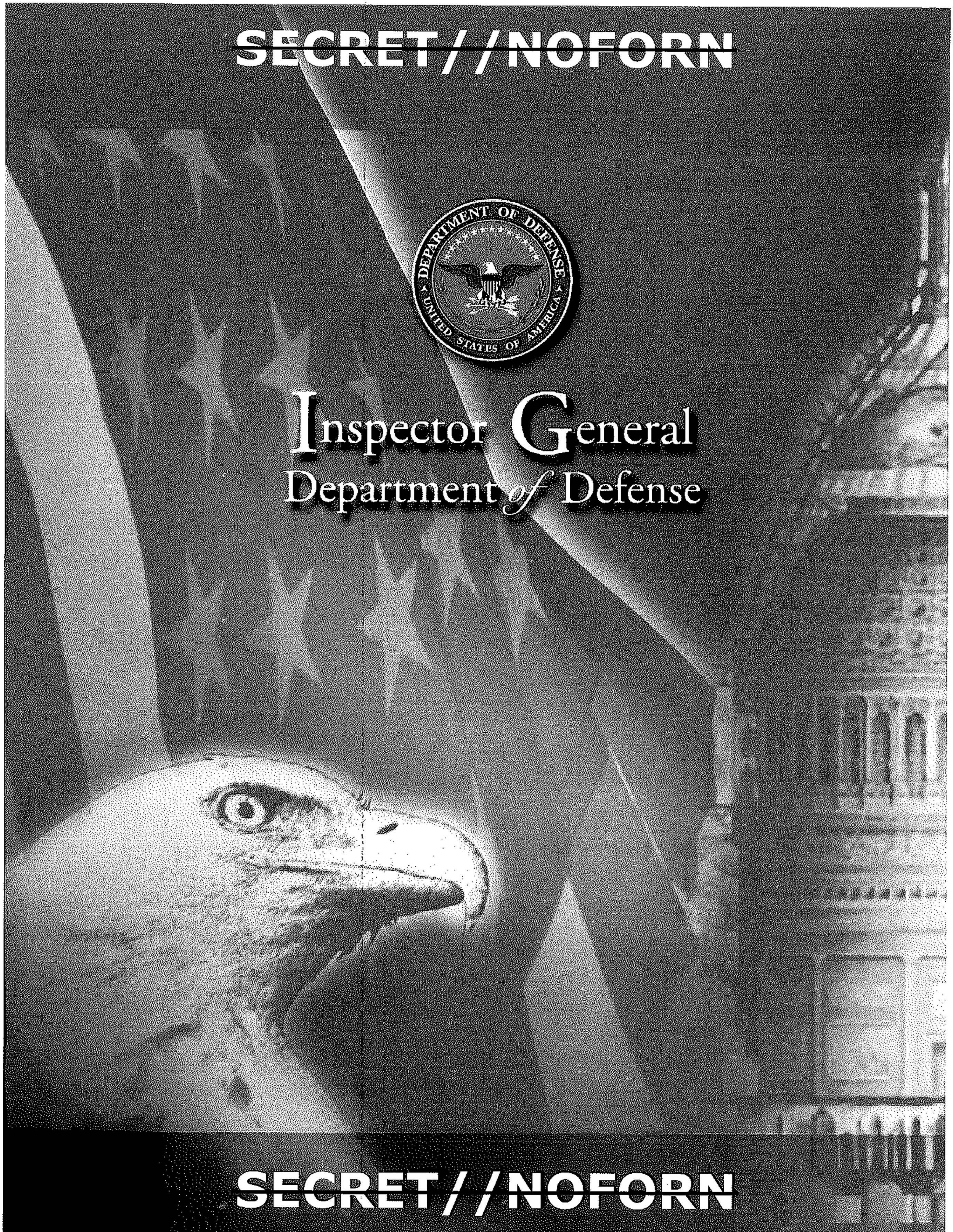
Below is the Commander, Navy Installations Command (CNIC) response to the recommendation. We concur with the recommendation.

Recommendation A.1.: We recommend that CNIC:

a. Revise the Navy physical security policy to synchronize efforts to uniformly protect critical program information with regard to the DoD-mandated Foreign Visits System and Foreign Visits System - Confirmation Module.

Response: CNIC concurs with the recommendation for CNIC to revise the Navy Physical Security policy to incorporate the DOD-mandated Foreign Visits System and Foreign Visits System-Confirmation module into local installation access control procedures. CNIC will modify the existing CNIC Instruction 5530.14 to reflect these changes, and notify installations with Commander, Naval Air Systems Command tenant commands to coordinate implementation of this revised policy. Target completion date for this recommendation is 14 November 2012.

Enclosure (1)



Inspector General
Department of Defense