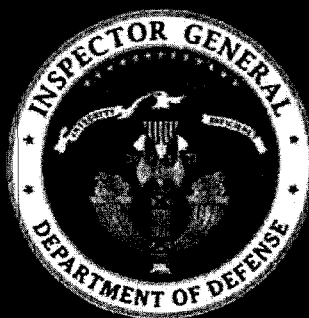


10-INTEL-09
August 6, 2010

Inspector General

United States
Department of Defense



DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

Assessment of Security Within the Department of Defense - Tracking and Measuring Security Costs

This document will not be released (in whole or in part) outside the Department of Defense without the prior written approval of the Inspector General of the Department of Defense.

FOR OFFICIAL USE ONLY

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for 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 www.dodig.mil/hotline

Acronyms and Abbreviations

IDA	Institute for Defense Analyses
ISOO	Information Security Oversight Office
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
USD(I)	Under Secretary of Defense for Intelligence

~~FOR OFFICIAL USE ONLY~~



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

August 6, 2010

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Assessment of Security Within the Department of Defense -
Tracking and Measuring Security Costs (Report No. 10-INTEL-09)

We are providing this report for your information and use. We issued a draft of this report on June 11, 2010. We considered comments from the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security in preparing the final report.

We appreciate the courtesies extended to the staff. Please direct questions to [REDACTED] at (703) 604-[REDACTED] (DSN 664-[REDACTED]) [REDACTED]@dodig.mil, or [REDACTED] at (703) 604-[REDACTED] (DSN 564-[REDACTED]) [REDACTED]@dodig.mil. If you desire, we will provide a formal briefing on the results.

Patricia A. Brannin
Deputy Inspector General
for Intelligence

~~FOR OFFICIAL USE ONLY~~

DISTRIBUTION:

OFFICE OF THE SECRETARY OF DEFENSE

Under Secretary of Defense (Acquisition, Technology, and Logistics)
Under Secretary of Defense (Policy)
Under Secretary of Defense (Intelligence)
Assistant Secretary of Defense (Networks and Information Integration)/
DoD Chief Information Officer
Deputy Under Secretary of Defense (HUMINT, Counterintelligence and Security)

DEPARTMENT OF THE ARMY

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

DEPARTMENT OF THE NAVY

Naval Inspector General
Auditor General, Department of the Navy

DEPARTMENT OF THE AIR FORCE

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

NON-DEFENSE ORGANIZATIONS

Office of Management and Budget

CONGRESSIONAL COMMITTEES AND SUBCOMMITTEES, CHAIRMAN AND RANKING

Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Select Committee on Intelligence
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Armed Services
House Permanent Select Committee on Intelligence
House Committee on Oversight and Government Reform
House Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform
House Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform



Results in Brief: Assessment of Security Within the Department of Defense - Tracking and Measuring Security Costs

What We Did

This is the first in a series of reports designed to provide an overall assessment of security policies and procedures within the Department. In this initial report, we address how the Department programs and tracks its security costs and measures the return on investment for security expenditures. We will address the classification and grading of security personnel, the process for the training, certification and professionalization, and the policies associated with these issue areas in subsequent reports.

What We Found

The process for determining the full scope and composition of tracking security resources is fragmentary; in part, because of the lack of an integrated security framework policy. DoD has policy with associated definitions for differing categories of security disciplines. However, because security spans the entire Department and touches all levels of command, implementation and integration of security policy occurs locally and is not consistent. As a result, it is difficult to develop and integrate risk-managed security and protection policies and programs, within a cohesive and integrated security framework.

What We Recommend

We recommend a comprehensive and integrated security framework to facilitate tracking security costs, more accurately programming future years security budgets and examining the return on investment for security expenditures.

Management Comments and Our Response

Comments from management were responsive and met the intent of the recommendation. The Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security concurred with the recommendation, stating that an overarching security policy is the necessary first step to provide a platform for functional integration, governance, and strategic resource management. Working with the Washington Headquarters Service he plans to craft the framework for this policy and will have a pre-coordination draft by August 31, 2010. A Director of National Intelligence approved study entitled "Federated Security" is expected to provide a way ahead for developing a more coherent and integrated security framework.

Table of Contents

Introduction	1
Objectives	1
Background	2
Finding. DoD Needs a Comprehensive Security Framework to Better Track and Measure Security Costs and Optimize Its Security Efforts	3
Appendix	
Information Security Oversight Office Government and Industry Cost Report Data for FY 1995 – FY 2008	7
Management Comments	
Deputy Under Secretary of Defense for HUMINT, Counterintelligence and Security	8

Introduction

Security spans the entire Department and is necessary for the Department to protect its resources. To underscore the importance of security and the corresponding costs, annual estimates for government security, as reported by the Information Security Oversight Office¹ (ISOO), have increased from \$5 billion in FY 2001 to almost \$9 billion in FY 2008 (see Appendix). Over 80 percent of the government annual costs are reported from DoD. Security, whether it is information security, personnel security, or physical security, is critical to the national defense. Given the importance of security and the cost to the Department, tracking security expenditures, measuring the return on investment for those expenditures, and ensuring the effective integration of security across the Department is essential.

Objectives

This is the first in a series of reports on security within the DoD and is responsive to a request made by the Under Secretary of Defense for Intelligence (USD(I)) for the Office of Inspector General, DoD to assess the effectiveness of security in the Department. Specifically, we will assess the following issue areas:

- how the Department programs and tracks its security costs and measures the return on investment for security expenditures;
- how security professionals' jobs are classified and graded;
- how security professional's are trained and certified/professionalized; and
- how effective security policy is in addressing the security needs of the Department.

This report addresses how the Department programs and tracks its security costs.

Scope and Methodology

This assessment was conducted in accordance with Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we plan and perform the assessment to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our assessment objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our assessment objectives. We conducted the work for this report from October 2009 through May 2010.

Because of the size and complexity of addressing security within the Department of Defense, we are performing this assessment in phases. While this phase focused on security costs, remaining phases will consist of a more detailed focus on the specific issue areas mentioned in the objective above. Subsequent reports may also address security cost issues within a larger context as additional information is developed. To accomplish the objective, we reviewed relevant policies and guidance, and interviews officials responsible for security policy development and implementation and cost reporting.

¹ The Information Security Oversight Office, a component of the National Archives and Records Administration, is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program.

Prior Coverage

During the last five years, neither the Government Accountability Office nor the Department of Defense Inspector General has issued any reports addressing the objectives of this assessment.

Background

DoD tracks security costs as part of the requirement in E.O. 13526, "Classified National Security Information," December 29, 2009, to report those costs to the ISOO. E.O. 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. It supersedes E.O. 12958, "Classified National Security Information," as amended by E.O. 13292, "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information," March 25, 2003. Section 5.2, "Information Security Oversight Office (ISOO)," of both executive orders states that the ISOO shall:

- develop directives for the implementation of the order,
- oversee agency actions, and
- report at least annually to the President on the implementation of the order.

Section 5.4, "General Responsibilities," of both executive orders require that the heads of agencies designate a senior agency official to direct and administer the program, whose responsibilities shall include:

- overseeing the agency's program,
- promulgating implementing regulations, and
- accounting for the costs associated with the implementation of the order, which shall be reported to the Director of the ISOO for publication.

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),", November 23, 2005, specified that the USD(I) shall serve as the Principal Staff Assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on all intelligence, counterintelligence, and security matters. The USD(I) proposes DoD resource programs, formulates budget estimates, recommends resource allocations and priorities, and monitors the implementation of approved programs in order to ensure adherence to approved policy and planning guidance. With respect to security policy matters, the USD(I) develops and integrates risk-managed security and protection policies and programs.

In addition, the USD(I) coordinates and oversees the implementation of DoD policy, programs, and guidance for personnel, physical, industrial, information, operations, chemical/biological, and DoD Special Access Program security as well as research and technology protection. The USD(I) is further tasked with the performance of all duties and responsibilities of the Secretary of Defense regarding the National Industrial Security Program.

Finding. DoD Needs a Comprehensive Security Framework to Better Track and Measure Security Costs and Optimize its Security Efforts

The DoD needs a comprehensive methodology to track security costs, more accurately program future years security budgets, and examine the return on investment for security expenditures. The ability to do so is complicated by the lack of an overarching framework for security. Current DoD security policy is delineated and primarily focuses on distinct security disciplines. As a result, it will be difficult to develop and integrate risk-managed security and protection policies and programs, including the ability to assess the resource needs and the effectiveness and efficiency of the use of the security resources.

DoD Security Policy

The USD(I) is the Principal Staff Assistant to the Secretary and Deputy Secretary of Defense for Security and has the authority to develop and integrate risk-managed security and protection policies and programs; and develop, coordinate, and oversee the implementation of DoD security policies and programs.

The Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security, through the OUSD(I) Director of Security, is responsible for maintaining 43 policies in the functional areas of information security, industrial security, operations security, research and technology protection, personnel security, physical security, and special access programs. However, no overarching policy exists that blends these policies into an integrated security framework for the Department.

DoD Security Disciplines and Associated Definitions

DoD has policy with associated definitions for differing categories of security disciplines, such as personnel security, physical security, and information security, to name a few. The following publications contain definitions that provide a broad perspective of security disciplines:

- DoD 5200.1-R, "Information Security Program," January 1997, defines information security as "the system of policies, procedures, and requirements . . . to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security."
- DoD 5200.2-R, "Personnel Security Program," January 1987, defines a personnel security investigation as "Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation."

- DoD 5200.08-R, "Physical Security Program," April 9, 2007, refers the reader to Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended through October 31, 2009, which defines physical security as "that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft."

Current Methodology for Estimating Security Costs

Security is not a budget line item, but it touches most everything in the Department. OUSD(I) Security Directorate personnel stated that there is no DoD implementing policy on reporting security costs. The OUSD(I) does not issue a tasker or data call to the Services, Combatant Commands, and Defense agencies to report their security costs. Since 1991, the OUSD(I) has employed the Institute for Defense Analyses (IDA) to assist them with determining the cost of security, which the OUSD(I) reports to the ISOO.

IDA report, "Resource Estimates for Counterintelligence and Security Countermeasures (U)," September 1992 (SECRET), was issued in response to a tasking from the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures), Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. The report states that:

The resources, as well as the management of the activities themselves, tend to be deeply embedded in the overhead of defense programs, and little centralized oversight has been applied. Furthermore, even within the Services, the expertise . . . tends to be compartmented, with little broad understanding outside the specialized areas. For example, experienced military police may understand physical security thoroughly but know little about industrial security, document control, or communications security.

The report specified that the estimates are essentially educated guesses and that if budgetary decisions are to be based on information of this type, more extensive work (including data calls from the Services) would be warranted.

IDA report, "Security Resources in the DoD Infrastructure (U)," April 1998 (SECRET), states that knowledge of security resources is an important part of the oversight the Office of the Secretary of Defense is expected to assert over the defense infrastructure, but that knowledge of the full scope and composition of security resources has been limited. In addition, management of and responsibility for the resources tend to be fragmentary. Physical security and most other aspects of security are executed at the discretion of unit commanders, with little or no top-level visibility. These findings are still true today.

Summarizing Security Costs: Institute for Defense Analyses.

IDA methodology for estimating DoD security costs is based on Defense Manpower Data Center² information, the Planning, Programming, and Budgeting information developed for the President's budget, and interviews.

² The Defense Manpower Data Center is a key DoD support organization that, among other things, generates quantitative data and analysis for defense organizations such as the Services, the Office of the Secretary of Defense, and the Joint Staff.

To estimate security costs, IDA divides security into six functional areas, as follows: Physical Security; Information Security; Information System Security; Personnel Security; Counterintelligence and Investigations; and Cross Disciplinary.

Summarizing Security Costs: Information Security Oversight Office.

The security categories contained in the ISOO cost report are Personnel Security, Physical Security, Information Security, Miscellaneous (includes Operations Security and Technical Surveillance Countermeasures); Professional Education, Training, and Awareness; Security Management and Planning; and Unique Items (Department or Agency specific activities that are not reported in any of the primary categories but are nonetheless significant and need to be included).

DoD costs reported to the ISOO encompass the cost categories reflected in the ISOO report; however, DoD information reported to the ISOO does not directly correlate with ISOO security cost requirements. An example would be the "Counterintelligence and Investigations" category, which is not an ISOO category and whose costs may be reported through other mechanisms like the military and national intelligence programs. This potential inconsistency could be addressed through a change in data collection methodology which would be assisted by the implementation of a comprehensive security architecture within the DoD.

Conclusion

DoD has policy for differing categories of security disciplines, but because security spans the entire Department and touches all levels of command, implementation and integration of security policy occurs locally. Also, in today's environment the lines between distinct categories are beginning to merge. As a result, it is difficult for a cohesive and integrated DoD security framework to exist. Further, identifying the multiple categories of security does not provide an encompassing paradigm for security, nor will fragmentary security disciplines assist commands and security practitioners with implementing a comprehensive, integrated security framework. DoD needs standardized guidance to assist DoD commands and security practitioners with implementing a comprehensive and integrated security framework. The compartmentalization of security identified in the 1992 IDA report still exists today.

In addition, the statement in the 1998 IDA report that knowledge of the full scope and composition of security resources has been limited and that management of and responsibility for security resources is fragmentary, remains true as well. The OUSD(I), Services, Combatant Commands, and Defense agencies need to know the total costs relative to security. Specifically, the DoD needs a comprehensive methodology to: track security costs, more accurately program future years security budgets, and examine the return on investment for security expenditures and make risk-based decisions on the best use of the security resources across the categories. A comprehensive methodology would allow DoD to optimize oversight and determine the most efficient and effective means to accomplish its security mission. However, without a cohesive and integrated framework, the Department is unlikely to reach that goal.

Recommendation, Management Comments, and Our Response

We recommend that the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security, in consultation with the Unders Secretary of Defense, the Services, Combatant Commands, and Defense agencies, develop a policy that provides guidance for a comprehensive and integrated security framework, including a methodology for tracking and measuring DoD security costs.

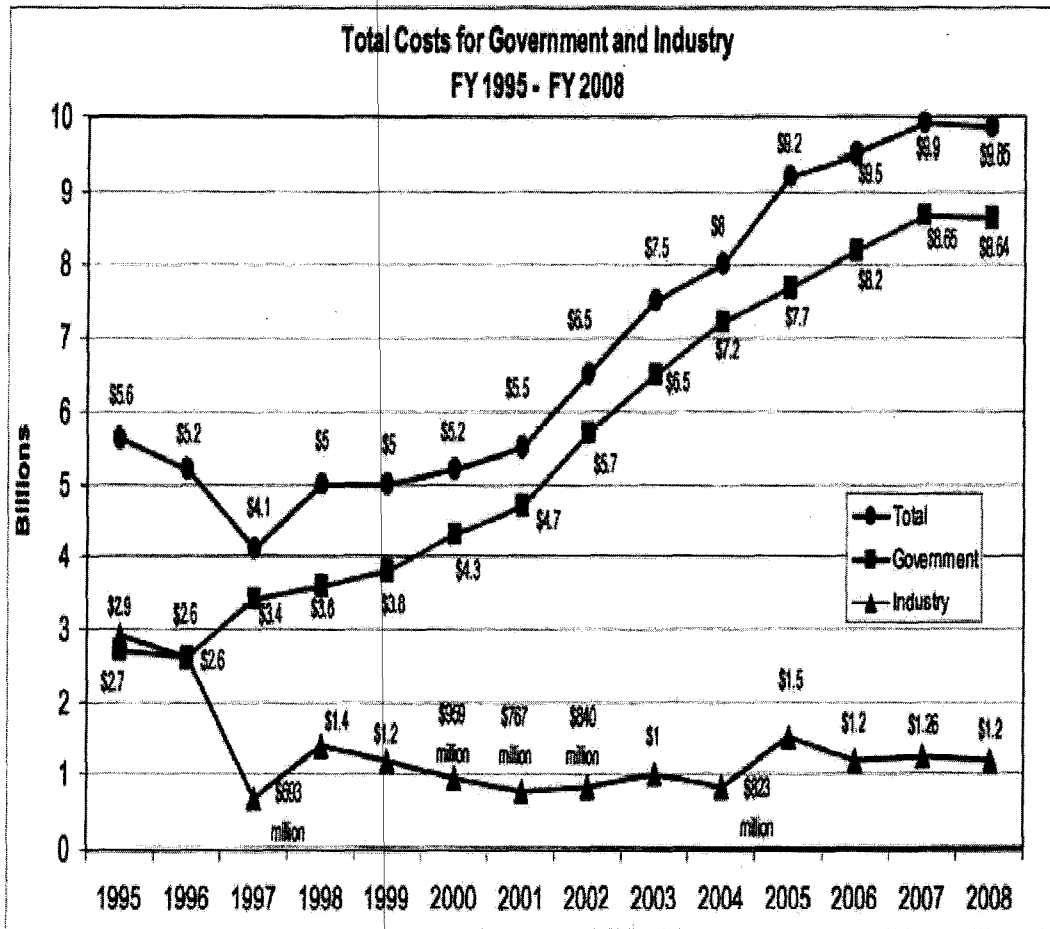
Management Comments

The Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security concurred with the recommendation, stating that an overarching security policy is the necessary first step to provide a platform for functional integration, governance, and strategic resource management. The Office of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security is working with the Washington Headquarters Service to craft a framework and intends to have a pre-coordination draft by August 31, 2010. The Office of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security is preparing to conduct a study, approved by the Director of National Intelligence, entitled "Federated Security." They expect the study to provide a way ahead for developing a more coherent and integrated security framework, while using our future assessment results to inform that effort. The Office of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security has also inserted language into the Defense Intelligence Strategy, which includes a provision to establish a common lexicon for Security for the Department.

Our Response

The comments of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security are responsive and meet the intent of the recommendation. Please provide a draft of the policy prior to issuance.

APPENDIX: Information Security Oversight Office Government and Industry Cost Report Data for FY 1995 – FY 2008



(Data from Information Security Oversight Office FY 2008
Report on Cost Estimates for Security Classification Activities)

Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security Comments



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

JUL 21 2010

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL FOR INTELLIGENCE EVALUATIONS

SUBJECT: Assessment of Security Within the Department of Defense – Tracking and Measuring Security Costs (Project No. D2010-DfINT01-0066.000)

Thank you for the opportunity to review your June 11, 2010, draft report. We concur with the general findings and provide the following comments for consideration:

The report correctly highlights security as a critical function in the Department of Defense. If the Department is unable to accurately measure costs and return on investment, security oversight suffers, and it is impossible to establish an effective strategic direction.

We agree that an overarching security policy is the necessary first step to provide a platform for functional integration, governance, and strategic resource management; however, we cannot meet the objective without the appropriate staffing, authorities, and governance within the Office of the Secretary of Defense (OSD). Security policy administration within OSD is also fragmented. For example, information systems security comprises a significant portion of the costs incurred, but policy administration and oversight of this critical function are external to the Office of the Under Secretary of Defense for Intelligence. An OSD process for decision-making and governance would have to be established to achieve the comprehensive security framework you recommend.

We are working with Washington Headquarters Services to craft a framework and intend to have a draft for pre-coordination edit by August 31, 2010. The draft directive proposes definitions, establishes lines of authority and a governance body, and directs components to identify a single senior security official who will maintain cognizance over all security-related activities in the component, to include resources.

Also, the Office of the Director of National Intelligence has approved our request for a study entitled "Federated Security." We expect this study to provide a way ahead for developing a more coherent and integrated security enterprise. Your series of assessments will inform that effort, and we look forward to working with you on the rest of the series.


We particularly appreciate your observations regarding security definitions and how they reinforce the breakdown (rather than the integration) of security by discipline.



Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security Comments

This year, for the first time, we have inserted security language into the Defense Intelligence Strategy, which includes a provision to establish a common lexicon for security for the Department.

Thank you for raising the awareness of security issues within the Department. This critical function is often eclipsed by the urgency of our warfighting activities, yet—as your study aptly points out—impacts all defense mission areas. My points of contact are (b)(6) at (703) 607- (b)(6) or (b)(6) @osd.mil, and (b)(6) at (703) 604- (b)(6) or (b)(6) @osd.mil.


Laurence K. Burgess
Deputy Under Secretary of Defense
(HUMINT, Counterintelligence & Security)



Inspector General
Department of Defense

FOR OFFICIAL USE ONLY