



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

Ref: 10-00251-F

DEC 20 2010

OCCL

Steven Aftergood  
Federation of American Scientists  
1725 DeSales Street, NW  
Suite 600  
Washington, D.C. 20036


Dear Mr. Aftergood:

This is in response to your Freedom of Information Act (FOIA) request dated, June 02, 2010. You are seeking a copy of the following reports: 10-INTEL-0, 16 April 2010 and 10-INTEL-06, 21 May 2010. Your request was received in this office on June 03, 2010, and assigned case number 10-00251-F.

The enclosed documents are responsive to your request. However, I am withholding portions of the documents pursuant to Exemptions 2, 6 and 7(C) of the FOIA, specifically, 5 U.S.C. § 552(b)(2), which pertains to the internal rules and practices of the agency and would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission; 5 U.S.C. § 552(b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy; and 5 U.S.C. § 552(b)(7)(C), which pertains to information compiled for law enforcement purposes, the release of which could reasonably be expected to constitute an unwarranted invasion of the personal privacy of third parties.

If you are not satisfied with this action, you may submit an administrative appeal to Mr. John R. Crane, Assistant Inspector General, Office of Communications and Congressional Liaison, Room 1021, 400 Army Navy Drive, Arlington, VA 22202-4704. Your appeal should be postmarked within 60 days of the date of this letter, should cite to case number 10-000251-F, and should be clearly marked "Freedom of Information Act Appeal."

Sincerely,

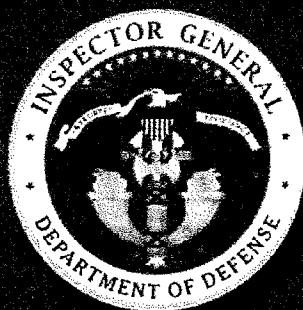
  
Jeanne Miller  
Chief, Freedom of Information and  
Privacy Office

Enclosures:  
As stated

10-INTEL-06  
May 21, 2010

# Inspector General

United States  
Department of Defense



## DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

**Summary Report of FY 2009 Inspections on  
Security, Technology Protection, and  
Counterintelligence Practices at DoD Research,  
Development, Test, and Evaluation Facilities**

**FOR OFFICIAL USE ONLY**

## **Additional Information and Copies**

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

## **Suggestions for Future Audits and Evaluations**

To suggest ideas for, or to request future audits and 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

DEPARTMENT OF DEFENSE

**hotline**

**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.mil](mailto:hotline@dodig.mil) [www.dodig.mil/hotline](http://www.dodig.mil/hotline)

~~FOR OFFICIAL USE ONLY~~



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

MAY 21 2010

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

We are providing report for your information and use. We issued a draft of this report on March 19, 2010. No written response to this report was required and none was received. Therefore, we are publishing this report in final form.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8800 (DSN 664-8800).

A handwritten signature in black ink, reading "Patricia A. Brannin".

Patricia A. Brannin  
Deputy Inspector General  
for Intelligence

~~FOR OFFICIAL USE ONLY~~

DISTRIBUTION:

OFFICE OF THE SECRETARY OF DEFENSE

Under Secretary of Defense for Acquisition, Technology, and Logistics  
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

NON-DEFENSE ORGANIZATIONS

Office of Management and Budget

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 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

~~FOR OFFICIAL USE ONLY~~



# Results in Brief: Summary Report of FY 2009 Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test, and Evaluation Facilities

## What Was Done

This report provides summaries of inspection results from the Service Inspectors General and, where available, notes the best practices identified by participating Inspectors General. The Service Inspectors General selected 37 of the 121 research, development, test, and evaluation facilities under their purview for inspection. These annual inspections provide a uniform system of periodic reviews for compliance with directives concerning security, technology protection, and counterintelligence practices. See Appendix A for a discussion of the scope and methodology.

## What Was Found

The Service Inspectors General identified some consistent trends across the Services. They also identified several areas that needed attention and made suggestions for improvements in those areas.

These reports revealed consistent trends across the Services specifically related to information assurance and physical security. For example, all Services identified compliance issues related to information assurance, specifically in the areas of verification, accreditation, and certification. The Army identified laptops that lacked current information assurance vulnerability management updates. The Navy noted firewall, system accreditation and information assurance technician certification issues at some laboratories. The Air Force identified a unit wherein 125 members opened an e-mail attachment from an unknown source leaving the network vulnerable to exploitation and attack.

The Services also identified physical security deficiencies at various commands. The Army expressed particular concern regarding the oversight and management of security guard training programs; noting the impermanence of the security forces due to constant contract turnover. The Navy noted deficiencies where commands only provided security personnel with on the job training and assigned security as a collateral duty. The Air Force identified a repeat physical security deficiency noted in an earlier inspection, which left the command vulnerable to access by unverified personnel. In all cases, adequate resources and training were identified as security needs.

The Service Inspectors General also identified several areas of improvement in areas identified in past reports, during the course of their inspections. The Army noted significant improvements in all biological surety related functional areas, especially in the areas of inventory management and accountability. The Navy identified some units that made notable improvements in their information assurance programs – attributing this success to the hiring of quality, trained personnel. The Navy also noted security professionals embedded in some of its programs as a best practice. The Air Force noted that the majority of inspected facilities were in compliance with industrial security program standards with only one unit exhibiting deficiencies.

In general, the Service Inspectors General inspections positively affected the overall readiness of research, development, test, and evaluation facilities by identifying weaknesses – both minor and substantial. Where deficiencies were found, command leadership was engaged to take corrective steps. As a consequence, inspection findings resulted in significant programmatic improvements across the board.

# Table of Contents

<b>Introduction</b>	<b>1</b>
Objective .....	1
Background .....	1
<b>A. Army Inspection Results for FY 2009</b> .....	<b>2</b>
Personnel Security .....	2
Information Security .....	2
Communications Security .....	3
Information Assurance .....	3
Physical Security .....	3
Operations Security .....	4
Industrial Security .....	4
Continuity of Operations Plan .....	4
Foreign Disclosure .....	4
Biological Surety .....	5
Chemical Surety and Safety .....	5
Summary .....	6
<b>B. Navy Inspection Results for FY 2009</b> .....	<b>7</b>
General and Physical Security .....	7
Information Assurance .....	7
Research and Technology Protection .....	8
Counterintelligence .....	8
International Security .....	8
Best Practice .....	8
Summary .....	9
<b>C. Air Force Inspection Results for FY 2009</b> .....	<b>10</b>
General Security .....	10
Physical Security .....	10
Personnel Security .....	10
Information Security .....	11
Information Assurance .....	11
Operations Security .....	11
Industrial Security .....	12
Security Education .....	12

~~FOR OFFICIAL USE ONLY~~

Security/Counterintelligence Support for Acquisition Systems .....	12
Summary .....	13

## **Appendices**

A. Scope and Methodology.....	14
B. List of Facilities Inspected. ....	15
C. Memorandum of Understanding .....	17

~~FOR OFFICIAL USE ONLY~~



# Introduction

## Objective

The overall objective was to consolidate and report the inspection results and best practices of participating Inspectors General who inspect counterintelligence, security, and technology protection practices at research, development, test, and evaluation facilities. The scope and methodology of this effort are detailed in Appendix A.

## 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. No major problems were identified. As a result of these efforts, the Deputy Secretary of Defense chartered an Overarching Integrated Process Team to better frame the recommendations and to oversee their implementation. From February 12 to May 12, 2000, the Deputy Secretary of Defense signed a total of 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 of Defense signed a memorandum requesting that the DoD Office of the Inspector General ensure that a uniform system of periodic reviews, through the existing agency and Service inspection processes, for compliance with directives concerning security, technology protection, and counterintelligence practices was implemented. 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 DoD Office of Inspector General develop inspection list guidelines for Department-wide Inspectors General to enhance consistency of the inspections.

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 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 Inspector General annually issues this summary report of inspections of security, technology protection, and counterintelligence practices at DoD research, development, test, and evaluation facilities.

~~FOR OFFICIAL USE ONLY~~

## **A. Army Inspection Results for FY 2009**

During FY 2009, representatives from the Department of the Army's Inspector General inspected 11 out of 30 Army research, development test and evaluation facilities supporting Army programs and conducted assistance visits at four others. The inspections centered on counterintelligence practices, security, technology protection, personnel reliability, accountability, surety, and safety at research, development, test, and evaluation facilities.

### **Personnel Security**

Although there were no significant trends within the area of personnel security, issues were identified at two facilities. At the first facility, the organization's guard force training files/certifications were incomplete and inaccessible because the organization did not have clear procedures or written and defined standards. Furthermore, inspectors found that the second organization was not using electronic questionnaires for personnel security investigations processing because the facility did not have Joint Personnel Adjudication System authorization. In essence, the facility had not switched to electronic questionnaires for personnel security investigations processing because there was no penalty for not doing so.

### **Information Security**

Classification marking requirements remain a problem at Army laboratories. The most common issues are a lack of declassification instructions, as well as failures to mark classified folders, media, and working papers properly. The proper classification marking requirements for information systems media and documents as required by regulation were found as issues at three Army laboratory locations. In addition, Standard Forms 700 (Security Container Information) and 702 (Security Container Check Sheet) were not always properly annotated, and safe combinations were not consistently changed. Annual security education also posed a challenge for two inspected laboratories. For example, although annual training statistics were typically adequate, inspectors observed that the required content as outlined in Army Regulation 380-5, "Department of the Army Information Security Program," September 29, 2000, was missing from the training slides and on a few occasions, the training was given on a "read and initial" basis.

~~FOR OFFICIAL USE ONLY~~

## Communications Security

One Army laboratory communications security program did not have documentation to support communications security requirements such as a trained hand receipt holder, inspections, inventories, procedures and emergency measures in accordance with Technical Bulletin 308-41, "Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material," July 1, 1981.

## Information Assurance

Security and information assurance inspectors observed a small improvement in this area, relative to the past two years, and they expect incrementally better performance in the next FY series of inspections. [REDACTED]

[REDACTED] However, overall data at rest compliance is improving relative to last year. The use of portable electronic devices in areas where classified information is discussed continues to be a problem for one-third of the Army laboratories inspected.

## Physical Security

Three laboratories had issues in the area of [REDACTED] and two facilities had issues with the [REDACTED].

---

<sup>1</sup> Data-at-rest is the term used to describe all data in storage but excludes any data that frequently traverses the network or that which resides in temporary memory. Data at rest includes but is not limited to archived data, data which is not accessed or changed frequently, files stored on hard drives, USB thumb drives, files stored on backup tape and disks, and also files stored off-site or on a storage area network.

b(2)

~~FOR OFFICIAL USE ONLY~~

Oversight and management of security guard training programs remains a concern based on numerous issues identified during inspections. Turbulence in the security forces caused by constant contract turnover has contributed to this. Both contractor and facility leadership should employ effective oversight to include frequent checking of documentation to verify that contract requirements are being met. These actions would prevent a majority of the recurring deficiencies. The conversion to a Department of the Army civilian guard force mandates that the leadership develop an effective oversight program to ensure compliance with security requirements as the transition continues.

## **Operations Security**

In addition to one facility not having an operations security program, or a trained operations security officer as required by Army Regulation 530-1, "Operations Security (OPSEC)," April 19, 2007, inspectors encountered two Army laboratories where employees displayed inadequate knowledge of their organization's essential elements of friendly information. The inspectors also noted that facility operations security plans at two facilities required refinement and better linkages with respect to each of the organization's mission essential functions and stated critical information and essential elements of friendly information. Overall, however, inspectors observed that the vast majority of Army facilities' operations security officers are doing a better job at creating and distributing localized operations security graphic training aids to employees to keep at their desks; thus, providing good continuous operations security awareness education.

## **Industrial Security**

The inspectors noted that in limited instances, DD Forms 254, "Department of Defense Contract Security Classification Specification," December 1999, did not include the applicable security references required for the classified contract/performance of work. A positive trend is that the overwhelming majority of DD Forms 254 are being reviewed and signed by the user agency, the requiring activity, and the cognizant security authority.

## **Continuity of Operations Plan**

Five Army laboratories inspected did not have a finalized continuity of operations plan. These facilities failed to have a sufficiently detailed, resourced and tested organizational continuity of operations plan. This failure was primarily due to a lack of understanding that their respective facilities required individual continuity of operations plans; and a lack of resources, specifically time and personnel.

## **Foreign Disclosure**

No significant issues or trends.

~~FOR OFFICIAL USE ONLY~~

## **Biological Surety**

Significant improvements were noted in all biological surety related functional areas, especially in the areas of inventory management and accountability. While continuing emphasis is still needed, the Army clearly has made great strides during the past year by strengthening biological surety policy and ensuring Army research, development, test, and evaluation facility compliance with the enhanced standards.

All biological facilities inspected this year had excellent overall safety programs and culture. Nevertheless, work remains to be done to bring biological safety related standard operating procedures into full compliance with the Army revised safety and biosafety requirements promulgated since 2007. Continued emphasis must be placed on ensuring that facility standard operating procedures are updated.

## **Chemical Surety and Safety**

Compliance inspections determined that chemical surety and safety operations sustained their level of performance. This can be attributed to the maturity of the chemical surety programs at Army facilities and the now routine internal and external compliance inspections and oversight.

Inspectors identified a weakness of particular concern at an Army laboratory related to the management of the chemical personnel reliability program. The inspection team addressed this issue with the site Commander during the visit. The Commander took immediate corrective action, and quickly implemented revised processes. The Department of the Army's Inspector General believes that the immediate leadership attention and emphasis demonstrated at facilities where program weaknesses were identified, is direct evidence of the seriousness with which the Army views surety programs.

Inspectors noted significant improvements in the management and accountability procedures related to non-traditional agents. While not characterized as surety materials, non-traditional agents have similar properties and require parallel safeguards. These improvements should be viewed as very positive steps. Overall, it is clear that the new procedures for accurate accountability and safe handling of non-traditional agents have improved. As a direct result of our inspections, both Office of the Secretary of Defense and the Army have taken on the task of developing formal policy for non-traditional agents.

~~FOR OFFICIAL USE ONLY~~

## **Summary**

The development of a new Department of the Army Inspector's General follow-up methodology for inspections is expected to enhance overall compliance among Army research, development, test, and evaluation facilities. In addition, proactive security measures are underway to ensure that appropriate attention is placed on research and technology protection within the areas of protecting critical program information and developing laboratory counterintelligence support plans.

Over the last year, the Army has seen improvements at some of their sites and has made several policy recommendations that have been adopted as policy. Army inspectors found no significant deficiencies suggesting systemic issues threatening program security. However, inspectors did find issues and trends that demonstrate facilities are assuming risks that merit attention and impact the overall readiness of the Army's research, development, test, and evaluation facilities. As they continue their inspections of research, development, test, and evaluation facilities during FY 2010, they will continue to measure organizational compliance and monitor continuous improvements.

~~FOR OFFICIAL USE ONLY~~

## B. Navy Inspection Results for FY 2009

Inspections were conducted at nine of 32 identified Navy research, development, test, and evaluation facilities during FY 2009. The inspections covered the following areas: security, information assurance, research and technology protection, counterintelligence, and international security. The overall findings indicated that the commands are generally in compliance with DoD and Department of the Navy requirements in these areas.

### General and Physical Security

Generally, the commands' security programs complied with regulations. [REDACTED]. Operations security programs, however, continue to be a noted concern at Navy laboratories. There was a discernible correlation between identified strong security and operations security programs and a command's decision to invest in training security personnel and to provide personnel with the authority and resources to do their jobs. This contrasted positively with commands that only provided personnel with on the job training and assigned command security as a collateral duty.

### Information Assurance

[REDACTED] Since FY 2006, information assurance has been identified as an area requiring increased emphasis and funding. As laboratories align with the Navy-Marine Corps Intranet infrastructure, they are more likely to be in compliance with regulations and standards, and enjoy a concomitant strengthening of their information assurance posture. Many of the laboratories, however, are still not aligned with the Navy-Marine Corps Intranet. [REDACTED]

[REDACTED] Some units made significant improvements in their programs. These improvements were attributed to the hiring of quality, trained personnel.

## **Research and Technology Protection**

The Naval Criminal Investigative Service has moved forward at most Navy laboratories to establish comprehensive counterintelligence support plans where critical program information has been identified. [REDACTED]

[REDACTED] One command was noted to have no formal research and technology protection program, and was unable to show compliance with research and technology protection policies and acquisition policies for research and technology protection. Of note, there was only one resident Naval Criminal Investigative Service agent at that command.

## **Counterintelligence**

All installations were determined to be in satisfactory compliance with counterintelligence requirements. As with everything else discussed, a common complaint was that there were insufficient numbers of Naval Criminal Investigative Service agents to address the demands of the counterintelligence mission.

## **International Security**

All installations were determined to be in satisfactory compliance with international security requirements.

## **Best Practice**

One command had a top-notch research and technology strategy because of its comprehensive approach in educating and assisting program managers with critical program information identification. The various command programs have fully integrated and funded security representatives who proactively track, review, and assist throughout the research and development process. This smart move to use security professionals in the programs has greatly contributed to the success of reaching developmental milestones. Where applicable, it is highly recommended that other commands employ this approach to mitigate program security shortfalls and meet mission goals in a timely manner.

~~FOR OFFICIAL USE ONLY~~



## **Summary**

The results of the FY 2009 and earlier inspections indicate an inconsistent adherence to DoD/Navy directives across the board. The problem usually stems from insufficient resources allocated to security and especially to information assurance, a branch of exponentially increasing complexity. Although some of the deficiencies noted were significant, they are being resolved and should not suggest systemic problems that directly threaten program security. In fact, one command fully integrated and funded security representatives who proactively track, review, and assist throughout the research and development process. Security professionals embedded in the programs have greatly contributed to the success of reaching developmental milestones. Where applicable, it is highly recommended that other commands employ this approach to mitigate program security shortfalls and meet mission goals in a timely manner.

~~FOR OFFICIAL USE ONLY~~

## **C. Air Force Inspection Results for FY 2009**

Air Force major command Inspectors General teams inspected 17 of 59 Air Force research, development, test, and evaluation facilities on multiple levels of security, research and technology protection, and counterintelligence in accordance with DoD Inspector General's security and counterintelligence inspection guidelines.

### **General Security**

Four inspected units experienced general security deficiencies. These deficiencies included failing to conduct periodic reviews of force protection guidance to ensure program currency, faulty entry control procedures into a unit's command post, substandard performance within a unit's standardization and evaluation section, and a unit's poor management of classified documents (to include North Atlantic Treaty Organization classified). In all cases, re-training, re-emphasis, and leadership involvement were prescribed to resolve the program deficiencies.

### **Physical Security**

Two units showed physical security deficiencies that were immediately triaged, but will require a permanent solution. At one Air Force Space Command unit, a [REDACTED] and a ground level [REDACTED] were unmanned; allowing unverified [REDACTED] to the installation. As this issue was also identified during a 2007 compliance inspection, the repeat deficiency was a matter of particular concern. Air Force Materiel Command identified a unit that did not provide adequate personnel, equipment, and facilities for protection level resources, no security camera coverage of the installation entry control points or of the flight line. This situation is also being resourced for a permanent solution.

### **Personnel Security**

Air Force Materiel Command identified a unit whose installation security program manager was not meeting program requirements. Some security information files were not forwarded to the Air Force central adjudication facility within 120 days; not all sub-contractors performing work on classified contracts acknowledged the visitor group security agreements in writing; and the manager did not provide adequate training in order to prevent the unauthorized reproduction of classified information. The unit commander and Air Force Materiel Command's security forces division are implementing corrective actions.

~~FOR OFFICIAL USE ONLY~~

## **Information Security**

Air Force Materiel Command identified that a unit's network operations and security center did not ensure a time compliance network order was implemented on the appropriate proxy servers; potentially allowing unauthorized files to enter the base network servers. At an Air Force Space Command location, personnel did not mark all computers and equipment with the appropriate classification level labels and did not develop plans for the protection, removal, or destruction of classified material in case of an emergency. At another location, the communications security responsible officer did not execute an effective communications security inventory program; identifying instances where inventories were not conducted after safes were accessed. In all cases, unit leadership was quickly engaged and major command functional assistance offered to resolve the deficiencies.

## **Information Assurance**

Four units experienced deficiencies within the information assurance category. At one unit, the communications and information systems officer did not implement a voice systems security program that addresses all aspects of security and information assurance practices. At another, the communications group chief information officer did not ensure all automated information systems were certified and accredited using the DoD information technology security classification and accreditation process/DoD information assurance certification and accreditation process prior to operation. One unit required attention brought to its emission security assessment program; specifically, the need for more fidelity in those assessments. Finally, a unit failed to take appropriate actions when presented with an e-mail from an unknown source, wherein 125 members opened an e-mail attachment which left the network vulnerable to exploitation and attack. Re-training, re-emphasis and leadership involvement were prescribed to resolve these information assurance deficiencies.

## **Operations Security**

Ensuring operations security integration into day-to-day and contingency operations was an issue at two units during this inspection cycle. A unit did not ensure end-of-day security checks were conducted at some of their [REDACTED] and did not ensure personnel were checked for unauthorized material prior to entering and exiting a [REDACTED]. Another unit required better management of the operations security program in general. Continuity binders were missing training certificates, not in correct sequence, and missing other required items.

~~FOR OFFICIAL USE ONLY~~

## **Industrial Security**

Air Force Space Command inspectors identified only one unit in need of a more effective industrial security program. Beginning with the unit failing to maintain a current listing of all on-base visitor group management officials or security representatives and failing to maintain a current listing of all on-base visitor group management officials or security representatives, this lack of effective program management manifested itself into other deficiencies as well. All other inspected units within Space Command and those inspected by Air Force Materiel Command were in compliance with industrial security program standards.

## **Security Education**

Seven units experienced deficiencies within the security education category, which is the largest focus area for the Air Force this inspection cycle. In nearly every case, the communications and information systems officers either did not develop training materials, conduct training, or document training for unit customers/users. In units where training was conducted, recurring or refresher training was not always provided to ensure awareness of applicable security requirements. In all cases, unit leadership was quickly engaged and major command functional assistance offered to resolve the deficiencies.

## **Security/Counterintelligence Support for Acquisition Systems**

Five units experienced reportable deficiencies related to the acquisition program. At one Air Force Materiel Command unit, four program managers did not ensure all required elements were addressed in the program protection plan. More specifically, they did not break out cost by security disciplines; did not create nor implement a system specific critical program information training program to inform appropriate program personnel of the efforts, procedures, and methods to protect its critical program information; did not establish a formal charter with the documentation of members; and critical program information countermeasures did not address specific vulnerabilities nor were they event- or time-phased.

Within a Space Command unit, it was discovered that the wing failed to note the security requirements that their satellite operations center was to be protected as a protection [REDACTED]. Additionally, the wing failed to communicate this deficiency and the need for additional resources to meet this requirement with their owning command. In all cases, unit leadership was quickly engaged and major command functional assistance offered to resolve the deficiencies.

Air Force Materiel Command identified that one of their unit's program managers did not seek a current counterintelligence support plan. A corrective action plan was quickly implemented to resolve the deficiency.

## **Summary**

Major command Inspectors General teams critically inspected DoD and Air Force security and technology protection requirements within 17 facilities this cycle. Although discrepancies were identified during inspections, no systemic problems were identified that would threaten program security. Where unsatisfactory findings were identified, resolution plans are either already in place or in progress to resolve critical issues.

~~FOR OFFICIAL USE ONLY~~

## 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. Each year, the participating Inspectors General prepare and forward to the DoD Office of Inspector General<sup>2</sup> lists of the research, development, test and evaluation facilities within their organizations subject to inspection. The Air Force did not include their inspection schedule to facilitate no-notice inspections. The DoD Office of Inspector General consolidates and distributes the lists to the participating Inspectors General, the Deputy Under Secretary of Defense for Laboratories and Basic Sciences, and the Director, Defense Test Resource Management Center. The Deputy Under Secretary of Defense for Laboratories and Basic Sciences, and the Director, Defense Test Resource Management Center may recommend additional Defense agency facilities for inspection.

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 the course of the inspection programs of the participating Inspectors General, to include, in the case of military Inspectors General, the inspection programs of their subordinate Inspectors General. To ensure uniformity and consistency of inspections, the participating Inspectors General coordinate modifications or customizations 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 Inspector General, in coordination with the other participating Inspectors General, develops this overarching report.

---

<sup>2</sup> 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 research and technology protection practices at research, development, test and evaluation facilities.

## **Appendix B. List of Facilities Inspected**

### **A. Army Research, Development, Test and Evaluation Facilities Inspected During FY 2009**

1. Army Research Laboratory, Aberdeen Proving Ground, MD
2. Dugway Proving Grounds, Dugway, UT
3. Edgewood Chemical Biological Center, Aberdeen Proving
4. Engineering Research and Development Center, Vicksburg, MS
5. Medical Research and Materiel Command, Fort Detrick, MD
6. Medical Research Institute of Chemical Defense, Aberdeen Proving Ground, MD
7. Research, Development and Engineering Command, Aberdeen Proving
8. Reagan Test Center, U.S. Army Kwajalein Atoll
9. U.S. Army Medical Research Institute of Infectious Diseases, Fort Detrick, MD
10. Walter Reed Army Institute of Research, Forest Glen, MD
11. White Sands Test Center, White Sands, NM

### **B. Navy Research, Development, Test and Evaluation Facilities Inspected During FY 2009**

1. Corona Division, Naval Surface Warfare Center, Corona, CA
2. Naval Air Systems Command, Patuxent River, MD
3. Naval Air Warfare Center Aircraft Division, Patuxent River, MD
4. Naval Air Warfare Center Aircraft Division, Lakehurst, NJ
5. Naval Air Warfare Center Aircraft Division, St. Inigoes, MD.
6. Naval Ordnance Safety and Security Activity, Indian Head, MD
7. Naval Undersea Warfare Center Division, Newport, RI
8. Naval Undersea Warfare Center Division, Keyport, W A
9. Space and Naval Warfare Systems Center Atlantic, Charleston, SC

### **C. Air Force Research, Development, Test and Evaluation Facilities Inspected During FY 2009**

1. Air Force Materiel Command, Aeronautical Systems Center, Wright-Patterson Air Force Base, OH
2. Air Force Materiel Command, Aerospace Maintenance and Regeneration Center, Davis-Monthan Air Force Base, AZ
3. Air Force Materiel Command, Air Armament Center, Eglin Air Force Base, FL
4. Air Force Materiel Command, Air Force Flight Test Center, Edwards Air Force Base, CA

~~FOR OFFICIAL USE ONLY~~

5. Air Force Materiel Command, Air Force Nuclear Weapons Center Kirtland Air Force Base, NM
6. Air Force Materiel Command, Air Force Research Laboratory, Hanscom Air Force Base, MA
7. Air Force Materiel Command, Air Force Research Laboratory/Directed Energy Directorate, Kirtland Air Force Base, NM
8. Air Force Materiel Command, Air Force Research Laboratory/Propulsion Directorate, Edwards Air Force Base, CA
9. Air Force Materiel Command, Air Force Research Laboratory/Sensors Directorate, Hanscom Air Force Base, MA
10. Air Force Materiel Command, Air Force Research Laboratory/Space Vehicles Directorate, Hanscom Air Force Base, MA
11. Air Force Materiel Command, Air Force Research Laboratory/Space Vehicles Directorate, Kirtland Air Force Base, NM
12. Air Force Materiel Command, Electronic Systems Center, Hanscom Air Force Base, MA
13. Air Force Materiel Command, Ogden Air Logistics Center, Hill Air Force Base, UT
14. Air Force Space Command, Space and Missile System Center site, Kirtland Air Force Base, NM
15. Air Force Space Command, Space and Missile System Center site, Los Angeles Air Force Base, CA
16. Air Force Space Command, Space and Missile System Center site, Patrick Air Force Base, FL
17. Air Force Space Command, Space and Missile System Center, Rapid Reaction Squadron, Peterson Air Force Base, CO

~~FOR OFFICIAL USE ONLY~~



# 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

~~FOR OFFICIAL USE ONLY~~

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,<sup>1</sup> 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.

<sup>1</sup> The Office of Intelligence Review is the Office of Primary Responsibility within the Office of the Inspector General, DoD, for matters relating to this MOU.

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

*F. REPORTING INSPECTION RESULTS*

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

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

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

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

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

- a. Cover memorandum
- b. Summary of new findings and recommendations (maximum one paragraph per item)
- c. Status of recommendations previously reported
- d. Details of new findings and recommendations (text taken verbatim from inspection reports)
- e. Winners of Deputy Under Secretary of Defense for Laboratories and Basic Sciences "Best Practices" Awards for technology protection at DoD RDT&E facilities.

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

- a. Senate Subcommittee on Defense, Committee on Appropriations;
- b. Senate Armed Services Committee;
- c. Senate Governmental Affairs Committee;
- d. Senate Select Committee on Intelligence;
- e. House Subcommittee on Defense, Committee on Appropriations;

- f. House Armed Services Committee;
- g. House Government Reform Committee; and
- h. House Permanent Select Committee on Intelligence.


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

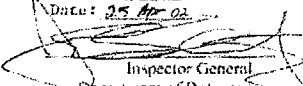
**G. REVIEW**

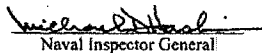
- 1. The signatories will review this MOU two years after it is signed.
- 2. The participating IGs, in coordination with the OIPT, will review the DoD Inspection Guidelines annually.

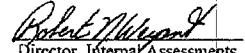
**H. PARTICIPATION BY ADDITIONAL INSPECTORS GENERAL**

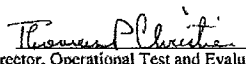
Subject to the approval of the Inspector General, DoD, Defense Agency Inspectors General may sign and become participants in this MOU.

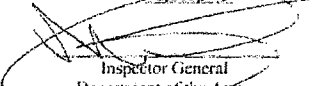
  
Deputy Under Secretary of  
Defense for Laboratories and Basic  
Sciences  
Date: 25 Apr 02

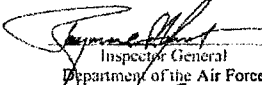
  
Inspector General  
Department of Defense  
Date: 5-8-02

  
Naval Inspector General  
Date: 20 DEC 2001

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

  
Director, Operational Test and Evaluation  
Department of Defense  
Date: 26 Jan 2002

  
Inspector General  
Department of the Army  
Date: 4-15-02

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



# Inspector General Department of Defense

**FOR OFFICIAL USE ONLY**