Report No. 06-INTEL-14
September 20, 2006
Summary Report

DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

FY 2005 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test and Evaluation Facilities

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

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

September 20, 2006

MEMORANDUM FOR 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: Report on FY 2005 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test, and Evaluation Facilities (Report No. 06-INTEL-14)

We are providing this report for your information and use. We issued a draft of this report on August 11, 2006. No written response to this report was required, and none was received. Therefore, we are publishing this report in final form.

The team members are listed inside the back cover. Questions should be directed to Mr. Donald 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-14 **September 20, 2006**
(Project No. D2006-DINT01-0227)

Report on FY 2005 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test, and Evaluation Facilities

Executive Summary

Who Should Read This Report and Why? DoD civilian and military personnel who are responsible for, supervise any aspect of, or provide support for protecting technology in DoD laboratory facilities should read this report. This report summarizes significant results of 29 inspections of security, technology protection, and counterintelligence practices at DoD research, development, test, and evaluation facilities by the Inspectors General of the Army, Navy, Air Force, and the Director, Program Integration, Internal Management Review during FY 2005.

Background. On May 8, 2002, the Inspector General, DoD; the Deputy Under Secretary of Defense for Laboratories and Basic Sciences; the Director, Operational Test and Evaluation; the Service Inspectors General; and the Director, Program Integration, Internal Management Review, 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 prepare and forward to the DoD Office of the Inspector General any significant findings and recommendations at the end of each inspection. The DoD Office of the Inspector General issues a summary report of inspections of security, technology protection, and counterintelligence practices at DoD research, development, test, and evaluation facilities. The facilities inspected are listed in Appendix B.

Results. The Offices of the Inspectors General and the Director, Program Integration, Internal Management Review, Missile Defense Agency did not identify significant systemic deficiencies that would threaten program security; however, they did identify areas that needed attention and made suggestions for improvements in those areas.

Management Comments. We issued a draft of this report on August 11, 2006. No written response to this report was required, and none was received.

Table of Contents

Executive Summary i

Background 1

Objective 1

Inspection Results for FY 2005

A. Army 2
B. Navy 5
C. Air Force 7
D. Missile Defense Agency 7

Appendixes

A. Scope and Methodology 9
B. List of Facilities Inspected 10
C. Memorandum of Understanding 11
D. Report Distribution 15

Background

In early 1999, then-Deputy Secretary of Defense, Dr. John Hamre 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, Dr. Hamre chartered an Overarching Integrated Process Team to better frame the recommendations and to oversee their implementation. From February 12 to May 12, 2000, Dr. Hamre and his successor, Mr. Rudy DeLeon, signed a total of 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, Dr. Hamre signed a memorandum requesting that the DoD Office of Inspector General ensure that a uniform system of periodic reviews, through the existing agency and Service inspection processes, be performed for compliance with directives concerning security, technology protection, and counterintelligence practices. These reviews were to assist with the protection of the technology-dependent cutting edge of U.S. weapon systems. The memorandum also requested that the Office of Inspector General develop inspection list guidelines for Department-wide 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 security, technology protection, and counterintelligence inspections.

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

On February 28, 2006, the Office of the Deputy Inspector for Intelligence issued revised inspection guidelines, “Inspection Guidelines for DoD Research and Technology Protection, Security and Counterintelligence for 2006,” Report No. O6-INTEL-03.

Objective

The overall objective was to consolidate and report the inspection results and best practices of participating inspectors general. See Appendix A for a discussion of the scope and methodology.

A. Army

During FY 2005, representatives from the Army Office of the Inspector General inspected 3 Contractor Owned-Contractor Operated and 10 Government Owned-Government Operated facilities out of 61 Army research, development, test, and evaluation facilities supporting Army programs. Specific aspects of Physical Security and Personnel Security were part of the six functional areas inspected. The inspections found weaknesses in information security and information assurance practices and that personnel were not trained in aspects of the physical security and personnel reliability program.

Personnel Security

No significant issues or trends.

Information Security

Information security controls specified in Army Regulation 380-5,"Information Security," September 29, 2000, presented challenges of noncompliance in five of seven facilities inspected. Improperly marked documents and a failure to conduct end-of-day security checks represented most of the shortcomings and may reflect poor understanding and retention of required security training. Additionally, a lack of established and tested emergency action plans failed to address organizational procedures to secure, safeguard, and preserve essential information files in the event of an incident requiring evacuation of facilities.

Information Assurance

Information assurance continues to present challenges to Army research, development, test, and evaluation facilities. Many of the issues associated with shortfalls in information security programs translate into similar noncompliance in the information technology sphere. Inspected organizations often relied on poorly thought out continuity of operations plans or lacked them altogether. This can represent a significant risk to the reestablishment of operations and reconstitution of data stored electronically in the event of damage to a facility and its equipment. Inspectors also observed problems with access controls and improperly applied protective measures such as passwords, anti-virus software updates, and Information Assurance Vulnerability Management. In some cases, the absence of an effective information assurance oversight structure, manned by qualified personnel as part of an integrated and synchronized team, contributed to the negative impact of these shortcomings.

Physical Security

Currently, no formalized training is offered to security specialists who are responsible for guarding chemical agents. Although the U.S. Army Military Police School does offer a physical security course, it does not cover the unique requirements associated with surety sites. Consequently, many of the Department of the Army civilian security specialists that are required to ensure the security of chemical sites are not adequately trained to perform their duties. This is a repeat finding. This condition will be exacerbated as biological research facilities that use select agents and toxins implement the new biological surety program. The following are some of the deficiencies noted during recent inspections, which an adequate training program could have prevented:

- Higher headquarters did not process required annual reviews of vulnerability assessments and physical security plans in a timely manner;

- Key Control Officers failed to properly document returned surety locks and keys.

- Key Control Officers failed to maintain surety key and lock chain accountability by allowing alternative Key Control Officers to concurrently perform receipt and issue activities.

- Key Control Officers failed to properly fill out Key Control Register and Inventory (DA Form 5513R) and Hand Receipt/Annex Number (DA Form 2062).

Operations Security

Many facility operations security programs lack rigor and detail in execution and are based on poorly articulated Essential Elements of Friendly Information. This lack is compounded by a failure to identify specific critical information requiring protection which, in turn, leads to generic operations security measures (countermeasures).

Personnel Reliability Program Training

As documented in the DoD Inspector General Draft Report, “The Nuclear Weapons Personnel Reliability Program,” May 7, 2004, and validated during recent inspections, the Services failed to establish formal training for the personnel reliability program. In many cases, this lack of formal training is producing Reviewing Officials, Certifying Officials, Surety Monitors, Surety Officers, and Competent Medical Authorities, who are not prepared to effectively execute their Personnel Reliability Program duties. Specifically, they failed to recognize and appropriately act upon potentially disqualifying information that would make individuals ineligible for the personnel reliability program.

Summary

Deficiencies in physical security include a repeat finding of a lack of a formal training program for security specialists who are responsible for guarding chemical agents. The Army had not made any improvements since inspectors first identified this problem. Initial vulnerability assessments did not include all of the buildings containing chemical surety materiel and required annual reviews of vulnerability assessments and physical security plans were either not performed or occurred out of sequence. Additionally, Key Control Officers failed to properly document returned surety locks and keys, maintain surety key and lock chain accountability by allowing alternative Key Control Officers to concurrently perform receipt and issue activities, and failed to properly fill out Key Control Register and Inventory (DA Form 5512R) and Hand Receipt/Annex Number (DA Form 2062). Because the Army did not establish formal training for the Personnel Reliability Program, many reviewing officials, certifying officials, surety monitors, surety officers, and competent medical authorities, are not prepared to effectively execute their Personnel Reliability Program duties. Specifically, they failed to recognize and appropriately act upon potentially disqualifying information that would make individuals ineligible for the Personnel Reliability Program.

B. Navy

Representatives from the Office of the Naval Inspector General inspected 7 of 31 Naval research, development, test, and evaluation facilities, and investigated multiple levels of security, technology protection, counterintelligence, and international security. Of the seven commands inspected, only two reported problems with overall security programs and processes, while a third noted deficiencies in information assurance. Both of the facilities with notable issues also reported that, in many cases, the same problems had been identified at least once on a prior review or inspection. Most installations reported opportunities for improvement, particularly in the areas of operations security, physical security, information security, information assurance, and antiterrorism/force protection. Of note, several of these topic areas were also cited in last year's summary report.

Security (General) and Physical Security

Several of the facilities inspected identified augmentation to guard force staff as a concern, which in some instances required the host command/installation to provide additional personnel or support to tenant research, development, test, and evaluation facilities. To better document these requirements, the Naval Inspector General supported establishing agreements, as needed, to better delineate security-related responsibilities between tenant research, development, test, and evaluation facilities and host commands/installations. Other improvements also reported as under consideration include the use of the appropriate levels of security lighting, along with adequate monitoring mechanisms and tools. Finally, the development and use of a threat matrix, or updated physical security plan, was recommended for several commands inspected during FY 2005.

Information Security and Information Assurance

Several facilities reported issues relating to information security. These issues ranged from varying levels of compliance with existing policies to the need for local facility personnel to have better program awareness. Accreditation of systems, and appropriate training were also identified as areas for improvement in the area of information assurance.

Antiterrorism/Force Protection

Several of the installations noted the need for an assigned antiterrorism/force protection officer, which could explain why the need for a current antiterrorism/force protection plan was also cited as a finding in some facility inspections. Also, at least one facility did not implement or use random antiterrorism measures.

Summary

Despite some concerns, the majority of inspected research, development, test, and evaluation facilities reported no significant deficiencies. Where unsatisfactory findings were identified, in most cases the inspectors observed that they had already been documented in earlier inspections. Constrained resources (e.g. funding and personnel) were a major contributing factor. In addition, although the impact was not explicitly stated in most inspection reports, continuing to operate with deficient security processes and procedures may contribute to an increased risk to information, assets, and personnel. Notwithstanding, a positive common theme was that, at most facilities, the security programs appeared to be well implemented and effectively managed. This theme is complementary to the revitalization observed last year in several security program areas (e.g. education, policy, and industrial security).

C. Air Force

Representatives from the Air Force Office of the Inspector General inspected 8 out of 76 Air Force research, development, test, and evaluation facilities. The units were meeting the intent of DoD and Air Force security and technology protection requirements and no significant systemic problems existed that would threaten program security.

D. Missile Defense Agency

Representatives from the Missile Defense Agency inspected the Joint National Integration Center, focusing on the overall management and control of personnel security for civilian and military personnel.

Personnel Security and Access Controls

Recent inspections noted the following deficiencies:

- While informal policies and procedures were in place, management, administration and personnel security controls needed improvement because written policies and procedures were lacking.
- An internal database used to manage the security clearance process was incomplete and inaccurate.

The following recommendations were made to enhance the personnel security program:

- Complete and publish personnel security guidance and procedures to improve the management and control of the personnel program and access controls.
    - Establish personnel security policy for classification sensitivity; initiate security investigations and reinvestigations, as needed; authorize appointment of persons to sensitive positions for a limited time; and grant interim clearances for Top Secret and Secret access to classified information;
    - Establish agency procedures for key activities such as access and suspension of access to various types of restricted information; interim clearances; position sensitivity upgrades; and personnel security database management; and
    - Assign personnel security program responsibilities.

- Develop and implement internal procedures to provide appropriate access and database reconciliation.
- Assess the adequacy of internal controls over personnel security during the annual review of internal controls.

Summary

While there were no significant findings, opportunities for improvement existed in the management, administration, and control over the personnel security and personnel out-processing programs.

Appendix A. Scope and Methodology

This report covers inspections of security, technology protection, and counterintelligence activities at DoD research, development, test and evaluation facilities conducted by or at the direction of the participating Inspectors General, as outlined in the memorandum of understanding at Appendix C. The participating Inspectors General prepare and forward to the DoD Office of Inspector General[1] lists of the research, development, test and evaluation facilities in their organizations that may be inspected. The DoD Office of Inspector General consolidates and distribute the lists to the participating Inspectors General, the Deputy Under Secretary of Defense for Laboratories and Basic Sciences, and the Director, Defense Operational Test and Evaluation. The Deputy Under Secretary of Defense for Laboratories and Basic Sciences and the Director, Defense Operational Test and Evaluation may recommend additional Defense agency facilities that should be inspected.

Participating Inspectors General inspect or direct the inspection of the research, development, test and evaluation facilities of their respective organizations. The inspections are performed during inspection programs of the participating Inspectors General, to include, in the case of military Inspectors General, the inspection programs of their subordinate Inspectors General. By June of each year, the participating Inspectors General prepare and forward to the DoD Office of Inspector General lists of the facilities that will be inspected during the following fiscal year. The DoD Office of Inspector General consolidates and distributes the lists to the participating Inspectors General. To ensure uniformity and consistency of inspections, the participating Inspectors General coordinate modifications of the inspection guidelines. The participating Inspectors General conducting or directing inspections ensure that inspection findings and recommendations are addressed and implemented.

The participating Inspectors General use their own procedures to write findings and recommendations within their respective areas of responsibility. The participating Inspectors General prepare and forward any significant findings and recommendations upon the conclusion of each inspection to the DoD Office of Inspector General. The DoD Office of the Inspector General distributes significant findings, as appropriate, and in coordination with the other participating Inspectors General, develops this overarching report.

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

Appendix B. List of Facilities Inspected

Army

1. Army Research Laboratories-Cleveland, Cleveland, Ohio
2. Battelle Hazardous Material Research Center, Columbus, Ohio
3. Battelle Medical Research and Evaluation Facility, Columbus, Ohio
4. Communications-Electronics Research Development and Experimentation Center, Fort Monmouth, New Jersey
5. Dugway Proving Ground, Dugway, Utah
6. Engineering Research and Development Center, Alexandria, Virginia
7. Medical Research Institute of Infectious Diseases, Fort Detrick, Maryland
8. Missile Defense and Space Technology Center, Huntsville, Alabama
9. Night Vision Electronic Sensors Directorate, Fort Belvoir, Virginia
10. Redstone Technical Test Center, Huntsville, Alabama
11. Southwest Research Institute, San Antonio, Texas
12. Tank-Automotive Research Development and Experimentation Center, Warren, Michigan
13. Topographic Engineering Center, Fort Belvoir, Virginia

Navy

1. Naval Explosive Ordnance Disposal Technology Division, Indian Head, Maryland
2. Naval Research Laboratory, Washington, District of Columbia
3. Naval Sea Systems Command, Washington Navy Yard, District of Columbia
4. Naval Surface Warfare Center, Carderock Division, West Bethesda, Maryland
5. Naval Surface Warfare Center, Indian Head Division, Indian Head, Maryland
6. Naval Surface Warfare Center, Panama City, Florida
7. Space and Naval Warfare Systems Center, Charleston, South Carolina

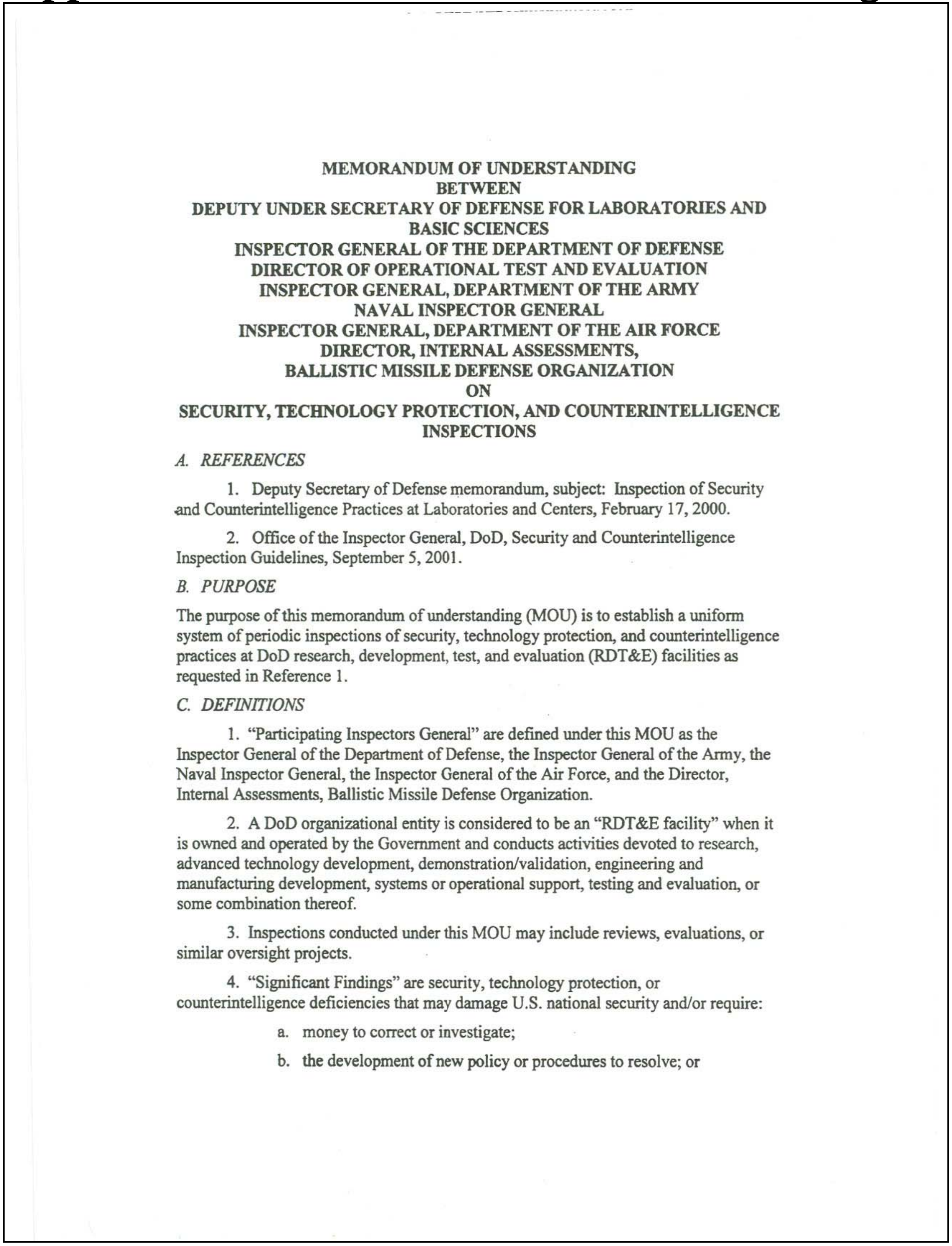
Air Force

1. Air Force Materiel Command, Arnold Engineering Development Center, Arnold Air Force Base, Tennessee
2. Air Force Materiel Command, Air Force Flight Test Center, Edwards Air Force Base, California
3. Air Force Materiel Command, Air Force Research Laboratory, Edwards Air Force Base, California
4. Air Force Materiel Command, Edwards Test Range, Edwards Air Force Base, California
5. Air Force Materiel Command, Air Force Research Laboratory, Kirtland Air Force Base, New Mexico
6. Air Force Materiel Command, Air Force Research Laboratory**,** Kirtland Air Force Base, New Mexico
7. Air Force Materiel Command, Warner-Robins Air Logistics Center, Warner-Robins Air Force Base, Georgia
8. Air Force Materiel Command, Air Force Research Laboratory Site, Warner-Robins Air Logistics Center, Warner-Robins Air Force Base, Georgia

Missile Defense Agency

Joint National Integration Center

Appendix C. 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.

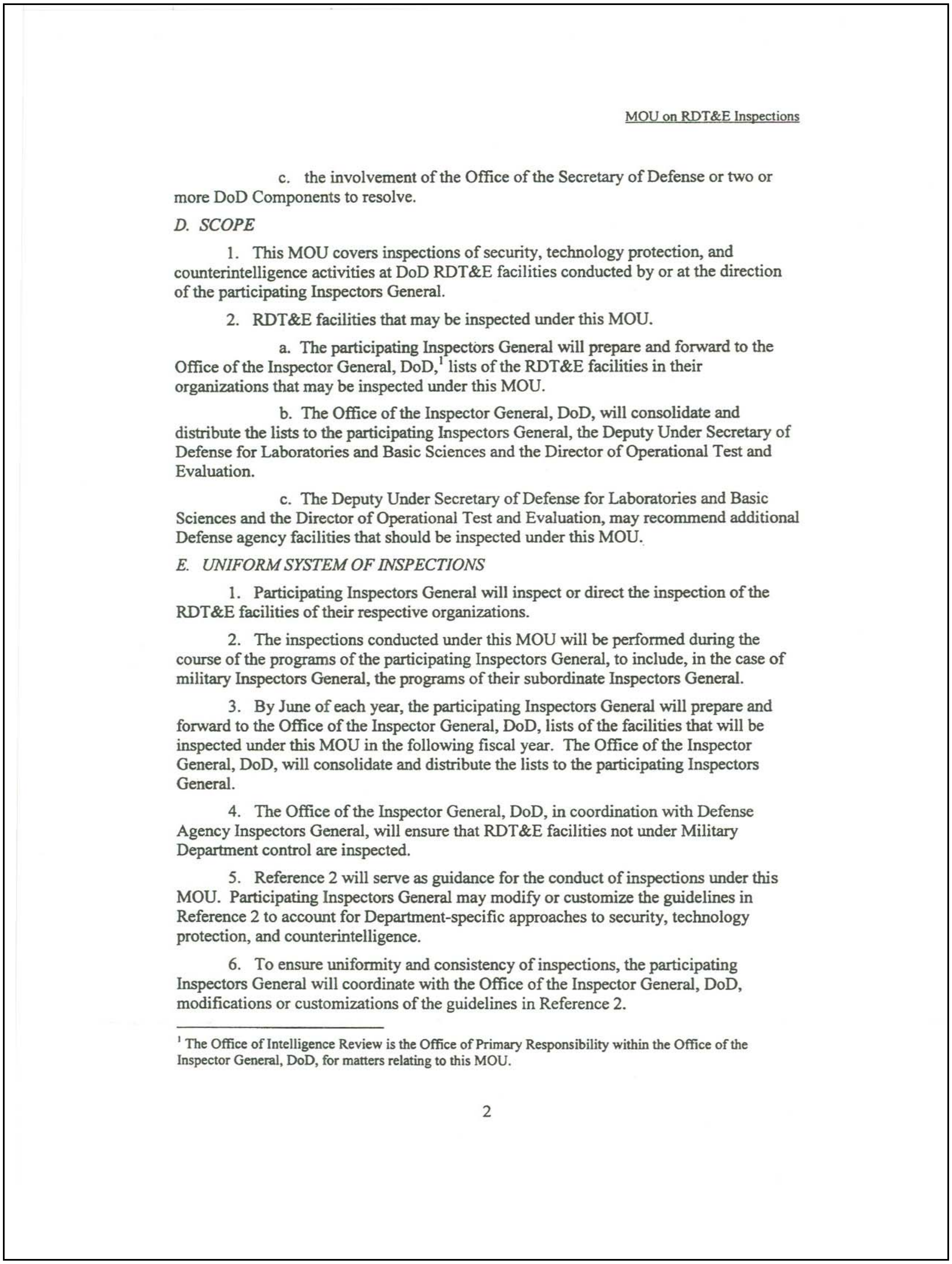
2. A DoD organizational entity is considered to be an "RDT&E facility" when it is owned and operated by the Government and conducts activities devoted to research, advanced technology development, demonstration/validation, engineering and manufacturing development, systems or operational support, testing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

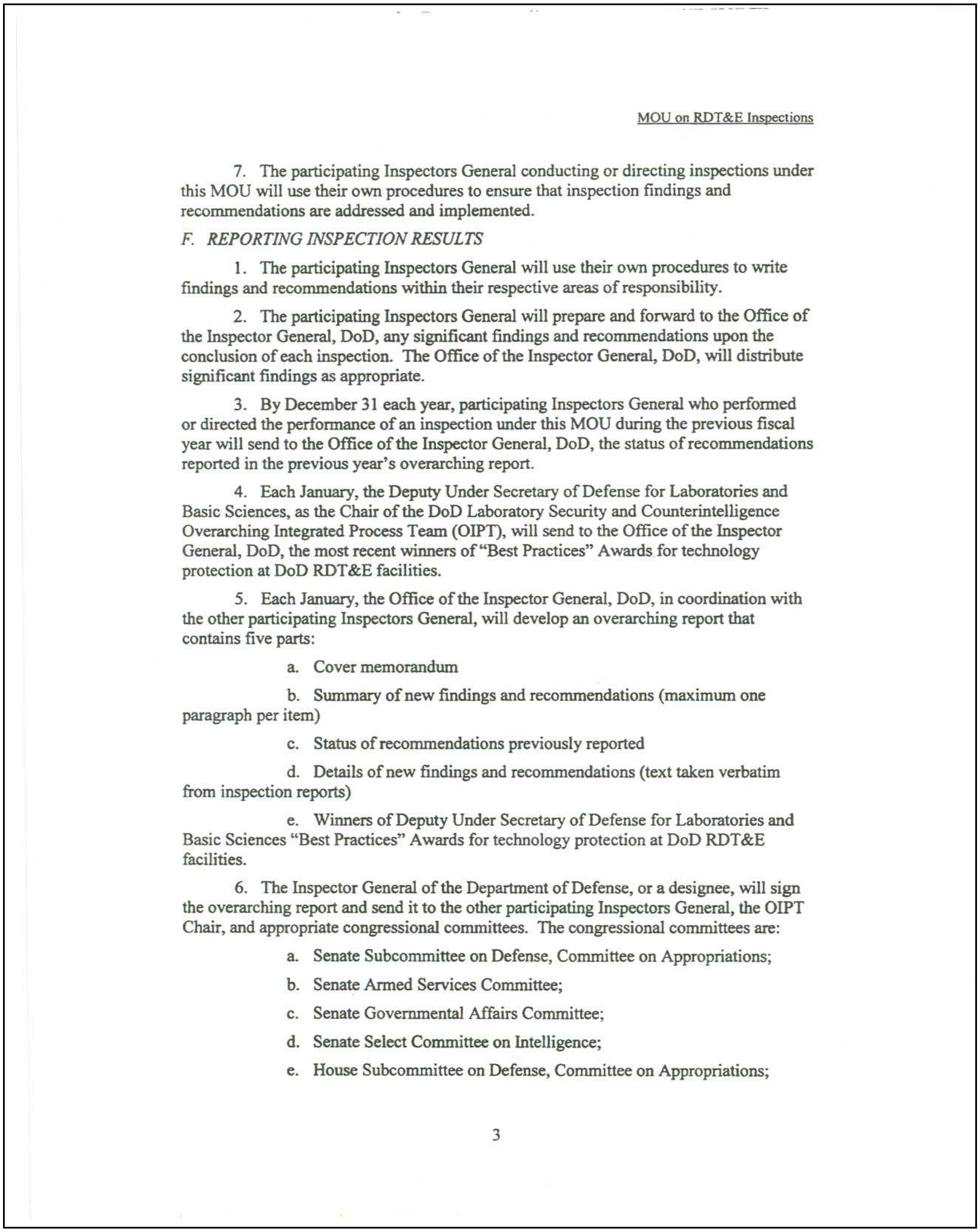
3. By June of each year, the participating Inspectors General will prepare and forward to the Office of the Inspector General, DoD, lists of the facilities that will be inspected under this MOU in the following fiscal year. The Office of the Inspector General, DoD, will consolidate and distribute the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

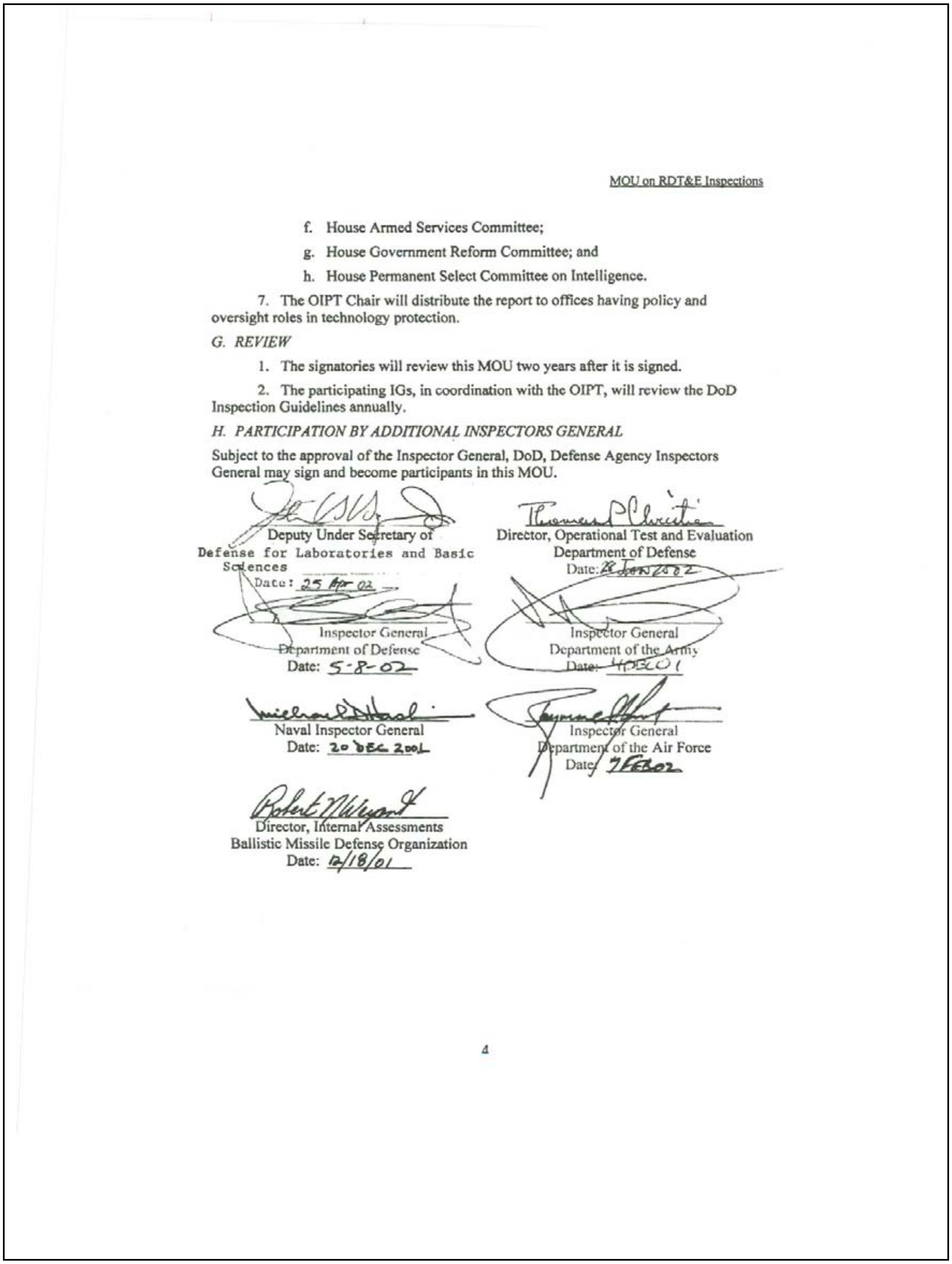
a. Senate Subcommittee on Defense, Committee on Appropriations;

b. Senate Armed Services Committee;

c. Senate Governmental Affairs Committee;

d. Senate Select Committee on Intelligence;

e. House Subcommittee on Defense, Committee on Appropriations;



MOU on RDT&E Inspections

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

Thomas P Christie
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: 4DEC01

Naval Inspector General
Date: 20 DEC 2001

Inspector General
Department of the Air Force
Date: 7FEB02

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

4

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Intelligence
Deputy Under Secretary of Defense for Laboratories and Basic Sciences*
Director, Defense Test Resource Management Center*

Department of the Army

Inspector General, Department of the Army*

Department of the Navy

Naval Inspector General*

Department of the Air Force

Inspector General, Department of the Air Force*

Other Defense Organizations

Director, Program Integration, Internal Management Review, Missile Defense Agency*

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Select Committee on Intelligence
Senate Committee on Governmental Affairs
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Permanent Select Committee on Intelligence
House Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

* Recipient of draft report.

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