Report No. 06-INTEL-03
February 28, 2006

DEPARTMENT OF DEFENSE
OFFICE OF
INSPECTOR GENERAL

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

Inspection Guidelines for DoD Research and Technology Protection, Security, and Counterintelligence for 2006

Additional Information and Copies

To obtain additional copies of this report, contact Mr. Donald A. Ragley at (703) 604-8896 (DSN 664-8896) or fax (703) 604-0045.

Suggestions for Future Evaluations

To suggest ideas for or to request future evaluations of Defense intelligence issues, contact the Office of the Deputy Inspector General for Intelligence at (703) 604-8896 (DSN 664-8896) or fax (703) 604-0045. Ideas and requests can also be mailed to:

Office of the Deputy Inspector General for Intelligence
Department of Defense Office of Inspector General
400 Army Navy Drive (Room 703)
Arlington, VA 22202-4704

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.osd.mil www.dodig.mil/hotline

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

February 28, 2006

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
DEPUTY UNDER SECRETARY OF DEFENSE FOR LABORATORIES AND BASIC SCIENCES
DIRECTOR, DEFENSE TEST RESOURCE MANAGEMENT CENTER
INSPECTOR GENERAL, DEPARTMENT OF THE ARMY
NAVAL INSPECTOR GENERAL
INSPECTOR GENERAL, DEPARTMENT OF THE AIR FORCE
DIRECTOR, PROGRAM INTEGRATION, INTERNAL MANAGEMENT REVIEW, MISSILE DEFENSE AGENCY

SUBJECT: Inspection Guidelines for DoD Research and Technology Protection, Security and Counterintelligence for 2006 (Report No. 06-INTEL-03)

We are providing this report on inspection guidelines for information and use. We considered management comments on a draft of this report in preparing the final report. The comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

The team members are listed inside the back cover. Questions should be directed to Mr. Donald A. Ragley at (703) 604-8896 (DSN 664-8896) or Mr. David Ingram at (703) 604-8826 (DSN 664-8826). See Appendix C for the report distribution.

Shelton Young

Shelton R. Young
Deputy Inspector General
for Intelligence

Department of Defense Office of Inspector General

Report No. 06-INTEL-03 **February 28, 2006**
(Project No. D2006-DINT01-0031)

Inspection Guidelines for DoD Research and Technology Protection, Security and Counterintelligence for 2006

Executive Summary

Who Should Read This Report and Why? DoD civilian and military personnel who are responsible for, supervise any aspect of, or provide oversight for the protection of research and technology information in DoD research, development, test and evaluation facilities should read this report. This report publishes the guidelines for inspecting research and technology protection, security, and counterintelligence practices at DoD research, development, test, and evaluation facilities to enhance Department-wide consistency in the oversight process.

Background. These guidelines satisfy the requirement in the Deputy Secretary of Defense memorandum for Inspection of Security and Counterintelligence Practices at Laboratories and Centers, February 17, 2000. On May 8, 2002, the DoD Inspector General; the Deputy Under Secretary of Defense for Laboratories and Basic Sciences; the Director, Operational Test and Evaluation; the Service Inspectors General; and the Director, Program Integration, Internal Management Review (formerly Internal Assessments), Missile Defense Agency signed a memorandum of understanding on security, technology protection, and counterintelligence inspections.

The memorandum of understanding requires participating Inspectors General and the Director, Program Integration, Internal Management Review, Missile Defense Agency to inspect research, development, test, and evaluation facilities as part of their normal inspection cycle, and prepare and forward significant findings and recommendations to the DoD Office of Inspector General at the end of each inspection. The DoD Office of Inspector General issues the summary report of inspections of security, technology protection, and counterintelligence practices at DoD research, development, test, and evaluation facilities.

Results. This report updates the Security, Research and Technology Protection, and Counterintelligence Inspection Guidelines, Report No. 03-INTEL-09, May 6, 2003.

Management Comments. No written response to this report was required.

Table of Contents

Background

In early 1999, the Deputy Secretary of Defense directed the Service Inspectors General to survey the counterintelligence and security programs at more than 60 research, development, test and evaluation facilities. The inspection teams identified a number of recommendations related to the specific sites. As a result of these efforts, the Deputy Secretary chartered an Overarching Integrated Process Team to better frame the recommendations and to oversee their implementation. From February 12 to May 12, 2000, the Deputy Secretary signed seven memoranda containing 27 tasks aimed at enhancing counterintelligence and security support to research, development, test and evaluation facilities and the acquisition process.

On February 17, 2000, the Deputy Secretary signed a memorandum requesting that the DoD Office of Inspector General develop a uniform system of periodic reviews, through the existing agency and Service inspection processes, for compliance with DoD Directives concerning research and technology protection, security, and counterintelligence practices. Those reviews were to assist in protecting the technology-dependent, cutting edge of U.S. weapon systems. The memorandum also requested that the DoD Office of Inspector General develop inspection list guidelines for DoD Inspectors General to enhance consistency.

On May 8, 2002, the DoD Inspector General; the Deputy Under Secretary of Defense for Laboratories and Basic Sciences; the Director, Operational Test and Evaluation; the Service Inspectors General; and the Director, Program Integration, Internal Management Review (formerly Internal Assessments), Missile Defense Agency signed a memorandum of understanding on research and technology protection, security, and counterintelligence inspections.

The memorandum of understanding requires participating Inspectors General to prepare and forward any significant findings and recommendations to the DoD Office of Inspector General at the end of each inspection. It also requires the DoD Office of Inspector General to issue a summary report of inspections of research and technology protection, security, and counterintelligence practices at DoD research, development, test, and evaluation facilities.

Objectives

The overall objective was to update the guidelines that comprise DoD policy and to improve DoD-wide consistency in inspections of research, development, test, and evaluation facilities. See Appendix A for a discussion of the scope and methodology.

Areas for Inspections

We updated the guidelines on DoD policy to include ways to better assess how DoD implements policy for research and technology protection, security, and counterintelligence. These guidelines focus on key areas of the requirement in the Deputy Secretary of Defense February 17, 2000, memorandum, to "develop inspection list guidelines for Department-wide Inspectors General to enhance consistency across DoD." Specifically, the inspection areas are research and technology protection, security, counterintelligence, and international security.

Security

General Security

Have security managers or other key security staff, or both, received specialized training to support Research, Development, Test and Evaluation facilities?

Is the security budget adequate to meet all requirements? If not, what are the effects?

Is the security staff adequate in size, rank/grade, and position within the organization?

Physical Security

Is there a designated point of contact to oversee the physical security program in accordance with, DoD Regulation 5200.8, Chapter 2, Section C2.2?

Are policies and procedures for physical security standards in place (e.g., vault and secure room construction standards, intrusion detection system standards, access controls and lock replacement), in accordance with DoD Regulation 5200.1, Appendix 7?

Are physical security planning procedures for acquisition of major systems appropriate and in accordance with DoD Regulation 5200.8, Chapter 2, Sections C2.5. and C2.6.; and Figure C2.F2?

Do procedures and policies in place restrict access to installations and facilities, in accordance with DoD Regulation 5200.8, Chapter 3, Sections C3.1. and C3.2. Specifically, do they:

- Use a security-in-depth concept to provide graduated levels of protection from the installation perimeter to critical assets?

- Determine the degree of control required over personnel and equipment entering or leaving the installation?

- Prescribe procedures for inspecting persons, property, and vehicles at entry and exit points of installations, at designated secure areas within an installation, and for searching persons and their possessions while they are on the installation?

- Enforce the removal of, or deny access to, persons who are a threat to the order, security, and discipline of the installation?

- Designate restricted areas to safeguard property or material?

- Use random antiterrorism measures within existing security operations to reduce patterns, change schedules, and visibly enhance the security profile to reduce the effectiveness of preoperational surveillance by hostile elements?

Does the security system provide the capability to detect, assess, communicate, delay, and respond to an unauthorized attempt at entry, in accordance with DoD Regulation 5200.8, Chapter 2, Section C2.3.2.?

Is there a matrix of physical security threats to use as a guide to develop program, system, command, and installation threat statements that assess potential security threats to critical assets, in accordance with DoD Regulation 5200.8, Chapter 2, Section C2.4. and Figures C2.F.1. and C2.F2?

Are plans to increase vigilance and restrict access in place at installations and facilities under the following situations, in accordance with DoD Regulation 5200.8, Chapter 3, Section C3.4.?:

- National emergencies?

- Disasters?

- Terrorist threat conditions (See DoD Directive 2000.12 for further information)?

- Significant criminal activity?

- Civil disturbances?

- Other contingencies that would seriously affect the ability of installation personnel to perform their mission?

Personnel Security

Has the organization designated a representative to direct and administer the Personnel Security Program (DoD Directive 5200.2, Section 4.3)?

Are personnel security investigations limited to those essential to current operations and authorized by DoD policies, in accordance with DoD Regulation 5200.2, Chapter 3, Sections C3.1. and C3.2.; and Appendix 3, Tables 1-5?

Are personnel assigned to proper billets (e.g., special access program, Top Secret/Sensitive Compartmented Information)?

Has the organization designated sensitive positions that require a personnel security investigation in accordance with DoD Regulation 5200.2, Chapter 3, Sections C3.1. and C3.2.; and Appendix 3, Tables 1-5? Was the designating official authorized to perform this function, in accordance with DoD Regulation 5200.2, Appendix 5?

Is the process for issuing Top Secret clearances standardized and controlled, in accordance with DoD Regulation 5200.2, Chapter 3, Section C3.1.5.?

Are periodic reinvestigations submitted in a timely manner, in accordance with DoD Regulation 5200.2, Section C3.7.?

Are policies and procedures in place for processing security clearances for military, DoD civilian, and contractor personnel who are employed by or are serving in a consulting capacity to DoD and who require access to classified information as part of their official duties, in accordance with DoD Regulation 5200.2, Chapters 2, 3, and 9; and Appendixes 3, 4, and 8?

Are Limited Access Authorization(s) granted to non-U.S. citizens under compelling circumstances or to further the DoD mission, in accordance with DoD Regulation 5200.2, Sections C2.1.1. and C3.4.3.; and Appendixes 5 and 6?

Information Security

Has the organization committed the necessary resources for the effective implementation of the DoD Information Security Program, in accordance with DoD Regulation 5200.1, Chapter 1, Section C1.2.2.2.?

Has the organization designated a security manager and provided that person with the requisite training to provide proper management and oversight of the organization's Information Security Program, especially those elements which create, handle, or store classified information, in accordance with DoD Regulation 5200.1, Chapter 1, Section C1.2.2.3. and Chapter 9?

Is all classified information (hard-copy documents and automated information systems media) clearly labeled, designated, or marked, in accordance with DoD Regulation 5200.1, Chapter 5 and DoD Pamphlet 5200.1?

Are policies and procedures in place for transmitting and transporting classified information or material approved for release within DoD or to foreign governments, in accordance with DoD Regulation 5200.1, Chapter 7 and Appendix 8?

Are procedures in place for reporting compromises of classified information or incidents that may put classified information at risk of compromise, in accordance with DoD Regulation 5200.1, Chapter 10?

- If a compromise of a foreign government's classified information occurred, were reports submitted to the Director, International Security Programs, Office of the Under Secretary of Defense (Policy), in accordance with DoD Regulation 5200.1, Chapter 10, Section C10.1.2.8.?

- Has classified information for DoD special access programs been compromised, and, if so, were reports submitted to the Director, Special Access Programs, Office of the Under Secretary of Defense (Policy), in accordance with DoD Regulation 5200.1, Chapter 10, Section C10.1.2.9.?

- Have computer systems, terminals, or equipment been compromised, and, if so, were reports submitted through appropriate channels to the Director, Information Assurance, Office of the Deputy Assistant Secretary of Defense (Security and Information Operations), in accordance with DoD Regulation 5200.1, Chapter 10, Section C10.1.2.7.?

Has the security manager established and maintained an ongoing self-inspection program that includes a periodic review and assessment of the facility's classified products, in accordance with DoD Regulation 5200.1, Chapter 1, Section C1.2.3.4.?

Is there a coordination process in place for host, tenant, and visiting security managers?

Are policies and procedures in place for sponsoring conferences, seminars, symposia, exhibits, or conventions at which classified information is disclosed and which is conducted by a DoD Component, by a cleared DoD contractor, or by an association, institute, or society whose membership consists of contractors, contractor employees, or DoD personnel, in accordance with DoD Regulation 5220.22, Chapter 1, Section C1.4.?

Information Assurance

Does the organization have an assigned Designated Approving Authority for its information systems, in accordance with DoD Directive 8500.1, Paragraphs 4.14.3 and 4.25?

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

Are procedures in place for the Information Assurance Officer to properly report information assurance incidents to the Designated Approving Authority and the DoD reporting chain, as required?

Are procedures in place for the information assurance manager and the information assurance officer to implement protective measures or

countermeasures in response to an information assurance incident or vulnerability?

Is information assurance-related documentation for DoD information systems current and accessible to properly authorized individuals?

Have information systems been categorized as automated information systems applications, enclaves (which include networks), outsourced information technology-based processes, or platform information technology connections, in accordance with DoD Directive 8500.1, Paragraph 4.2?

Have information systems been assigned a mission assurance category and a confidentiality level based on the classification or sensitivity of the information processed, in accordance with DoD Instruction 8500.2, Enclosure 4, Paragraph E4.1.9.?

Are applicable information assurance controls in place for the appropriate mission assurance category and information system confidentiality levels, in accordance with DoD Instruction 8500.2, Enclosure 4 and its attachments?

Have Information Technology Position Categories been designated for personnel occupying information systems positions performing on unclassified information systems, in accordance with DoD Instruction 8500.2, Enclosure 2, Paragraph E2.1.36, and DoD Regulation 5200.2?

Do information assurance managers, information assurance officers, and privileged users hold appropriate U.S. Government security clearances commensurate with the level of information processed by the facility's information systems or enclaves?

Do privileged-user personnel with management access to unclassified information systems have the appropriate background investigation, in accordance with DoD Instruction 8500.2, Enclosure 3, Table E3.T1?

Are personnel granted access to DoD information systems only on a need-to-know basis, in accordance with DoD Directive 8500.1, Paragraph 4.8 and DoD Instruction 8500.2, Paragraph 5.7.11?

Is foreign national access to information available on information systems controlled, in accordance with DoD Directive 5230.20, DoD Directive 8500.1, and DoD Instruction 8500.2?

Are all DoD information systems certified and accredited, in accordance with DoD Directive 8500.1 and DoD Instructions 8500.2 and 5200.40?

Does the facility have processes in place for reviewing and evaluating the content of all its associated Internet sites to determine whether they comply with DoD Web-site Administration and Procedures, November 25, 1998, and updates?

Is the Information Assurance Vulnerability Alert program managed in accordance with Deputy Secretary of Defense memorandum, "DoD Information Assurance Vulnerability Alert," December 30, 1999?

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.?

Operations Security

Has an operations security program been established, in accordance with National Security Decision Directive 298 and DoD Directive 5205.2, Paragraph 5.2.?

Are the operations security plans and programs reviewed and validated annually, in accordance with DoD Directive 5205.2, Paragraph 5.2.1.4.?

Is there an operations security education and awareness training program and does it comply with DoD Directive 5205.2, Paragraph 5.2.1.3.?

Industrial Security

Does the contractor have a designated security officer?

Were operations security requirements and security clauses included in contracts, when applicable, in accordance with DoD Directive 5205.2, Paragraph 5.2.4.?

Are policies and procedures in place for sponsoring conferences, seminars, symposia, exhibits, or conventions at which classified information is disclosed and which is conducted by a DoD Component, by a cleared DoD contractor, or by an association, institute, or society whose membership consists of contractors, contractor employees, or DoD personnel, in accordance with DoD Regulation 5220.22, Chapter 1, Section C1.4.?

Does the Component issue any classified contracts to facilities that are under foreign ownership, control, or influence? If so, how many? Does each facility that is under significant foreign ownership, control, or influence have a security clearance verification letter issued by the Defense Security Service that reflects the vehicle (Special Security Agreement, Proxy Agreement, Voting Trust Agreement) put in place to mitigate/negate the facility's significant foreign ownership, control, or influence, in accordance with DoD Manual 5220.22, "National Industrial Security Program Operating Manual," Chapter 2, Section 3?

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?

Has the organization outlined the industrial security functional responsibilities of contracting officers commensurate with those outlined in DoD Regulation 5220.22, Appendix 3?

Does the organization conduct analysis and take precautions before it authorizes contractors to release unclassified economic and technical information in press releases, advertisements, notices to stockholders, and annual or quarterly reports that could contribute to an accurate appraisal of the strategic intentions of the United States, in accordance with DoD Regulation 5220.22, Appendix 1?

Are security policies and procedures in place for contractor visits to the activities, in accordance with DoD Regulation 5220.22, Chapter 3?

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?

Are procedures in place for coordinating with the Defense Security Service on security issues (e.g., security violations, visit control, and security education) involving cleared contractor personnel or facilities?

Has the organization prescribed the requirements and established the procedures to identify the classification of information turned over to contractors? Has the organization outlined the responsibility for issuing instructions for disposing of classified information on final delivery of goods or services or on termination of a classified contract? Has the organization also identified other security requirements for prime contracts and subcontracts, in accordance with DoD Regulation 5220.22, Chapter 7?

Security Education

Has an employee security education program been established, evaluated, and maintained, in accordance with DoD Regulation 5200.1, Chapter 9?

Are employees aware of their security responsibilities, in accordance with DoD Regulation 5200.1, Chapter 9 and DoD Regulation 5200.2, Chapter 9, Section C9.2.?

Has the organization developed a foreign travel briefing for personnel with access to classified information to alert them to possible exploitation by foreign intelligence services, in accordance with DoD Regulation 5200.2, Chapter 9, Sections C9.1.4. and C9.2.4.?

Has an operations security education and awareness training program been established, in accordance with DoD Directive 5205.2, Paragraph 5.2.1.3.?

Does the security education program address the need to protect classified information and hardware and any other information or hardware that is considered sensitive by the organization?

Has the organization addressed the educational aspects and training requirements of the DoD Component's applicable regulations or DoD Regulation 5220.22, Chapter 6?

Has the organization developed a program to periodically brief personnel on the threats posed by foreign intelligence, foreign commercial enterprises, terrorists, computer intruders, and unauthorized disclosure, in accordance with DoD Instruction 5240.6, Paragraph 4.2 and 6.1?

Has the organization, where appropriate, developed training for implementing acquisition program protection and managing risk referred to in DoD Directive 5200.39, Paragraph 4.7, and DoD Manual 5200.1, Section C2.9.?

Is the security training program adequate to prepare the designated officer to oversee the activity's Information Security Program?

Research and Technology Protection

Counterintelligence Support for Facilities

Has critical program information been identified for the counterintelligence support plan?

Does the facility have an approved counterintelligence support plan?

Are agreed-upon counterintelligence support activities in the counterintelligence support plan being accomplished?

Are full-time, dedicated, counterintelligence specialists from DoD Components assigned to provide research and technology protection? If not, what type of service is provided? Is this adequate?

Does the facility or its programs have a current Multidiscipline Counterintelligence Threat Assessment?

Are the Program Managers or key acquisition program personnel, or both, receiving threat reports, threat estimates, and other threat analysis products on research and technology protection from DoD Component counterintelligence agencies on a recurring basis?

Are security, management, and acquisition program personnel kept current about local matters of counterintelligence interest?

Security and Counterintelligence Support for Acquisition Systems

Deputy Secretary of Defense memorandum, "Cancellation of DoD 5000 Defense Acquisition Policy Documents," October 30, 2002, replaced DoD Directive 5000.1, DoD Instruction 5000.2, and DoD Regulation 5000.2 with the Interim Defense Acquisition Guidebook, October 17, 2004.

Has the organization identified its critical program information in accordance with DoD Directive 5200.39, Paragraph 4.1. and the Interim Defense Acquisition Guidebook, Chapter 8?

Have programs with critical program information completed the following tasks, in accordance with DoD Directive 5200.39:

- Identified program goals and objectives to the supporting security, counterintelligence, and intelligence organizations (Paragraph 4.2.)?
- Identified system vulnerabilities (Paragraph 4.2.)?
- Performed risk management evaluations for cost-effective measures (Paragraph 4.2.)?

- Developed a program protection plan as described in DoD Manual 5200.1 (Chapters 2 and 3) and the Interim Defense Acquisition Guidebook, approved by the program manager, and reviewed by the milestone decision authority?

- Reported incidents of loss, compromise, or theft of identified critical program information in accordance with procedures in DoD Instruction 5240.4 and DoD Regulation 5200.1, Chapter 10?

Does the organization or acquisition program manager provide tailored counterintelligence support to acquisition programs with critical program information throughout their life cycles in accordance with DoD Directive 5200.39 and the Interim Defense Acquisition Guidebook, Chapter 8?

Does the program protection plan for each acquisition program with critical program information include an approved counterintelligence support plan?

Is the life-cycle counterintelligence support that is documented in the counterintelligence support plan being provided to protect critical program information?

Does the counterintelligence support plan include all required annexes for each facility where there is critical program information?

Is a DoD counterintelligence agency providing agreed-upon counterintelligence support as stated in the counterintelligence support plan?

Have the countermeasures identified in the program protection plan been employed in accordance with DoD Manual 5200.1, Section C3.9? Do the program manager and the program manager's staff know the results of the employment of the countermeasures?

Did the program manager request a multidiscipline counterintelligence threat assessment for programs having critical program information, in accordance with DoD Manual 5200.1, Section C3.8.? If so, did a DoD Component counterintelligence agency provide the assessment? How current is the document?

Is the program manager receiving foreign intelligence, and other related threats to acquisition programs with critical program information, from DoD counterintelligence and other agencies. Has the program manager received updated threat and other counterintelligence information from the point of contact of each program with critical program information throughout the life cycle of the program, in accordance with the Interim Defense Acquisition Guidebook, Chapter 8?

Did the program manager document and implement anti-tamper measures for programs or systems with critical program information, in accordance with the Interim Defense Acquisition Guidebook, Chapter 8?

If the program manager determines that there is no critical program information associated with the program (neither integral to the program nor inherited from a supporting program), a program protection plan is not required. Has the program manager made this determination in writing for review by the milestone decision authority, in accordance with DoD Directive 5200.39, Section 4.3.3.?

Is controlled unclassified information about programs, technologies, or systems identified, controlled, and protected from unauthorized disclosure, in accordance with DoD Regulation 5200.1, Appendix 3?

Has an integrated process team been established to develop program-specific protection plans and to coordinate security, counterintelligence, and intelligence issues as outlined in DoD Directive 5200.39, Section 4.5., and described in DoD Manual 5200.1, Section C3.2.?

Is basic DoD acquisition indoctrination and/or unique business training available for responsible security and counterintelligence personnel? Have they received that training?

Counterintelligence

Counterintelligence

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, Paragraph 5.5.7.1.?

Have all counterintelligence field personnel providing research and technology protection support received or scheduled required specialized training on how to perform this mission? If not, does the organization have a plan to train all personnel who require the specialized training?

Are dedicated, full-time counterintelligence specialists assigned to research and technology protection duties at major research, development, test, and evaluation sites?

Does the unit/program/activity need technical surveillance countermeasures support? If so, was the support provided and was it timely?

Has the counterintelligence and security program been assessed (once that program has been started)? When was the last assessment?

If you need or receive counterintelligence support, on a scale of 1 to 10, with 1 being the lowest and 10 being the highest, how would you rate the quality of the support you receive from your local counterintelligence office? Please explain.

International Security

Disclosure of Classified Military Information to Foreign Governments

Has the organization designated a disclosure authority, in accordance with DoD Directive 5230.11, Paragraphs 4.1. and 5.2.?

Is the designated disclosure authority familiar with the National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," and DoD Directive 5230.11?

When classified military information was disclosed to foreign governments in support of a lawful and authorized U.S. Government purpose by individuals who were specifically delegated disclosure authority:

- Were the disclosures made, in accordance with National Disclosure Policy-1 and DoD Directive 5230.11?
- Did the designated disclosure authorities receive security assurance on the individuals who were to receive the information, in accordance with DoD Directive 5230.11, Paragraph 4.4. and DoD Regulation 5200.1?
- Did the designated disclosure authority authorize, in advance, proposals to be made to foreign governments that could lead to the eventual disclosure of classified military material, technology or information, in accordance with DoD Directive 5230.11, Paragraph 4.5.?
- Were disclosures and denials of classified military information reported in the Foreign Disclosure and Technical Information System, in accordance with DoD Instruction 5230.18 and DoD Directive 5230.11?

Does the organization have procedures in place to preclude unauthorized access to controlled unclassified information and classified information by foreign visitors or their assignees, in accordance with DoD Directive 5230.20 and DoD Regulation 5200.1?

Did participation of foreign nationals or government representatives in classified meetings and conferences at the facility comply with the requirements of DoD Directive 5230.20 and DoD Directive 5230.11; that is, was assurance obtained in writing from the responsible Government foreign disclosure office(s) that the information to be presented was cleared for foreign disclosure?

Do the organization's procedures for releasing and transmitting classified information to foreign governments comply with the requirements of DoD Regulation 5200.1, Chapter 7 and Appendix 8?

Foreign Visits, Assignments, Exchanges and Travel

Is an automated capability or a visitor log maintained to track and document foreign visitor access at sensitive facilities?

Is confirmation of automated information on foreign visitors provided to the Counterintelligence Field Activity?

Are counterintelligence personnel reviewing the foreign visits system database for trends or data to be extracted for analysis?

Are commanders informed of how many foreign visitors are received, the reason for their visit, when they arrive, how long they stay, and what they are doing?

Do employees receive a security briefing before they visit foreign research facilities or attend foreign professional conferences?

Do counterintelligence personnel interview employees after employees return from travel to foreign laboratories or professional conferences?

Does any counterintelligence entity advise sponsoring organization personnel about the possible implications of their sponsorship of individual foreign visitors to the organization before and after visits?

Do procedures for approving each short- or long-term foreign visit differ for classified information and unclassified information?

Are reporting procedures in place to encourage employees to report suspicious contacts with foreign visitors to the security manager or a counterintelligence official?

Does the security manager or a counterintelligence official brief employees before and after foreign visits to the facility?

Does a counterintelligence entity report the results of foreign travel interviews and other anomalous incidents regarding laboratory employees'contact with foreign visitors?

Is the facility in compliance with the visitor control and processing requirements, as stated in DoD Directive 5230.20? Is an appropriate international agreement in place to cover the visit or assignment of foreign personnel for more than 30 days?

Do counterintelligence personnel conduct name checks on foreign visitors and report the results to the appropriate facility personnel?

Are security procedures in place for foreign nationals at the facility? If so, what are they?

- Are access controls in place for automated information systems?
- Do e-mail addresses clearly identify foreign nationals?

- Do badges identify the bearer as a foreign national?

Has a point of contact been designated to control the activities of foreign visitors, cooperative program personnel, foreign liaison officers, and exchange personnel?

Is a designated official reviewing the organization's compliance with DoD Directive 5230.11, applicable DoD Component guidelines for the release of classified and controlled unclassified information, and the specific disclosure guidelines established in the pertinent Delegation of Disclosure Authority Letter, in accordance with DoD Directive 5230.20?

Are all foreign nationals who are authorized unescorted access to DoD facilities issued with badges or passes that clearly identify them as foreign nationals, in accordance with DoD Directive 5230.20, Paragraph 4.12.?

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, and DoD Directive 5230.20, Paragraph 4.10.?

Has the organization coordinated with the Defense Security Service and appropriate DoD Components on the assignment of foreign liaison officers or extended visitors performing on a classified contract at a DoD-cleared contractor facility, in accordance with DoD Directive 5230.20?

Arms Control

Do facility security plans, policies, and procedures appropriately consider arms control agreements if the facility or program is involved in implementing arms control, in accordance with DoD Directive 5205.10, Paragraph 4.2?

Appendix A. Scope and Methodology

The DoD Inspectors General or officials responsible for providing oversight to research, development, test, and evaluation facilities should use the guidelines to assess how DoD implements policy for research and technology protection, security, and counterintelligence. We updated each reference from the 2003 inspection guidelines, then coordinated the revised guidelines with DoD Inspectors General or officials responsible for providing oversight to research, development, test, and evaluation facilities to ensure the currency of the guidelines.

Our scope was limited in that we did not include tests of management controls or validate the information or results reported in summarized reports. However, DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and that evaluating the adequacy of management controls should be an integral aspect of the inspection program.

Appendix B. References

National Security Decision Directive 298, "National Operations Security Program," January 22, 1998. http://www.fas.org/irp/offdocs/nsdd298.htm

National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations." (Classified)

Department of Defense Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003. http://www.dtic.mil/whs/directives/corres/html/200012.htm

Department of Defense Directive 5200.2, "DoD Personnel Security Program," April 9, 1999. http://www.dtic.mil/whs/directives/corres/html/52002.htm

Department of Defense Directive 5200.39, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection, "September 10, 1997. http://www.dtic.mil/whs/directives/corres/html/520039.htm

Department of Defense Directive 5205.2, "DoD Operations Security (OPSEC) Program," November 29, 1999.
http://www.dtic.mil/whs/directives/corres/html/52052.htm

Department of Defense Directive 5205.10, "Department of Defense Treaty Inspection Readiness Program (DTIRP)," December 5, 2000.
http://www.dtic.mil/whs/directives/corres/html/520510.htm

Department of Defense Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992. http://www.dtic.mil/whs/directives/corres/html/523011.htm

Department of Defense Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005.
http://www.dtic.mil/whs/directives/corres/html/523020.htm

Department of Defense Directive 8500.1, "Information Assurance (IA)," October 24, 2002.
http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf

Department of Defense Instruction 5230.18, "DoD Foreign Disclosure and Technical Information System (FORDTIS)," November 6, 1984.
http://www.dtic.mil/whs/directives/corres/html/523018.htm

Department of Defense Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)," December 30, 1997.
http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf

Department of Defense Instruction 5240.4, “Reporting of Counterintelligence and Criminal Violations,” September 22, 1992.
http://www.dtic.mil/whs/directives/corres/html/52404.htm

Department of Defense Instruction 5240.10, “Counterintelligence Support to the Combatant Commands and the Defense Agencies,” May 14, 2004.
http://www.dtic.mil/whs/directives/corres/html/524010.htm

Department of Defense Instruction 5240.6, “Counterintelligence (CI) Awareness, Briefing, and Reporting Programs,” August 7, 2004.
http://www.dtic.mil/whs/directives/corres/html/52406.htm

Department of Defense Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003.
http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf

Department of Defense Manual 5200.1, “Acquisition Systems Protection Program,” March 1994.
http://www.dtic.mil/whs/directives/corres/pdf/52001m_0394/p52001m.pdf

Department of Defense Manual 5220.22, “National Industrial Security Program Operating Manual,” (NISPOM) January 1995, Including July 1997 and February 2001 changes to NISPOM.
http://www.dtic.mil/whs/directives/corres/html/522022m.htm
NISPOM Supplement:
http://www.dtic.mil/whs/directives/corres/html/522022ms.htm

Interim Defense Acquisition Guidebook, October 17,2004.
http://akss.dau.mil/dag/DoD5000.asp

Department of Defense Regulation 5200.1, “Information Security Program,” January 1997. http://www.dtic.mil/whs/directives/corres/html/52001r.htm

Department of Defense Regulation 5200.2, “Personnel Security Program,” (change 3), February 23, 1996.
http://www.dtic.mil/whs/directives/corres/html/52002r.htm

Department of Defense Regulation 5200.8, “Physical Security Program.” May 1991. http://www.dtic.mil/whs/directives/corres/html/52008r.htm

Department of Defense Regulation 5220.22, “Industrial Security Regulation,” December 1985. http://www.dtic.mil/whs/directives/corres/html/522022r.htm

DoD Information Assurance Vulnerability Alert (IAVA) Program, December 30, 1999. http://iase.disa.mil/policy.html

DoD Web-Site Administration Policies & Procedures, November 25, 1998.
http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html

DoD Pamphlet 5200.1, “DoD Guide to Marking Classified Documents,” April 1997. http://www.dtic.mil/whs/directives/corres/html/52001ph.htm

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Intelligence
Under Secretary of Defense for Acquisition, Technology and Logistics
Deputy Under Secretary of Defense (Laboratories and Basic Sciences)

Department of the Army

Auditor General, Department of the Army
Inspector General, Department of the Army

Department of the Navy

Auditor General, Department of the Navy
Naval Inspector General

Department of the Air Force

Auditor General, Department of the Air Force
Inspector General, Department of the Air Force

Other Defense Organizations

Director, Defense Test Resource Management Center
Director, Program Integration, Internal Management Review, Missile Defense Agency

Team Members

The Department of Defense Office of the Deputy Inspector General for Intelligence, prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Shelton R. Young
Donald A. Ragley
David Ingram
Jacqueline Pugh