Report Number:
DoDIG-2012-142
September 28, 2012

Inspector General
United States Department of Defense

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE AND SPECIAL PROGRAM ASSESSMENTS

Summary Report of FY 2011 Inspections on Security, Intelligence, Counterintelligence, and Technology Protection Practices at DoD Research, Development, Test, and Evaluation Facilities

~~FOR OFFICIAL USE ONLY~~

Additional Information and Copies

For information and to request copies of this summary, contact the DoD Office of Inspector General at (703) 882-[b)(6)] or DSN 381-[b)(6)].

Suggestions for Future Audits and Evaluations

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-[b)(6)] (DSN 381-[b)(6)]) or UNCLASSIFIED fax (571) 372-7451. Ideas and requests can also be mailed to:

ODIG-ISPA (ATTN: ISPA Suggestions)
Department of Defense Inspector General
4800 Mark Center Drive (Suite 10J25)
Alexandria, VA 22350-1500

Acronyms and Abbreviations

ACAT	Acquisition Category
AFOSI	Air Force Office of Special Investigations
CPI	Critical Program Information
DoD CIO	DoD Chief Information Officer
DSS	Defense Security Service
IG	Inspector General
MDA	Missile Defense Agency
NCIS	Naval Criminal Investigative Service
OIG	Office of Inspector General
OPSEC	Operations Security
PM	Program Manager
RDA	Research, Development, and Acquisition
RDT&E	Research, Development, Test, and Evaluation
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence

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

September 28, 2012

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Summary Report of FY 2011 Inspections on Security, Intelligence, Counterintelligence, and Technology Protection Practices at DoD Research, Development, Test, and Evaluation Facilities
(Report No. DoDIG-2012-142)

We are providing this report for your information and use. We issued a draft of this report on September 24, 2012. No written response to this report was required and none was received. Therefore, we are publishing this report in final form.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 882-(b)(6) (DSN 381-(b)(6)).

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

DISTRIBUTION:

OFFICE OF THE SECRETARY OF DEFENSE
- Under Secretary of Defense for Acquisition, Technology, and Logistics
- Under Secretary of Defense for Policy
- Under Secretary of Defense for Intelligence
- DoD Chief Information Officer
- Director, Defense Information Systems Agency
- Director, Defense Security Service

DEPARTMENT OF THE ARMY
- Assistant Secretary of the Army for Acquisition, Logistics, and Technology
- Commanding General, Army Materiel Command
  - G-2, Army Materiel Command
- Deputy Chief of Staff, G-2
- Inspector General, Department of the Army
  - Auditor General, Department of the Army Service

DEPARTMENT OF THE NAVY
- Assistant Secretary of the Navy for Research, Development, and Acquisition
- Naval Criminal Investigative Service
- Naval Inspector General
- Auditor General of the Navy

DEPARTMENT OF THE AIR FORCE
- Assistant Secretary of the Air Force for Acquisition
- Administrative Assistant to the Secretary of the Air Force
- Inspector General, Department of the Air Force
- Commander, Air Force Materiel Command
- Commander, Air Force Office of Special Investigations
- Auditor General of the Air Force

CONGRESSIONAL COMMITTEES AND SUBCOMMITTEES, CHAIRMAN AND RANKING
- Senate Subcommittee on Defense, Committee on Appropriations
- Senate Committee on Armed Services
- Senate Select Committee on Intelligence
- Senate Committee on Homeland Security and Governmental Affairs
- House Committee on Armed Services
- House Permanent Select Committee on Intelligence
- House Committee on Oversight and Government Reform
- House Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform
- House Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform

Results in Brief: Summary of FY 2011 Inspections on Security, Intelligence, Counterintelligence, and Technology Protection Practices at DoD Research, Development, Test, and Evaluation Facilities

What Was Done

This summary is a compilation of inspection results from the DoD, Service, and Missile Defense Agency (MDA) Offices of Inspectors General (OIG) and, where available, notes the best practices of each. The DoD OIG assessed an acquisition category 1D program; the Service IGs selected 34 of 118 research, development, test, and evaluation (RDT&E) facilities under their purview for inspection; and the MDA looked at the effectiveness of their critical program information (CPI) identification and program protection planning efforts, as well as their international security program. These inspections ensure a uniform system of periodic reviews for compliance with directives concerning security, intelligence, counterintelligence, and technology protection practices. The OIGs used the biennial inspection guidelines that focus on eight key issue areas related to program protection.

What Was Found

Identifying CPI. Generally, an effective process for identifying CPI was found, with some having a standardized process for identifying CPI. However, 5 of the 35 sites inspected did not adequately identify specific CPI.

Program Protection Planning. Efforts to protect CPI are not integrated and synchronized to the greatest extent possible. In some instances, program protection plans were not completed and could not be assessed. However, in general CPI was incorporated into program protection plans.

Training and Education. Training for the protection of CPI was not tailored for intelligence and security personnel; and some personnel were not qualified to do the job. Moreover, the level of training related to CPI protection varied, with some personnel with no training, others with training acquired on the job and still others with training offered by the research, development, and acquisition (RDA) program support organization.

Resources. DoD OIG's assessment found no embedded program security support. The program management office did not track all security costs nor did they report program protection or security-related expenditures, in order to establish budget projections for security throughout the program's life-cycle and with measuring the return on the security expenditures.

Security and Other Support. Although program staff requested and were provided intelligence support, it was not timely nor tailored to CPI, adversely affecting the PM's ability to implement an effective program protection plan. Service findings ranged from PMs not using counterintelligence assets correctly to counterintelligence assets being spread thin due to deployments and ad-hoc tasking.

Foreign Visitor Program. No major issues were noted with the effectiveness of the programs inspected. MDA was using the Foreign Visits System – Confirmation Module.

Horizontal Protection. Data from an Air Force program was on a separate horizontal protection database, but recent guidance will allow Air Force to use the Acquisition Security Database.

CPI Policies. While DoD and Service policies to protect CPI have progressed in recent years, there is still a need for improvement.

Table of Contents

Introduction

In accordance with DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008, Enclosure 2, paragraph 5, this report consolidates the assessment and inspection results of participating Inspectors General (IGs) who inspect technology protection, security, intelligence, and counterintelligence practices at RDT&E facilities.

Scope and Methodology

This summary covers inspections of security, intelligence, counterintelligence, and technology protection, activities at DoD RDT&E facilities conducted by or at the direction of the participating IGs, as outlined in Appendix A. It also includes the results of the second in a series of three reports by the DoD OIG,[1] 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 DoD OIG consolidates and distributes the lists of major RDT&E facilities to the participating IGs, the Assistant Secretary of Defense for Research and Engineering, and the Director, Defense Test Resource Management Center. The Assistant Secretary of Defense for Research and Engineering and the Director, Defense Test Resource Management Center, may recommend additional Defense agency facilities for inspection. The participating IGs select from their respective lists those facilities that will be inspected and forward the selections to the DoD OIG, as outlined in Appendix B.

The inspections were performed during the course of the inspection programs of the participating IGs, to include, in the case of military IGs, the inspection programs of their subordinate IGs. To ensure uniformity and consistency of inspections, the DoD OIG biennially issues guidelines for DoD IGs. The participating IGs coordinate modifications or customizations of the inspection guidelines. The participating IGs conducting or directing inspections ensure that inspection findings and recommendations are addressed and implemented.

The participating IGs use their own procedures to write findings and recommendations within their respective areas of responsibility. The participating IGs prepare and forward any significant findings and recommendations, upon the conclusion of each inspection to the DoD OIG and the DoD OIG produces this summary. The DoD OIG did not review or verify the information provided.

Background

In 2010, the DoD OIG published the latest biennial version of inspection guidelines for use by IGs and other oversight practitioners to enhance the protection of CPI. Different from previous years, the guidelines are tailored to focus on the eight key issue areas that assist in determining the effectiveness to protect CPI.

---

[1] The Office of the Deputy Inspector General for Intelligence and Special Program Assessments is the Office of Primary Responsibility within the DoD OIG for matters relating to inspections of RDT&E facilities.

The inspection guidelines were developed to provide consistency across the Department when assessing security, intelligence, and counterintelligence support to RDA protection efforts aimed at protecting CPI. The guidelines focus on eight key issue areas that assist in determining the effectiveness to protect CPI. The eight key issue areas for inspections (with additions to this iteration highlighted) to address are:

1. CPI identification and *criticality analysis*;
2. program protection planning;
3. training and education to protect CPI, *critical functionality, and critical components*;
4. use of resources/billets to protect CPI, *critical functionality, and critical components;*;
5. security, intelligence, and counterintelligence support to protect CPI, *critical functionality, and critical components*;
6. foreign visits program;
7. horizontal protection of CPI, *critical functionality, and critical components*; and
8. policies to protect CPI, *critical functionality, and critical components*.

Success in each of the eight key issue areas leads to enhanced counterintelligence, intelligence, and security support to RDT&E facilities and the acquisition process. Focusing the annual inspections on these eight key areas provides a better ability to identify trends and systemic issues.

The office of the USD(AT&L), provided a chart depicting the vast amounts of policy related to RDA protection. The chart found at the link below, organizes acquisition security policies and guidance by purpose and 23 offices of responsibility. The chart shows the 145 policies that an acquisition program may need to comply with. http://www.acq.osd.mil/se/docs/acq-security-policy-tool/index.html.

1. Critical Program Information (CPI) Identification and Criticality Analysis

This issue area was assessed to determine whether published guidance for the identification of CPI is relevant 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.

DoD Office of Inspector General

In the case study of the acquisition category (ACAT) ID Air Force program, the program office staff had an effective process for identifying CPI and an integrated product team comprised of systems engineering, information assurance, engineering management, business management, software engineering experts, and the Air Force Office of Special Investigations (AFOSI). Security, counterintelligence, intelligence, and user representatives served in an advisory capacity. The Air Force program 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.

Office of the Army Inspector General

The Office of the Army IG had no significant findings in this issue area.

Office of the Naval Inspector General

Commands inspected had a standardized process for identifying CPI in accordance with governing instructions; and anti-tampering procedures were instituted where applicable.

Office of the Air Force Inspector General

Of the twenty-two inspected, five of six Center's PMs did not adequately identify specific CPI. PMs identified operations security information as CPI. PMs also identified broad CPI categories without proper drill down to identify CPI. The Air Force IG recommended that programs conduct more in-depth training and that PMs conduct full system decomposition of programs and work with associated programs to identify CPI and inherited CPI, and include support contractors in CPI protection efforts. One agency did not coordinate with owning sub-system program offices to obtain program protection plans so they could identify inherited CPI and associated countermeasures.

Missile Defense Agency (MDA)

MDA reviewed steps taken during the CPI assessment phase for one program. The program was selected because it was the first to execute the CPI assessment phase following issuance of MDA's new instruction, MDA Instruction 5200.08-INS, "Critical Program Information Protection Within the Missile Defense Agency," August 1, 2011, and draft CPI protection manual. Specifically, MDA identified and surveyed members of the integrated product team, determined if immediate countermeasures were identified, and determined if MDA 5200.08-INS and the MDA CPI protection manual were followed. The program used the following in identifying and protecting CPI during the CPI assessment phase:

- The program's integrated product team had a diverse workgroup to represent the key areas involved during the CPI/program protection planning process including acquisition, engineering, security, intelligence, and counterintelligence personnel.
- The functional decomposition list, which breaks down the entire program into smaller more tangible segments, included the areas evaluated for CPI and indentified sources and references.
- The integrated product team identified broad immediate countermeasures after the identification of candidate CPI.
- The Director for Engineering appropriately chaired and initiated the Acquisition Program Protection Panel to review and approve the candidate CPI, and signed the CPI assessment memorandum prepared in accordance with MDA guidance.
- Based on the identification of CPI, a program protection plan was drafted. The program protection plan is treated as a living document and is updated on a continuous/as needed basis until approved, and the program office is awaiting the multidisciplinary counterintelligence threat assessment from the counterintelligence personnel before moving forward with program protection plan approval.
- The program's security classification guide was initiated and included CPI protection information and they are awaiting the multidisciplinary counterintelligence threat assessment from the counterintelligence personnel before finalizing the draft security classification guide.

2. Program Protection Planning

This issue area was assessed to determine whether published guidance for the planning of program protection is relevant and adhered to by program, intelligence, counter-intelligence, and security personnel and to ensure that program protection planning was in accordance with DoD Instruction 5200.39 and corresponding Service policy.

DoD Office of Inspector General

Because the Air Force ACAT ID program office had not completed its program protection plan; we were unable to assess the plan's effectiveness. The program was taking the steps to formally notify the prime contractor, second-tier integrator, and relevant subcontractors of the potential existence of CPI, and had plans to direct appropriate protection measures. However, Defense Security Service (DSS) personnel were not informed that program CPI resided within the prime contractors' and subcontractors' facilities. One reason was that the presence of CPI was not identified in the DD Form 254. Program management offices should notify the DSS office covering cleared contractor facilities holding CPI of the CPI presence, nature, and any special concerns (unique compromising characteristics). Publishing guidance that provides model contract language would make it easier for programs to contract for CPI protection. Program management offices should:

- provide the DSS with the program protection plan and the program office's specific requirements for the cleared contractor and the related documents for the protection of CPI, a list of the related counterintelligence and security risks to the contractor, and a copy of the relevant counterintelligence support plan;
- ensure that contracts require the prime contractor to participate in the identification of CPI and to implement countermeasures for identified CPI at contractor facilities;
- ensure contracts and DD Forms 254 include clauses authorizing certain Government personnel access to prime contractor and subcontractor facilities to conduct surveys, assessments, inspections, and investigations as necessary to make sure CPI is properly protected; and
- include language in contracts that the prime contractor must:
    - communicate program protection requirements to subcontractors that will have access to or will be providing CPI,
    - require subcontractors to continually monitor protection measures, and
    - monitor the subcontractors' performance monitoring.

Once the program protection plan is complete, the PM should fully implement countermeasures articulated in the program protection plan, 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. The PM should also require the contractor to prepare a program protection implementation plan to inform the program management office how the contractor intends to protect CPI and implement the countermeasures articulated in the program protection plan.

Guidance was not developed that specifically addressed the protection requirements for CPI that resides on contractor-owned and -operated information systems. The DoD Chief Information Officer, in coordination with the USD(AT&L) and the Under Secretary of Defense for Intelligence (USD(I)) agreed to our recommendation to develop and publish security requirements for contractors processing CPI on contractor-owned and -controlled information systems; to which they concurred and initiated a Defense Federal Acquisition Regulation System case in March 2011.

The program staff requested and was provided the required counterintelligence and intelligence support and threat-related data. However, the threat data was not timely, affecting the PM's ability to formulate and implement an effective program protection plan. Furthermore, the threat data was not tailored to the CPI, decreasing the utility for program staff. The modular approach of the Virtual System Threat Assessment Report may offer a more streamlined process for creating and updating System Threat Assessment Reports.

Office of the Army Inspector General

Identified CPI was incorporated into program protection plans at all facilities inspected in 2011.

Office of the Naval Inspector General

In general, Navy PMs are trained on program protection planning processes for protecting CPI and on overall DoD and Navy acquisition security requirements. CPI elements were identified and incorporated into a program protection plan. Ability to correctly identify CPI elements at other facilities remains under examination as of this report. In addition, security personnel were working closely with other competencies to protect CPI through anti-tamper and CPI protection contract clauses. Specific attention and support is being provided to the Science and Technology office in order to build program protection plans into small business and rapid development contracts.

Office of the Air Force Inspector General

During the Office of the Air Force IG's inspection, two unit PMs did not seek milestone decision authority or commensurate execution authority approval in writing affirming that a program protection plan was not required due to the absence of CPI associated with their program's technologies. A system PM did develop and implement a program protection plan with cooperation from staff elements (i.e., security, foreign disclosure, counterintelligence, intelligence, modification managers, systems engineering, test and evaluation, technical staff and others) external to the program. As a result, one unit has accomplished a program protection plan waiver to document "No CPI" determinations and the other is developing a program protection plan waiver to document its "No CPI" determination.

Missile Defense Agency

MDA's internal audit of their CPI/program protection plan procedures determined they were appropriate and complied with both DoD and MDA policies to prevent the unauthorized disclosure of critical information. MDA limited the scope to the first phase of the program protection process—the CPI assessment phase—since only one MDA program had initiated the new process and had not begun the other phase. MDA determined the control and oversight for the CPI Assessment phase was adequate to protect CPI within MDA and horizontally across DoD and comply with applicable DoD and MDA guidance and instructions.

MDA's Research, Development and Acquisition Security Directorate recognized the need for CPI reassessments and proactively prioritized needed program protection plan assessments. Based on reviews for currency and appropriate approvals, MDA identified three of seven program protection plans were not completed and approved - two are already undergoing a reassessment review and the third, MDA is seeking the appropriate disposition.

3. Training and Education to Protect Critical Program Information, Critical Functionality, and Critical Components

This issue area was assessed to determine whether published guidance for training to identify and protect CPI is relevant and adhered to by program, intelligence, counterintelligence, and security personnel.

DoD Office of Inspector General

We determined that training and education for the protection of CPI was not tailored to the specific roles that are involved in RDA protection. While the amount of experience varied, the majority of the personnel interviewed about Air Force and the ACAT ID 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.

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. Training did not entail a review of the program protection process, including CPI assessment and the generation of the technology and protection plans. The Joint Counterintelligence Training Academy offers counter-intelligence support to RDA protection training and provides advanced counter-intelligence 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.

In April 2011, the Defense Security Service created an "Introduction to Critical Program Information" course, an introductory, web-based course for DoD or Defense Industrial personnel working on programs which may contain CPI. The training covers the purpose and identification process of CPI, including an explanation of how CPI identification and required continuous security protection procedures fit into the Defense acquisition life cycle. The course provides policy guidance, steps taken to identify CPI (threat assessment, vulnerabilities, risk management), required procedures to support CPI, and a review of the program protection plan and countermeasure requirements.

There was no tailored CPI protection training. In fact, intelligence and security-related training for the protection of CPI is inconsistent. Training tailored to participants' roles needs to be developed and made available by the organization most able to deliver it effectively and efficiently. Research, development, and acquisition program support organizations, the Defense Acquisition University, and the Defense Security Service should be considered as delivery mechanisms for training.

We recommended that the USD(AT&L), in collaboration with the USD(I), and the DoD Chief Information Officer develop standardized guidance for training in CPI protection for use by the RDA protection community; to which they concurred.

Office of the Army Inspector General

Operations Security (OPSEC) training was occurring in all facilities inspected, however, employee knowledge of Essential Elements of Friendly Information could be better. Most facilities had their Essential Elements of Friendly Information posted in common areas and also in office cubicles, so knowledge improved over previous years. All OPSEC Officers inspected had attended required training classes.

Office of the Naval Inspector General

Many CPI protection countermeasures identified in the DoD IG guidelines are beyond the skill set of security specialist inspectors and reflect a requirement for acquisition manager expertise to credibly inspect.

Overall, the programs inspected are properly staffed and the personnel are adequately trained. The security programs are robust, required training is conducted during New Employee Orientation, internal training resources are highlighted, and security awareness bulletins are posted on the SharePoint portal on a periodic basis. An internal OPSEC training module is provided that satisfies annual training requirements, and gives guidance on OPSEC policies and practices, including social media awareness.

One item worth mentioning is the user-friendly and helpful Space and Naval Warfare Systems Command Web 2.0, which is the internal web page that includes security blogs, educational wikis, and, other information, the latest in CPI policy and strategy. Also, it provides personnel with automated tools to complete various levels of security education requirements and its OPSEC Observer is an excellent initial reference resource for CPI and export controls.

Office of the Air Force Inspector General

In the area of training and education to protect CPI, three units failed to implement specific training programs. Therefore, personnel were not informed on the efforts, procedures and methods of protection. Development of a training plan was recommended.

Missile Defense Agency

MDA's Research, Development and Acquisition Security Directorate developed helpful and creative CPI training for MDA programs going through Phase 1-- CPI Assessment. The Directorate plans to provide additional training when programs get to the next phase of the CPI process. The Directorate also provided a virtual toolbox to further educate and train responsible personnel in the identification and protection of CPI.

4. Use of Resources/Billets to Protect Critical Program Information, Critical Functionality, and Critical Components

This issue area was assessed to determine whether program, intelligence, counter-intelligence, and security personnel assigned to protect CPI are appropriately used.

The Air Force ACAT ID program did not have embedded program security support. The program received security support from a Wing, which in addition to the ACAT ID program supported at least 14 other programs.

The program management office did not track all security costs. The draft program protection plan included estimated costs for program protection in the following categories: Systems Security Engineering, Information Security Program Management, and Security Management/Oversight. However, the program protection plan stated, "program protection costs associated with these categories are predominantly embedded costs as no program protection-specific work breakdown structures were established at contract award." Further, costs related to Systems Security Engineering, to include program personnel, are considered embedded costs and these costs cannot be easily identified or captured for estimating purposes.

Interviews of Air Force Office of Special Investigations (AFOSI) personnel noted a level of uncertainty about who has access to the CPI, as well as the method and timing for when they should be notified of such access. The interviews also noted uncertainty regarding processes for identifying the presence of CPI and controlling access to CPI; specifically, who can or should be informed. Additionally, AFOSI production of tailored threat products was being impacted by lack of resources, as well as the level of technical competencies of the analysts. The AFOSI analysts at the Integrated Threat Assessment Cell lacked engineering competencies that would assist in the analysis of science and technology matters. These analyst's backgrounds were primarily in the counterintelligence arena. Also, wartime levies on AFOSI personnel stretched thin the numbers of agents and their levels of RDA protection experience.

The DSS is responsible for approximately 13,000 cleared facilities. According to the DSS, there is a sizable deficit of industrial security representatives to cover cleared facilities as well as counterintelligence personnel to provide support to the protection of CPI in cleared companies. On January 15, 2009, the Deputy Secretary of Defense signed a memorandum directing 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.

These resources include 450 civilian 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, the ratio is still approximately 1 counterintelligence agent to 300-400 cleared defense facilities.

The Air Force ACAT ID program did not fully track security costs, nor did they report program protection or security-related expenditures. Tracking and reporting these expenditures assists program management offices with establishing budget projections for security throughout the program's life-cycle and with measuring the return on the security expenditures.

In DoD IG Report No. 10-INTEL-09, "Assessment of Security Within the Department of Defense – Tracking and Measuring Security Costs," August 6, 2010, we recommended a comprehensive and integrated security framework to facilitate tracking security costs, more accurately programming future years security budgets, and examining the return on investment for security expenditures, to which management concurred and draft DoD Directive 5200.LL, "Management of the Defense Security Enterprise," is expected to be signed by the Deputy Secretary of Defense in third quarter 2012.

Also, the newly created Defense Security Enterprise Executive Committee, which was created by the draft directive, was established and held its inaugural meeting on January 12, 2012. At that meeting security costs were discussed and the Executive Committee is currently researching additional information and guidance for identifying and tracking security costs. Both the Directive and the and the Defense Security Enterprise Executive Committee will begin the process of establishing a comprehensive and integrated security framework for the Department, to include developing DoD security cost factors to better track security costs, more accurately program future years security budgets, and examine the return on investment for security expenditures.

Office of the Army Inspector General

The Office of the Army IG did not note any significant findings in this area this year.

Office of the Naval Inspector General

The Office of the Naval IG did not note any significant findings in this area.

Office of the Air Force Inspector General

The Office of the Air Force IG did not inspect this area.

Missile Defense Agency

The Missile Defense Agency's auditors did not note any significant findings in this area.

5. Security, Intelligence, and Counterintelligence Support to Protect Critical Program Information, Critical Functionality, and Critical Components

This issue area was assessed to determine whether published guidance to enable counterintelligence, intelligence, and security personnel and programs to support the protection of CPI is relevant and adhered to by program, intelligence, counterintelligence, and security personnel.

DoD Office of Inspector General

The Air Force ACAT ID program staff did request and were provided requisite counterintelligence and intelligence support and threat-related data. However, because threat data was neither timely nor tailored to the CPI, it adversely affected the PM's ability to formulate and implement an effective program protection plan. Moreover, while counterintelligence personnel were known to program staff, DSS personnel were not. As a result, the DSS was not informed of the existence of CPI, nor was a program office point of contact for reporting violations annotated on the DD Form 254.

Counterintelligence support personnel were known to program management office personnel, participated in the CPI identification process, and prepared a counterintelligence support plan. The counterintelligence support plan contained sufficient detail for program management office personnel to understand the support that they could expect to receive from counterintelligence support personnel. Additionally, in accordance with the counterintelligence support plan, an integrated threat assessment was requested from AFOSI's Integrated Threat Assessment Cell. Program protection oversight personnel expressed concern that intelligence and counterintelligence threat products were not timely, thereby adversely impacting the PM's ability to formulate and implement an effective program protection plan once CPI was identified.

DoD and Air Force policies require the PM to immediately develop a program protection plan. The program protection plan guides the development of enhanced controls and establishes cost effective countermeasures for the protection of CPI based on the existing threat. Intelligence and counterintelligence threat products inform the formulation of program protection plans and allow the PM to make informed, objective, risk-based decisions resulting in the most cost-effective countermeasures for the protection of CPI. The production of threat products may take up to 180 days or more from the time CPI is identified. However, DoD Manual 5200.1-M, paragraph C2.4.2 states that the DoD goal for the return of a complete multidisciplinary counterintelligence threat assessment is 120 days from receipt of the request. Moreover, paragraph C2.4.3 states that to facilitate the preparation of an initial draft program protection plan, a summarized collection threat assessment should be provided to the program within 30 days of the request.

Threat products were taking in excess of 180 days from when they initiated their production process to the development of their integrated threat assessment product. The integrated threat assessment was an alternative to the DoD Manual 5000.1-M mandated multidisciplinary counterintelligence threat assessment, which is required to be a CPI-centric tailored threat assessment. The integrated threat assessments that were reviewed were not CPI-focused tailored threat assessments; nor did program officials believe the product was particularly useful.

The System Threat Assessment Report is a DoD 5000 series mandated intelligence product that must be reviewed by the Milestone Decision Authority at milestones B and C. The System Threat Assessment Report describes the future operational threat environment, the system-specific threat, and any reactive threats that could affect program decisions. The System Threat Assessment Report also addresses CPI in the subject weapons platform, but from a perspective of the threat at the time of fielding and in the battlespace. In response to the request from the program and in an attempt to deliver a more timely and relevant System Threat Assessment Report, the National Air and Space Intelligence Center recently used an innovative approach called the Virtual System Threat Assessment Report to produce a responsive intelligence product. The program's System Threat Assessment Report evolved from a series of Virtual System Threat Assessment Reports, a new methodology for building threat assessments for Air Force and Air Force-led force modernization programs.

The Virtual System Threat Assessment Report supplements the traditional paper System Threat Assessment Report with a modular, online product that is more up-to-date, easier to maintain, and more efficient to produce. The Virtual System Threat Assessment Report significantly expands the use of hyperlinks to provide the user with direct access to Intelligence Community reporting and databases for details on specific threat systems. Although the threat annexes in Appendix B of the System Threat Assessment Report are current, the online version will be continuously updated and provide a more general assessment of the overall threats.

The improved methodology resulted in a better crafted and more focused product for the program. However, as with the integrated threat assessment, program personnel believed the System Threat Assessment Report was not provided in a timely manner. They believed the milestone decision point was too late in the process for the System Threat Assessment Report to effectively inform program decisions; having the impact later may mean re-doing or re-thinking the design. Delayed receipt of the System Threat Assessment Report could have impacted cost, schedule, and performance of the acquisition program resulting in re-programming if the delayed report had revealed intelligence information, unknown at the time the acquisition plan was formulated, which could have negatively impacted systems capabilities.

In accordance with DoD Instruction 5200.39, the DSS 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 DSS will know what areas need enhanced levels of protection.

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 DSS 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 DSS 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.

Specific to the program, there was insufficient communication between the DSS and the prime contractor regarding subcontractors and the requirements established by program office staff for the protection of CPI. While program CPI is unclassified, it resides in a classified facility and the information still requires a greater level of protection than non-critical program information. The DSS was not informed of the existence of program CPI. It was not indicated in the DD Form 254, and there was no communication between the DSS and program office staff. Moreover, there was no place on the DD Form 254 to identify which subcontractors possessed CPI. If the program's DD Form 254 had specified the existence of unclassified CPI and the requisite protection measures, the DSS 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, DSS could have assisted in efforts to safeguard CPI by reviewing the levels of CPI protection during the course of regular inspections of the cleared defense facility.

Office of the Army Inspector General

The Office of the Army IG noted that counterintelligence support, provided by elements of the 902nd Military Intelligence Brigade, is being stretched thin due to deployments and a high operational tempo for 902nd counterintelligence agents. The inspected facilities all reported that they received outstanding support from the 902nd Military Intelligence Brigade, but their supporting office was short-handed due to deployments and support was more "on-call" than in previous years.

Office of the Naval Inspector General

At one headquarters, there is dedicated and sufficient counterintelligence support consisting of four Naval Criminal Investigative Service (NCIS) agents providing full-time, on-site presence. Counterintelligence support to program protection planning, foreign collection threats and awareness briefs is adequate. Counterintelligence analytical support is provided through reach-back to subject matter experts at NCIS headquarters. However, given the nature of research and development, along with the known threat and exploitation efforts of any number of Foreign Intelligence Services, on-site agents are encouraged to conduct a more aggressive out-reach effort in order to foster closer working relationships with the intelligence, counterintelligence, and law enforcement communities.

It was noted during inspections of other organizations that highly successful security programs are often enhanced by close, cooperative, and effective working relationships between individuals, and a sound policy. Where a counterintelligence support plan is in place, the NCIS provides substantive counterintelligence support through a dedicated NCIS agent presence. For FY 2012, NCIS has adopted a new support concept that focuses on known threats against specific technologies. By concentrating on specific critical technologies facing known intelligence threats, NCIS hopes to optimize its investment in supporting security and counterintelligence efforts.

Office of the Air Force Inspector General

Five of six PMs did not adequately use the counterintelligence threat assessment with system-specific CPI and vulnerabilities to develop appropriate countermeasures. PMs lacked knowledge of system specific CPI and were unfamiliar with their counterintelligence threat assessments. As a result, it was recommended that PMs and the system security working group use integrated threat assessments provided by AFOSI to develop appropriate countermeasures and provide documentation for program protection planning and system security working group minutes at all meetings. PMs will also include support contractors in program protection efforts.

Missile Defense Agency

MDA auditors found that counterintelligence personnel were involved early in the CPI assessment phase, participating in the integrated product teams.

6. Foreign Visits Program

This issue area was assessed to determine whether published guidance for foreign visits is relevant and adhered to by program, intelligence, counterintelligence, and security personnel.

DoD Office of Inspector General

As part of our assessment to determine whether published guidance for foreign visits is relevant to and adhered to by program, intelligence, counterintelligence, and security personnel, we also assessed this issue area because in a policy letter, "Accountability of Department of Defense (DoD) Sponsored Foreign Personnel in the United States (U.S.)," May 18, 2004, the Deputy Secretary of Defense requires all IGs to verify compliance with the sponsored foreign personnel policy through their inspection processes.

We also assessed this issue area to ensure that 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.[2] 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.

The Air Force ACAT ID program management office did not have any foreign government or international organization involvement in program development. It was noted, however, that some programs that will be part of the system of systems that the program will support have international aspects.

If a cooperative development arrangement with a foreign government or international organization is contemplated in the future, an international agreement should be negotiated, and the required documents, such as the summary statement of intent and the delegation of disclosure authority letter, will detail the countermeasures necessary to protect U.S. Air Force information and technology under such a program. With regard to any potential of a foreign military sale (including coproduction), the ACAT ID program management office will defer to the Deputy Under Secretary of the Air Force for International Affairs and the Assistant Secretary of the Air Force for Acquisition for the formulation of the Air Force export policy for the program.

Office of the Army Inspector General

The Office of the Army IG found no significant findings in this issue area.

Office of the Naval Inspector General

The Office of the Naval IG found that a more robust database program would no doubt enhance security, but inspections did find evidence that foreign visit request vetting against known program security restrictions is generally effective.

Office of the Air Force Inspector General

The Office of the Air Force IG found that unit PMs did not complete a technology assessment/control plan when foreign participation was authorized. As a result, the unit completed the technology assessment/control plan and expanded the system security working group process to include all stakeholders. A step-by-step checklist was also implemented, to ensure future compliance with technology assessment/control plan requirements prior to initial acquisition board and acquisition strategy panel.

Missile Defense Agency

MDA assessed the International Security, Security & Emergency Management, and Counterintelligence Directorates to assess the procedures for processing foreign national and foreign visitor requests and further, that MDA's control and oversight for foreign nationals and visitors to prohibit unauthorized disclosure of military information complies with applicable DoD and MDA guidance and instructions.

---

[2] 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.

MDA reviewed whether the in-place procedures and associated controls were adequate to prevent the unauthorized disclosure of military information to foreign nationals and visitors. MDA personnel examined the five most recent foreign national and visitor requests. MDA, during their self-assessment found:

- MDA uses the Foreign Visits System - Confirmation Module, to document all visits (walk-in, scheduled, or unscheduled) to MDA facilities. International Security personnel complete Foreign Visitor Data Sheets for each foreign national or foreign visitor seeking access to MDA facilities and all data collected is entered into the Foreign Visits System - Confirmation Module. MDA Security Operations Center PM is responsible for updating the Foreign Visits System - Confirmation Module and filling in all required fields.
- Foreign nationals and visitors do not have access to information systems at MDA.
- Foreign nationals and visitors are required to wear yellow badges indicating their foreign visitor status, even if they are accredited and assigned as a foreign liaison officer. They must present picture identification and current passport number for access into MDA facilities. Request for foreign national visits are coordinated by international security personnel and front desk security personnel at facilities to be visited.
- ~~(FOUO)~~ Incoming foreign national and visitor requests are also coordinated by international security personnel with the Counterintelligence Directorate. Counterintelligence personnel check all available data on visitors and determine the threat level for the visit. The assigned threat level determines the visitor's access to MDA facilities and personnel. Should counterintelligence personnel identify a potential threat associated with a visit, additional threat mitigation measures are taken before the visit.
- Counterintelligence personnel routinely provide threat briefings and regular training to MDA employees prior to any foreign national or visitor arrival. In addition, counterintelligence personnel conduct debriefings at the conclusion of each visit.

7. Horizontal Protection of Critical Program Information, Critical Functionality, and Critical Components

This issue area was assessed to determine whether published guidance for horizontal protection is relevant and adhered to by program, security, intelligence, and counterintelligence personnel. We assessed the 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 Office of the Inspector General

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.

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.

The Acquisition Security Database, a horizontal protection database, provides the RDA community with greater access to CPI. Use of a single 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 a single 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.

Air Force Pamphlet 63-1701, requires the System Security Working Group make horizontal protection determinations for identified CPI, but there is no policy or standard process for review of databases to accomplish this objective. Program officials stated that horizontal protection was considered and the Acquisition Security Database was consulted during the conduct of the System Security Working Group. However, the Air Force had developed its own horizontal protection database. Recent guidance provides a way ahead for the Air Force to use the Acquisition Security Database exclusively for horizontal protection purposes. This will ensure consistent application of horizontal protection across services and acquisition programs.

Office of the Army Inspector General

The Office of the Army IG found no significant findings in this area.

Office of the Naval Inspector General

The Office of the Naval IG found that there is no clear cohesive horizontal protection strategy of CPI across the Navy at this time; however, the Deputy Assistant to the Secretary of the Navy for Research, Development, Test and Evaluation plans to implement the USD (AT&L) memorandum, "Document Streamlining – Program Protection Plan," July 18, 2011, and Directive-Type Memorandum 09-016 – "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems," March 25, 2010. Therefore, the Department of the Navy now requires ACAT ID, IAM and Special Interest programs to follow the July 18, 2011, memorandum. ACAT IC, ACAT II thru ACAT IV, and Abbreviated Acquisition Programs will tailor the memo to their program. This new approach to program protection plan expands the existing DoD IG guidance criteria and recognizes program protection as the Navy's holistic approach for delivering trusted systems. The priority for memo implementation will be ACAT ID programs as the Navy conducts a phased approach to Navy Enterprise implementation of the memo.

Office of the Air Force Inspector General

The Office of the Army IG did not inspect this area of the guidelines.

Missile Defense Agency

MDA reviewed programs with CPI to determine whether they developed a program protection plan and sampled three to determine whether CPI information was recorded and tracked into the DoD Acquisition Security Database, for horizontal protection: MDA reviewed program protection plans for seven MDA programs to determine whether they were current and appropriately approved. Four of the seven programs had a completed and appropriately approved program protection plan. Three of the seven programs did not have a completed and appropriately approved program protection plan. The information on CPI from the three sampled programs matched the information in the Acquisition Security Database. CPI in the program protection plans and the Acquisition Security Database matched for the three sampled programs because actions of MDA's Research, Development and Acquisition Security Directorate horizontally protected CPI by appropriately recording it in the Acquisition Security Database.

8. Policies to Protect Critical Program Information, Critical Functionality, and Critical Components

This issue area was assessed to determine whether published guidance for the identification and protection of CPI is relevant and adhered to by program, intelligence, counterintelligence, and security personnel.

DoD Office of the Inspector General

We primarily assessed RDA protection efforts using DoD Instruction 5200.39; however, there are many issuances on related areas, and from multiple agencies that address RDA protection.

Air Force policies do not focus on total integration of security, intelligence, and counterintelligence throughout a program's lifecycle. It was noted that Air Force policies on program protection, namely Air Force Policy Directive 63-17 and Air Force Pamphlet 63-1701, reference out-of-date DoD policy and were developed prior to the Air Force's establishment of its Integrated Lifecycle Management Enterprise policies. Consequently, the primary Air Force policies focused on the protection of CPI are not consistent with Air Force Instruction 63-101, and can cause confusion in terms of Air Force policy definitions relative to CPI.

The program office has yet to negotiate and agree on specific protections to be implemented for the sites hosting CPI. DoD Instruction 5200.39 guidance on this subject has yet to be promulgated. Enclosure 2, paragraph 4.b. of DoD Instruction 5200.39 tasks the DoD Chief Information Officer to "identify minimum security requirements for contractor owned and operated information systems for the protection of CPI." Directive-Type Memorandum 08-027, "Security of Unclassified DoD Information on Non-DoD Information Systems," July 31, 2009, addresses security requirements for contractors processing DoD information on non-DoD information systems and may provide a model for this, but it does not address the protection of CPI specifically.

Office of the Army Inspector General

The Office of the Army IG did not inspect this area of the guidelines.

Office of the Naval Inspector General

The Office of the Naval IG found that the full implementation of the new USD (AT&L) policies would make great strides towards delivering trusted systems to the warfighting community. However, that implementation will require application of new skills and some revision to the Navy's current "command inspection" approach to research and technology protection.

Office of the Air Force Inspector General

The Office of the Air Force IG inspected this area and found no deficiencies in this area.

Missile Defense Agency

MDA reviewed the CPI/program protection plan guidance to determine if there was standardized and approved MDA guidance that was in accordance with DoD Instruction 5200.39. MDA has approved guidance on CPI/program protection planning with their MDA Instruction, 5200.08-INS, "Critical Program Information (CPI) Protection Within the Missile Defense Agency," August 1, 2011. The Director, MDA approved MDA Instruction, 5200.08-INS. The MDA Instruction is in accordance with DoD guidance, and like the DoD Instruction, it directs the early identification of CPI and appropriate protection throughout the system life cycle.

The MDA's Research, Development and Acquisition Security Directorate developed a standardized and repeatable process providing additional guidance and describing detailed procedures for performing specific protection tasks in a draft CPI Protection Manual, "Procedures for CPI Protection Within the Missile Defense Agency." The Directorate is instructing programs with CPI to follow the manual as standard operating procedures.

Appendix A. Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING
BETWEEN
DEPUTY UNDER SECRETARY OF DEFENSE FOR LABORATORIES AND BASIC SCIENCES
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL, DEPARTMENT OF THE ARMY
NAVAL INSPECTOR GENERAL
INSPECTOR GENERAL, DEPARTMENT OF THE AIR FORCE
DIRECTOR, INTERNAL ASSESSMENTS,
BALLISTIC MISSILE DEFENSE ORGANIZATION
ON
SECURITY, TECHNOLOGY PROTECTION, AND COUNTERINTELLIGENCE INSPECTIONS

A. REFERENCES

1. Deputy Secretary of Defense memorandum, subject: Inspection of Security and Counterintelligence Practices at Laboratories and Centers, February 17, 2000.

2. Office of the Inspector General, DoD, Security and Counterintelligence Inspection Guidelines, September 5, 2001.

B. PURPOSE

The purpose of this memorandum of understanding (MOU) is to establish a uniform system of periodic inspections of security, technology protection, and counterintelligence practices at DoD research, development, test, and evaluation (RDT&E) facilities as requested in Reference 1.

C. DEFINITIONS

1. "Participating Inspectors General" are defined under this MOU as the Inspector General of the Department of Defense, the Inspector General of the Army, the Naval Inspector General, the Inspector General of the Air Force, and the Director, Internal Assessments, Ballistic Missile Defense Organization.

2. A DoD organizational entity is considered to be an "RDT&E facility" when it is owned and operated by the Government and conducts activities devoted to research, advanced technology development, demonstration/validation, engineering and manufacturing development, systems or operational support, testing and evaluation, or some combination thereof.

3. Inspections conducted under this MOU may include reviews, evaluations, or similar oversight projects.

4. "Significant Findings" are security, technology protection, or counterintelligence deficiencies that may damage U.S. national security and/or require:

a. money to correct or investigate;

b. the development of new policy or procedures to resolve; or

c. the involvement of the Office of the Secretary of Defense or two or more DoD Components to resolve.

D. SCOPE

1. This MOU covers inspections of security, technology protection, and counterintelligence activities at DoD RDT&E facilities conducted by or at the direction of the participating Inspectors General.

2. RDT&E facilities that may be inspected under this MOU.

a. The participating Inspectors General will prepare and forward to the Office of the Inspector General, DoD,[1] lists of the RDT&E facilities in their organizations that may be inspected under this MOU.

b. The Office of the Inspector General, DoD, will consolidate and distribute the lists to the participating Inspectors General, the Deputy Under Secretary of Defense for Laboratories and Basic Sciences and the Director of Operational Test and Evaluation.

c. The Deputy Under Secretary of Defense for Laboratories and Basic Sciences and the Director of Operational Test and Evaluation, may recommend additional Defense agency facilities that should be inspected under this MOU.

E. UNIFORM SYSTEM OF INSPECTIONS

1. Participating Inspectors General will inspect or direct the inspection of the RDT&E facilities of their respective organizations.

2. The inspections conducted under this MOU will be performed during the course of the programs of the participating Inspectors General, to include, in the case of military Inspectors General, the programs of their subordinate Inspectors General.

3. By June of each year, the participating Inspectors General will prepare and forward to the Office of the Inspector General, DoD, lists of the facilities that will be inspected under this MOU in the following fiscal year. The Office of the Inspector General, DoD, will consolidate and distribute the lists to the participating Inspectors General.

4. The Office of the Inspector General, DoD, in coordination with Defense Agency Inspectors General, will ensure that RDT&E facilities not under Military Department control are inspected.

5. Reference 2 will serve as guidance for the conduct of inspections under this MOU. Participating Inspectors General may modify or customize the guidelines in Reference 2 to account for Department-specific approaches to security, technology protection, and counterintelligence.

6. To ensure uniformity and consistency of inspections, the participating Inspectors General will coordinate with the Office of the Inspector General, DoD, modifications or customizations of the guidelines in Reference 2.

---

[1] The Office of Intelligence Review is the Office of Primary Responsibility within the Office of the Inspector General, DoD, for matters relating to this MOU.

7. The participating Inspectors General conducting or directing inspections under this MOU will use their own procedures to ensure that inspection findings and recommendations are addressed and implemented.

F. REPORTING INSPECTION RESULTS

1. The participating Inspectors General will use their own procedures to write findings and recommendations within their respective areas of responsibility.

2. The participating Inspectors General will prepare and forward to the Office of the Inspector General, DoD, any significant findings and recommendations upon the conclusion of each inspection. The Office of the Inspector General, DoD, will distribute significant findings as appropriate.

3. By December 31 each year, participating Inspectors General who performed or directed the performance of an inspection under this MOU during the previous fiscal year will send to the Office of the Inspector General, DoD, the status of recommendations reported in the previous year's overarching report.

4. Each January, the Deputy Under Secretary of Defense for Laboratories and Basic Sciences, as the Chair of the DoD Laboratory Security and Counterintelligence Overarching Integrated Process Team (OIPT), will send to the Office of the Inspector General, DoD, the most recent winners of "Best Practices" Awards for technology protection at DoD RDT&E facilities.

5. Each January, the Office of the Inspector General, DoD, in coordination with the other participating Inspectors General, will develop an overarching report that contains five parts:

a. Cover memorandum

b. Summary of new findings and recommendations (maximum one paragraph per item)

c. Status of recommendations previously reported

d. Details of new findings and recommendations (text taken verbatim from inspection reports)

e. Winners of Deputy Under Secretary of Defense for Laboratories and Basic Sciences "Best Practices" Awards for technology protection at DoD RDT&E facilities.

6. The Inspector General of the Department of Defense, or a designee, will sign the overarching report and send it to the other participating Inspectors General, the OIPT Chair, and appropriate congressional committees. The congressional committees are:

a. Senate Subcommittee on Defense, Committee on Appropriations;

b. Senate Armed Services Committee;

c. Senate Governmental Affairs Committee;

d. Senate Select Committee on Intelligence;

e. House Subcommittee on Defense, Committee on Appropriations;

f. House Armed Services Committee;

g. House Government Reform Committee; and

h. House Permanent Select Committee on Intelligence.

7. The OIPT Chair will distribute the report to offices having policy and oversight roles in technology protection.

G. REVIEW

1. The signatories will review this MOU two years after it is signed.

2. The participating IGs, in coordination with the OIPT, will review the DoD Inspection Guidelines annually.

H. PARTICIPATION BY ADDITIONAL INSPECTORS GENERAL

Subject to the approval of the Inspector General, DoD, Defense Agency Inspectors General may sign and become participants in this MOU.

Deputy Under Secretary of Defense for Laboratories and Basic Sciences
Date: 25 Apr 02

Director, Operational Test and Evaluation
Department of Defense
Date: 28 JAN 2002

Inspector General
Department of Defense
Date: 5-8-02

Inspector General
Department of the Army
Date: APR 01

Naval Inspector General
Date: 20 DEC 2001

Inspector General
Department of the Air Force
Date: 7 FEB 02

Director, Internal Assessments
Ballistic Missile Defense Organization
Date: 12/18/01

Appendix B. List of Service Facilities Inspected

A. U.S. Army Research, Development, Test and Evaluation Facilities Inspected During FY 2011

1. Night Vision and Electronic Sensors Directorate, Fort Belvoir, VA
2. Space and Missile Defense Technical Center, Space and Missile Defense Command, Redstone Arsenal, AL
3. Aberdeen Test Center, Army Test and Evaluation Center, Aberdeen Proving Grounds, MD
4. Engineer Research and Development Center, U.S. Army Corps of Engineers, Vicksburg, MS
5. Redstone Technical Test Center, Army Test and Evaluation Command, Redstone Arsenal, AL
6. Tank-Automotive Research Development Test and Evaluation Center, Army Materiel Command, Warren, MI

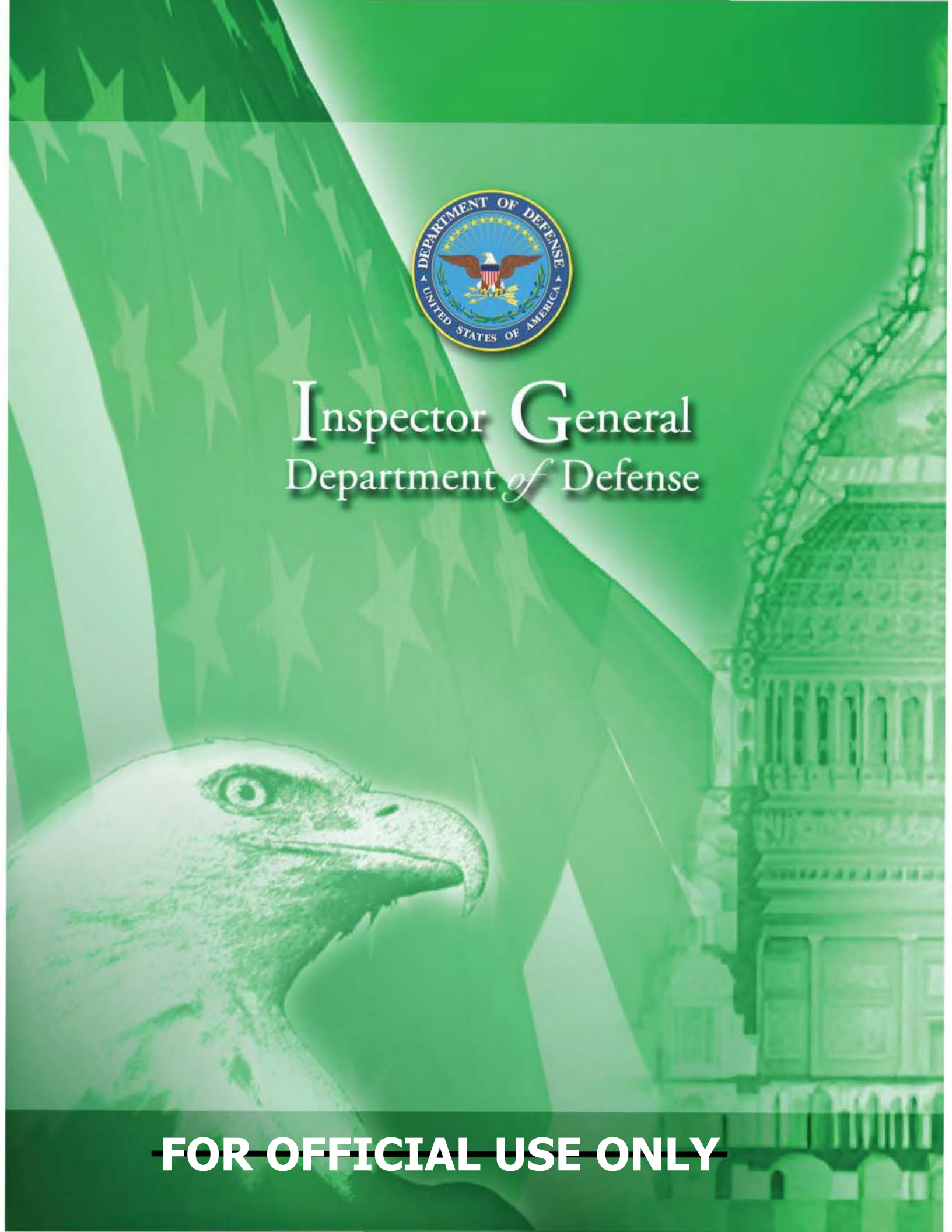
B. Navy Research, Development, Test and Evaluation Facilities Inspected During FY 2011

1. Surface Combat Systems Center, Wallops Island, VA
2. Coastal Systems Station Dahlgren Division, Naval Surface Warfare Center, Panama City, FL
3. Carderock Division, Naval Surface Warfare Center, West Bethesda, MD
4. Naval Ship Systems Engineering Station, Carderock Division, Naval Surface Warfare Center, Philadelphia, PA
5. Naval Surface Warfare Center, Indian Head Division, Indian Head, MD
6. Naval Research Laboratory, Washington, DC

C. Air Force Research, Development, Test and Evaluation Facilities Inspected During FY 2011

1. Air Force Materiel Command, Electronic Systems Center/C2ISR Directorate/Space C2 and Surveillance Division, Peterson Air Force Base, CO
2. Air Force Materiel Command, Aeronautical Systems Center Staff and 88th ABW Program Protection Functions, Wright-Patterson Air Force Base, OH
3. Air Force Materiel Command, Aeronautical Systems Center Agile Combat Support Directorate, Wright-Patterson Air Force Base, OH

4. Air Force Materiel Command, Aeronautical Systems Center Mobility Directorate, Wright-Patterson Air Force Base, OH
5. Air Force Materiel Command, Aeronautical Systems Center Fighters and Bombers Directorate, Wright-Patterson Air Force Base, OH
6. Air Force Materiel Command, Aeronautical Systems Center ISR Directorate, Wright-Patterson Air Force Base, OH
7. Air Force Materiel Command, Oklahoma City Air Logistics Center Staff, Tinker Air Force Base, OK
8. Air Force Materiel Command, Oklahoma City Air Logistics Center/76th Maintenance Wing, Tinker Air Force Base, OK
9. Air Force Materiel Command, Oklahoma City Air Logistics Center/Aircraft Sustainment Directorate, Tinker Air Force Base, OK
10. Air Force Materiel Command, Warner-Robins Air Logistics Center Staff, Warner-Robins Air Force Base, GA
11. Air Force Materiel Command, Warner-Robins Air Logistics Center/402nd Maintenance Wing, Warner-Robins Air Force Base, GA
12. Air Force Materiel Command, Warner-Robins Air Logistics Center/Aircraft Sustainment Directorate, Warner-Robins Air Force Base, GA
13. Air Force Materiel Command, Air Force Office of Scientific Research, Joint Base Andrews/Arlington, VA
14. Air Force Materiel Command, Headquarters Air Force Research Laboratory, Wright-Patterson Air Force Base, OH
15. Air Force Materiel Command, Air Force Research Laboratory, Air Vehicles Directorate, Wright-Patterson Air Force Base, OH
16. Air Force Materiel Command, Air Force Research Laboratory, Materials and Manufacturing Directorate, Wright-Patterson Air Force Base, OH
17. Air Force Materiel Command, Air Force Research Laboratory, Sensors Directorate, Wright-Patterson Air Force Base, OH
18. Air Force Materiel Command, Air Force Research Laboratory, Propulsion Directorate, Wright-Patterson Air Force Base, OH
19. Air Force Materiel Command, Air Force Research Laboratory/Information Directorate, Rome, NY
20. Air Force Materiel Command, AF Global Logistics Support Center/448th Supply Chain Management Wing, Tinker Air Force Base, OK
21. Air Force Materiel Command, AF Global Logistic Support Center, 591st Supply Chain Management Group, Wright-Patterson Air Force Base, OH
22. Air Force Materiel Command, AF Global Logistic Support Center/448th Supply Chain Management Wing/638th Supply Chain Management Group, 404th Supply Chain Management Squadron, 405th Supply Chain Management Squadron, 406th Supply Chain Management Squadron, Robins Air Force Base, GA


Inspector General
Department of Defense
FOR OFFICIAL USE ONLY