10-INTEL-08
August 6, 2010

Inspector General
United States Department of Defense

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

Inspection Guidelines for DoD Security, Intelligence, and Counterintelligence Support to Research, Development, and Acquisition Protection for 2010

FOR OFFICIAL USE ONLY

Additional Information and Copies

For information and to request copies of this report, contact the DoD Office of Inspector General at (703) 604-8841 or (DSN 664-8841).

Suggestions for Assessments

To suggest ideas for, or to request future audits or evaluations, contact the Office of the Deputy Inspector General for Intelligence at (703) 604-8800 (DSN 664-8800) or UNCLASSIFIED fax (703) 604-0045. Ideas and requests can also be mailed to:

ODIG-INTEL (ATTN: Intelligence Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 703)
Arlington, VA 22202-4704

Acronyms and Abbreviations

CPI	Critical Program Information
RDA	Research, Development, and Acquisition

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

August 6, 2010

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Inspection Guidelines for DoD Security, Intelligence, and Counterintelligence Support to Research, Development, and Acquisition Protection for 2010 (Report No. 10-INTEL-08)

We are providing this report of inspection guidelines for information and use. We considered comments on a draft of this report in preparing the final report. We publish these guidelines biennially to ensure a consistent and effective oversight tool, and compliance with DoD policy in order to provide uncompromised and secure military systems to the warfighter. We specifically focus on critical program information protection through the application of counterintelligence, intelligence, security, systems engineering, and other defensive countermeasures to mitigate risk. These guidelines can and should be tailored to account for Component policies and program uniqueness.

We appreciate the courtesies extended to the staff. Please direct questions to [redacted] at (703) 604-[redacted] (DSN 664-[redacted] or [redacted] at (703) 604-[redacted] (DSN 664-[redacted].

Patricia A. Brannin
Deputy Inspector General
for Intelligence

DISTRIBUTION:

OFFICE OF THE SECRETARY OF DEFENSE
- Under Secretary of Defense (Acquisition, Technology, and Logistics)
- Under Secretary of Defense (Policy)
- Under Secretary of Defense (Intelligence)
- Assistant Secretary of Defense (Networks and Information Integration)/ DoD Chief Information Officer
- Deputy Under Secretary of Defense (HUMINT, Counterintelligence and Security)
- Deputy Under Secretary of Defense (Laboratories and Basic Sciences)
- Director, Defense Security Service

DEPARTMENT OF THE ARMY
- Inspector General, Department of the Army
- Auditor General, Department of the Army

DEPARTMENT OF THE NAVY
- Naval Inspector General
- Auditor General, Department of the Navy

DEPARTMENT OF THE AIR FORCE
- Inspector General, Department of the Air Force
- Auditor General, Department of the Air Force

NON-DEFENSE ORGANIZATIONS
- Office of Management and Budget

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

Introduction

Purpose of the Guidelines

This report updates the 2008 inspection guidelines that improve DoD-wide consistency in inspections of security, intelligence, and counterintelligence practices at research, development, test, and evaluation facilities and the acquisition processes that impact the identification of and protection of critical program information (CPI). The DoD Inspectors General and officials responsible for providing oversight to research, development, test, and evaluation facilities should use the guidelines to assess how DoD implements policy and guidance for the protection of research, development, and acquisition (RDA) activities or programs, and how well security requirements are implemented, and intelligence and counterintelligence support are integrated into the RDA effort.

Background

Inspectors General annually inspect the security, intelligence, and counterintelligence practices at RDA activities or programs. The DoD Office of Inspector General,[1] who summarizes the significant findings and recommendations identified by the inspections. Effective and current policies are the cornerstone of oversight efforts. Assessing CPI protection efforts has been enhanced with the publication of DoD Instruction 5200.39; however, many issuances, covering many subject areas, and coming from many agencies also enhance program protection oversight efforts.

Areas for Inspections

These guidelines are developed to provide consistency across the Department when assessing security, intelligence, and counterintelligence support to RDA protection efforts aimed at protecting CPI. The format of this report has changed from the 2008 report by focusing on eight key areas that assist in determining the effectiveness to protect CPI. The areas and related questions for inspections to address are:

1. CPI identification;
2. development of a program protection plan;
3. training and education to protect CPI;
4. use of resources/billets to protect CPI;
5. security, intelligence, and counterintelligence support to CPI;
6. foreign visit program;
7. application of horizontal protection to protect CPI; and
8. policies to protect CPI.

[1] The Office of the Deputy Inspector General for Intelligence is the Office of Primary Responsibility within the DoD Office of Inspector General for matters relating to inspections of counterintelligence, security, and RDA protection practices at research, development, test, and evaluation facilities.

1. Critical Program Information (CPI) Identification

Is CPI being determined within programs or facilities (whether inherent to or inherited by a program)? Is there an understanding of what CPI is by personnel tasked to identify and protect CPI in accordance with DoD Instruction 5200.39, Paragraph 4d and Enclosure 2, Paragraph 6d?

Has the RDA program manager established a working group comprised of subject matter experts in technology and system engineering to evaluate the information, technology, and components to determine if CPI exists? If so, has a consistent process to select CPI as early in the research and engineering or acquisition process as feasible been implemented in accordance with DoD Instruction 5200.39, Paragraph 4d and Enclosure 2, Paragraph 6c, d, and q?

Is there a standardized and approved process to identify CPI at facilities or within acquisition programs? Is that process being utilized in accordance with DoD Instruction 5200.39, Paragraph 4d and Enclosure 2, Paragraphs 6c and d?

Is there training or education on the identification of CPI in the facility or acquisition program in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6i (Some providers would include the Defense Acquisition University, the Joint Counterintelligence Training Academy, and the Defense Security Service)?

Is the identification of CPI occurring at each milestone in accordance with DoD Instruction 5200.39, Paragraph 4d and DoD Instruction 5000.02, Enclosure 4, Table 3?

Was the presence of CPI at contractor, to include sub-contractor, locations identified and addressed in accordance with DoD Instruction 5200.39, Paragraphs 2b and 4h, and Enclosure 2, Paragraphs 6p and t?

Were members of the Component anti-tamper community engaged in determining if any elements of CPI were suitable for anti-tamper, were the anti-tamper requirements delineated in the design phase of a critical component, and identified as a funding requirement in the RDA program or activity in accordance with in accordance with DoD Instruction 5200.39, Paragraph 4b and Enclosure 2, Paragraphs 6c and 10?

Is the cognizant RDA program manager informing the milestone decision authority that the process to identify CPI resulted in a no CPI decision? How is the milestone decision authority informed, in writing or another manner in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6n?

Did the CPI identification process include identification of components that are critical themselves or provide access to critical system functions to include commercial off-the-shelf technology? If so, was a supply chain risk assessment conducted to identify and mitigate for supply chain risk (e.g., criticality analysis) in accordance with DoD Instruction 5200.39, Paragraph 4g and Enclosure 2, Paragraph 6u?

Were all items (information, technology, or components) considered for CPI documented along with a rationale for inclusion or exclusion from?

Were threat assessment products (i.e., System Threat Assessments, Foreign Intelligence Service threat assessments, or other products generated by counterintelligence) that are less than 2 years old, used to inform the CPI identification process?

Did the CPI identification process include the re-assessment of the full system for CPI even if the program is just a block update or incremental upgrade to an existing system?

2. Program Protection Planning

If CPI is present (whether inherent or inherited), is there a program protection plan in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 4b, 4e, and 6e?

Is there sufficient training to identify the components that comprise a program protection plan in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6i and DoD Manual 5200.1, Paragraph C.2.9?

Is the program protection plan reviewed and updated to reflect technology changes in the acquisition program in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 4e and 6e?

Have DoD information systems storing, processing, or transmitting CPI been assigned a Mission Assurance Category and a Confidentiality Level based on the mission impact and sensitivity of the information processed, in accordance with DoD Instruction 8500.2, Enclosure 4, Paragraph E4.1.9.? Are information assurance controls applicable to the assigned Mission Assurance Category and Confidentiality Level in place for DoD information systems storing, processing, or transmitting CPI, in accordance with DoD Instruction 8500.2, Enclosure 4 and its attachments?

Is there an operations security plan for the protection of resident CPI? Is it attached as an annex to the program protection plan and is it reviewed annually in accordance with Defense Acquisition Guidebook, Paragraph 8.4.6.6.?

Are procedures in place for releasing and transmitting controlled unclassified information, such as information subject to export controls, in accordance with DoD Regulation 5200.1, Appendix 3, Directive Type Memorandum 04-010, and DoD Directive 5230.20, Paragraph 4.10.?

Once CPI has been identified in an RDA program, has the cognizant program manager established a working group to determine cost effective measures to protect CPI that includes subject matter experts from security, counterintelligence, foreign disclosure, information assurance, and others (i.e., anti-tamper or international programs) as deemed necessary to aid in constructing a viable program protection plan in accordance with DoD Instruction 5200.39, Paragraph 4a and Enclosure 2, Paragraphs 6c, f, and q; and Defense Acquisition Guidebook, Chapter 8, Paragraphs 8.4.2. and 8.4.6.?

Is the anti-tamper community engaged in the acquisition process to determine if anti-tamper requirements are necessary to be incorporated in the design of a critical component or system when CPI is determined to be present (inherent to or inherited by a system) in accordance with DoD Instruction 5200.39, Paragraph 4b?

Is security, intelligence, and counterintelligence support requested and provided adequate to support the implementation of the program protection plan in accordance with in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6c?

Does the program protection plan identify all locations (DoD owned or operated, cleared defense contractors, and when known, sub-contractors) where CPI is anticipated or known to exist and has this information been shared with the Defense Security Service and the supporting Defense counterintelligence Component in accordance with DoD Instruction 5200.39, Paragraph 4d and Enclosure 2, Paragraphs 6t and 8?

Does the technology development strategy address candidate CPI and potential countermeasures in accordance with DoD Instruction 5200.39, Paragraph 4d?

Is the PPP for an RDA program with CPI reviewed at each major phase of a research and engineering activity, prior to a major milestone in the acquisition process, prior to fielding, and/or as CPI evolves or adapts due to changes in the operational environment or foreign collection threat picture in accordance with DoD Instruction 5200.39, Paragraph 4d and Defense Acquisition Guidebook, Chapter 8, Paragraph 8.4.11.2?

Is there evidence that the countermeasures in the program protection plan are implemented, and has the RDA program manager instituted a process to randomly test the countermeasures for effectiveness, risk mitigation, and consistent, life-cycle protection feasibility in accordance with DoD Instruction 5200.39, Paragraph 4a?

Has the prime contractor or other appropriate contractor provided the cognizant RDA program manager with a plan (known as a program protection implementation plan) that illustrates how the contractor will employ the protection requirements outlined in the program protection plan at facilities under their control and at sub-contractors when applicable in accordance with Defense Acquisition Guidebook, Paragraph 8.4.10.1 and 8.4.11.1?

Does the acquisition strategy summarize program protection planning status in accordance with DoD Instruction 5200.39, Paragraph 4d?

Was the horizontal protection database consulted during the identification of CPI in accordance with DoD Instruction 5200.39, Paragraph 4c and Enclosure 2, Paragraph 6g?

Does the contract include clauses that address identification of CPI, program protection, flow down of these clauses to subcontractors, inclusion of program protection in the requirements and verification of program protection requirements at each of the systems engineering technical reviews in accordance with DoD Instruction 5200.39, Paragraph 4h?

Is a configuration management process in place that controls access to all software code and hardware components throughout the system lifecycle?

3. Training and Education to Protect Critical Program Information

Does the training include implementation of applicable security requirements, and the role of counterintelligence in supporting protection of CPI in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 1d and 6i?

Are RDA program personnel trained in requirements for international program security, technology transfer, security classification guidance for classified and controlled unclassified information, applicable export-control regulations, and procedures for control of foreign visits and assignments of foreign nationals in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 1d and 6i?

Is training available on CPI identification, program protection planning, anti-tamper requirements, the role of security, intelligence, and counterintelligence in supporting acquisition programs, international program security requirements, technology transfer programs, identifying, marking and disseminating controlled unclassified information, and export control regulations in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 6i and 10e? If not, why not?

Is information assurance awareness training provided to all personnel with access to DoD information systems, in accordance with DoD Instruction 8500.2, Section 5.7.7.?

Has the unit/program/activity identified personnel with access to CPI to the servicing security/counterintelligence office to receive awareness briefings prior to foreign travel in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6m and DoD Instruction 5240.6, Paragraph 6.4.1.?

4. Use of Resources/Billets to Protect Critical Program Information

Have RDA programs identified the need for additional resources to execute program protection requirements, and requested funding to attain and sustain these resources in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6b?

Are the responsibilities associated with the security of CPI and attendant requirements for program protection clearly articulated by the cognizant RDA program manager, and is this function adequately staffed in RDA programs with CPI in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6c?

Does the organization holding CPI in electronic form have an assigned Designated Accrediting Authority for its information systems, in accordance with DoD Directive 8500.01E, Paragraphs 4.14.3 and 4.25?

Are countermeasure costs to protect CPI included in program budgets in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6b and Defense Acquisition Guidebook, Chapter 8, Paragraph 8.4.10?

Are program budgets for security measures adequate to meet all baseline requirements to protect CPI in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6b and Defense Acquisition Guidebook, Chapter 8, Paragraph 8.4.10?

Do personnel tasked with RDA protection processes have adequate staff, in size, rank/grade, and position within the organization to implement processes to protect CPI in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6c and Defense Acquisition Guidebook, Chapter 6, Paragraph 6.3.2.?

Is the counterintelligence specialist performing duties (excluding deployments) not related to counterintelligence support to the facility or site?

Is the counterintelligence specialist performing duties (excluding deployments) not related to counterintelligence support to the facility or site in accordance with?

Are program protection personnel imbedded in the program or is program protection support provided only from a higher command level? What is the impact?

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

Have counterintelligence personnel been trained or educated in supporting research, development, test, and evaluation facilities or sites in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6i?

Is the supporting Defense counterintelligence Component providing foreign collection threat information to RDA programs and assisting RDA programs obtain foreign intelligence analysis of foreign requirements for program related critical technology to include CPI in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 6l, 6s, and 7c?

What analytical products, intelligence reporting, or other intelligence-related products have been provided?

Has the RDA program manager requested counterintelligence analysis of CPI and has a counterintelligence analytical product that incorporates foreign intelligence requirements (e.g., a technology targeting risk assessment) for CPI been integrated into or produced in conjunction with the counterintelligence product by a Defense Intelligence Component in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 1g and 6k?

Has the supporting Defense counterintelligence Component provided a subject matter expert to assist the Component Acquisition Executive with protecting CPI in Component RDA programs in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6c?

Has the supporting Defense counterintelligence Component identified a counterintelligence point-of-contact for RDA programs with CPI and is this person available to assist the program manager as needed in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 1f and 6t?

Do the contractor and/or subcontractor report to the Defense Cyber Crime Center's DoD-Defense Industrial Base Collaborative Information Sharing Environment the discovery of any cyber intrusion events that affect DoD information resident on or transiting the contractor's unclassified information systems in accordance with DoD Directive 5505.13E?

Are practices in place to mitigate supply chain vulnerabilities in accordance with DoD Instruction 5200.39 paragraph 4g"

Are practices and procedures in place to address supply chain risk early and across the system life cycle in accordance with Directive Type Memorandum 09-016? Specifically, do they include:

- Incorporation of all-source intelligence analysis into assessments of the supply chain for covered systems?

- Controls to ensure that such all-source intelligence assessments are conducted in accordance with all applicable laws, Executive Orders, policies, and regulations governing intelligence activities and the safeguarding of classified information?

- Processes to assess threats from potential suppliers providing critical components to covered systems?

- Processes to control the quality, configuration, and security of software, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources?

- Processes to detect the occurrence, reduce the likelihood of occurrence, and mitigate the consequences of products containing counterfeit components or malicious functions?

- Processes to ensure that the fabrication of integrated circuits that are custom-designed and/or custom-manufactured (generally referred to as "application-specific integrated circuits") for a specific DoD end use within covered systems are, as appropriate to the risk, performed by suppliers of integrated circuit-related services accredited through an authority designated by the Under Secretary of Defense for Acquisition, Technology, and Logistics, unless expressly waived by the milestone decision authority established pursuant to DoD Directive 5000.01?

- Enhanced developmental and operational test and evaluation capabilities, including software vulnerability detection methods and automated tools that are compliant with the security content automation protocol and enhanced information assurance certification established by DoD Instruction 8510.01?

Has the supporting Defense counterintelligence Component coordinated a counterintelligence support plan with the cognizant RDA program manager? Does the counterintelligence support plan identify the activities that the supporting Defense counterintelligence Component will conduct at RDA programs with CPI, and at cleared defense contractors where RDA program CPI is located in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 6t and 8a?

Has the supporting Defense counterintelligence Component coordinated implementation of the counterintelligence support plan for a cleared defense contractor with the cognizant Defense Security Service industrial security representative, the Defense Security Service counterintelligence representative, the concerned Facility Security Officer, and is the Defense Security Service provided with a copy of the counterintelligence support plan in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 6t and 8a?

Has the supporting Defense counterintelligence Component informed the RDA program manager of threats and vulnerabilities associated with foreign capability to collect information using technical (e.g., close-in or proximity) means, and was a technical threat analysis performed by the counterintelligence Component's technical surveillance countermeasure element when deemed appropriate in accordance with DoD Instruction 5240.05, Paragraph 6.1.2?

Is there evidence that the activities described in the counterintelligence support plan are being carried out? If not, why not, and what has hindered or impeded execution in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 6t and 8a?

Was the technical surveillance countermeasure support requested and conducted in accordance with DoD Instruction 5240.05, Paragraph 4.1? If not, why not?

Is the supporting Defense counterintelligence Component informing the RDA contract office of foreign collection threats to CPI at all sites and facilities to include those that are not participants in the National Industrial Security Program and is there evidence that contracts are constructed or modified based on this information in accordance with DoD Instruction 5200.39, Paragraph 4h and Enclosure 2, Paragraph 8b?

Is the supporting Defense counterintelligence Component conducting foreign collection threat awareness briefings and conducting debriefings as necessary for RDA program personnel with knowledge of CPI? Are these action specified in the counterintelligence support plan in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6t and DoD Instruction 5240.06, Paragraph 4.2?

What actions are the supporting Defense counterintelligence Component conducting to assist a supported RDA program evaluate foreign collection threats to CPI when such information is included in foreign military or direct commercial sales programs or other international transfers of technology? Are these actions specified in the counterintelligence support plan when relevant in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6t?

Are records of incidents and reported information maintained by the organization, in accordance with DoD Instruction 5240.6, Paragraphs 4.1. and 6.2.?

If the organization is a DoD Component that does not have a counterintelligence capability, as highlighted in the Lead Agency assignment list in DoD Instruction 5240.10, Enclosures 4 and 5, does the Component and its supporting counterintelligence office have a signed counterintelligence support agreement, in accordance with DoD Instruction 5240.10, Enclosure 3, Paragraph E3.1.2.?

Does a security classification guide exist for the protection of CPI in accordance with Defense Acquisition Guidebook, Chapter 8, Paragraph 8.4.6.5.?

Is CPI and controlled unclassified information (specifically technical data that is not releasable to the public and/or is export-controlled) identified within the security classification guide in accordance with Defense Acquisition Guidebook, Chapter 8, Paragraph 8.4.6.5.?

Are instructions provided as to how CPI is to be marked, stored, and disseminated in accordance with Defense Acquisition Guidebook, Chapter 8, Paragraph 8.3.2.1.?

Are procedures in place at the facility or within an acquisition program for security and policy reviews of scientific and technical papers prior to release to the public at-large, at conferences, or at other international fora in accordance with DoD Directive 5230.09, Paragraph 4 and DoD Instruction 5230.27, Paragraph 5.5?

Are security efforts integrated with the systems engineering efforts, in accordance with DoD Instruction 5200.39, Paragraph 4a?

Are DoD information systems storing, processing, or transmitting CPI certified and accredited, in accordance with DoD Directive 8500.1 and DoD Instructions 8500.2 and 8510.01?

Are required Information Assurance protection measures negotiated and agreed to in contract or sharing agreements for non-DoD information systems containing CPI in accordance with DoD Directive Type Memorandum 08-027? Do protection requirements flow down through prime to subcontractors, as appropriate?

Is there a current accreditation decision issued by the Defense Security Service Designated Accrediting Authority for contractor information systems accredited under the National Industrial Security Program?

Has the organization designated, in writing, all information assurance-related positions (e.g., information assurance manager, information assurance officers, and privileged users) for DoD information systems storing, processing, or transmitting CPI, in accordance with DoD Instruction 8500.2, Section 5.8?

Are reports of Information Assurance protection self-assessments submitted to the program office periodically for DoD contractor information systems containing CPI? Do reports include appropriate levels of follow-up activity to clear discrepancies?

At facilities, sites, or acquisition programs involved in an international cooperative venture (research and development, technology development, foreign military sales, or other technology transfer program), have security personnel assisted in and/or reviewed (in accordance with DoD Directive 5230.09, DoD Instruction 5230.27, and Defense Acquisition Guidebook, Chapter 11, Paragraph 11.2.) the:

- Program Protection Plan?
- Technology Assessment and Control Plan?
- Data Exchange Agreement?
- Delegation of Disclosure Authority Letter?
- Program Security Instruction?

Are security requirements for non-releasable technical data or information communicated and executed for facilities that use foreign test and evaluation facilities in accordance with Defense Acquisition Guidebook, Chapter 11, Paragraph 11.2.?

Are there security officers and a security staff dedicated to providing for the security needs of programs (physical, personnel, information, communication, and other security) in accordance with DoD Instruction 5200.39, Paragraph 4a?

If the Component issued classified contracts to facilities under significant foreign ownership, control, or influence, has the Component contacted the applicable Defense Security Service office to determine how the foreign owned, controlled, or influenced mitigation/negation vehicle is working in accordance with DoD Manual 5220.22, Chapter 2, Section 3?

Does the organization use DD Form 254, "DoD Contract Security Classification Specification" and the guidance contained in DoD Regulation 5220.22, Appendix 4, when considering and applying classifications to a particular plan, program, project or study?

Are procedures in place to conduct administrative inquiries, investigations, and other administrative actions in connection with reports of sabotage, espionage, and subversive activities, and the loss, compromise, suspected compromise, or security violations involving the United States and foreign classified information established as outlined in DoD Regulation 5200.1, Chapter 10 and DoD Regulation 5220.22, Chapter 5?

6. Foreign Visit Program

What security procedures are in place for foreign national visits, or assignments to the facility to include access to automated information systems in accordance with DoD Directive 5230.20, Paragraphs 5.4.4.1., 5.5., and 5.6.?

Does the facility use the Foreign Visits-Confirmation Module to document all visits to the facility (walk-in, scheduled, or unscheduled)? If not, why not? If it is not being used, how is the facility documenting foreign visits and confirming that the visit took place in accordance with DoD Directive 5230.20, Paragraphs 4.8 and 5.4.3.2, and Directive Type Memorandum 09-012, Attachment 2, Paragraph 2.a?

Is foreign national access to information available on information systems controlled in accordance with DoD Directive 5230.20, DoD Directive 8500.01E, and DoD Instruction 8500.2?

Do badges identify the bearer as a foreign national, even if the foreign national is accredited and assigned as a foreign liaison officer?

Are foreign visits coordinated with the supporting Defense counterintelligence Component to determine if the visit or the visitor represents a potential collection threat in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 6c, l, m, s and t?

What actions are the supporting Defense counterintelligence Component conducting to assist the supported facility or RDA program evaluate collection threats posed by visits and assignments of foreign nationals in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraphs 6c, l, m, s and t?

If a potential foreign collection threat is associated with a foreign visit what actions are taken to mitigate the threat and monitor the activities of the foreign visitor in accordance with DoD Directive 5230.20, Paragraph 5.4.4.2. and DoD Instruction 5200.39, Enclosure 2, Paragraph 6s?

Are personnel who will come in contact with or host a foreign visitor receiving briefings that alert them to the security and collection threats, and do they know how to and to whom they should inform, should a reportable incident or event occur in accordance with DoD Directive 5230.20, Paragraph 5.4.4.2. and DoD Instruction 5240.06, Paragraph 4.2 and DoD Instruction 5200.39, Enclosure 2, Paragraph 6s?

In multi-national research and development facilities or foreign test and evaluation sites, are personnel provided with briefings regarding the potential threats unique to those environments and the reporting requirements for events or incidents in accordance with DoD Directive 5230.20, Paragraph 5.4.4.2. and DoD Instruction 5240.06, Paragraph 4.2 and DoD Instruction 5200.39, Enclosure 2, Paragraph 6s?

Are Limited Access Authorization agreements for access to DoD classified information in place for any foreign nationals present at the facility? Non-U.S. citizens do not qualify for a security clearance. However, if a non-U.S. citizen requires access to U.S. classified information for a compelling reason and meets the requirements of paragraph 2-209 and 2-210 of the National Industrial Security Program Operating Manual (DoD Manual 5220.22), a Limited Access Authorization, no higher than the Secret level, may be issued.

7. Horizontal Protection to Protect Critical Program Information

Is horizontal protection[1] practiced in your facility or acquisition program to include the protection of technology, CPI, and other controlled unclassified information in accordance with DoD Instruction 5200.39, Enclosure 2, Paragraph 6g and DoD Manual 5200.1, Paragraph C2.8.1.?

Is information related to facility, site, or program CPI put into the Acquisition Security Database to record and track CPI for horizontal protection, compromise, and analysis purposes in accordance with Under Secretary of Defense (Acquisition, Technology, and Logistics) memorandum, "Horizontal Protection of DoD Critical Program Information," July 22, 2010?

Is guidance related to the mitigation of risks identified in supply chain vulnerabilities in RDA programs that are assessed to contain CPI being implemented in accordance with DoD Instruction 5200.39, Paragraph 4g?

Are incidents of loss, compromise, or theft of CPI and anti-tamper breaches reported in accordance with DoD Directive O-5240.02, DoD Instruction 5200.39, Enclosure 2, Paragraph 6r, and DoD Regulation 5200.1?

Has the program's record in the horizontal protection database been kept current throughout the acquisition lifecycle in accordance with DoD Instruction 5200.39, Paragraph 4c and Enclosure 2, Paragraph 6g?

Was the horizontal protection database used to ensure that the CPI is being protected similarly in other programs across the DoD in accordance with DoD Instruction 5200.39, Paragraph 4c and Enclosure 2, Paragraph 6g?

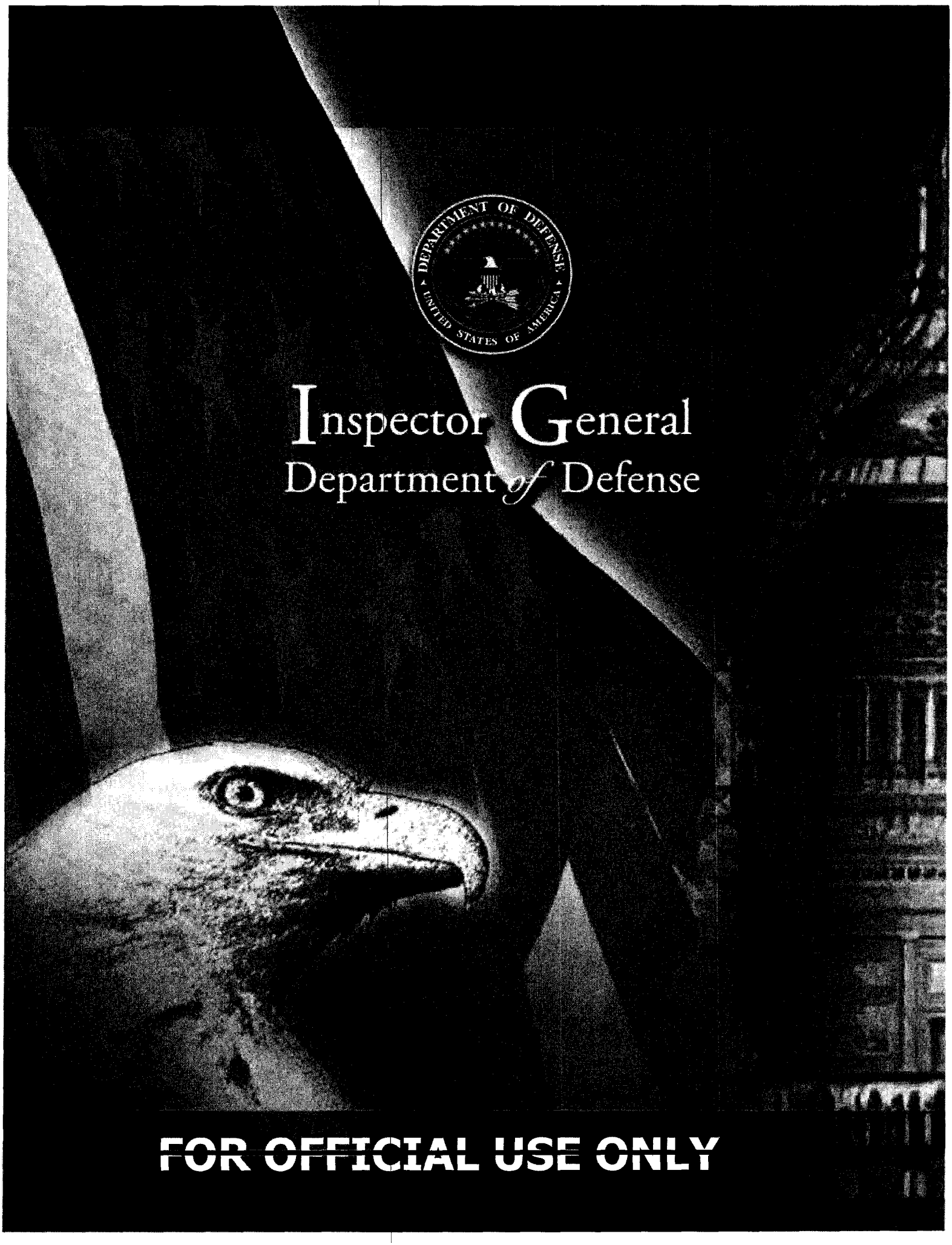
Was the program's CPI assessed to determine whether it is being used differently from other programs and determined to need different or enhanced protection in accordance with DoD Instruction 5200.39, Paragraph 4c and Enclosure 2, Paragraph 6g?

8. Policies to Protect Critical Program Information

Are issuances for the identification and protection of CPI current, understood by those who have to use them, and aligned with Department policies and guidance? If not, why not?

---

[1] The process that determines if critical Defense technologies, to include CPI, associated with more than one RDA program are protected to the same degree by all involved DoD activities.


DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
Inspector General
Department of Defense
FOR OFFICIAL USE ONLY