

DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

Survey of the Science and Technology
Directorate



Office of Inspections, Evaluations & Special Reviews

OIG-04-24

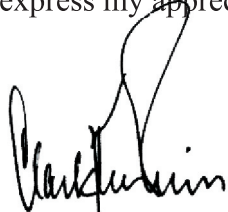
March 2004

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (Public Law 107-296) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, investigative, and special reports prepared by the OIG periodically as part of its oversight responsibility with respect to DHS to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the program, operation, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed on the basis of the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that this report will result in more effective, efficient, and/or economical operations. I express my appreciation to all of those who contributed to the preparation of this report.



Clark Kent Ervin
Inspector General

Contents

Introduction.....	3
Results in Brief	4
Background.....	5
Purpose, Scope, and Methodology.....	5
The Budgetary Programs and Organizational Elements of the Science and Technology Directorate.....	6
Management’s Response.....	19
Issues For Future OIG Reviews.....	19

Appendices

Appendix A:	Summary of S&T Statutory Functions	25
Appendix B:	Budget and FTE Statistics for Fiscal Year 2003 and 2004.....	26
Appendix C:	RDT&E Program Nomenclature.....	27
Appendix D:	S&T Portfolios	28
Appendix E:	Major Contributors To This Report	35
Appendix F:	Report Distribution	36

Abbreviations

BAA	Broad Agency Announcement
CIP-MSAP	Critical Infrastructure Protection-Modeling, Simulation, and Analysis Program
COS	Chief of Staff
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DoD	Department of Defense
DoE	Department of Energy
EML	Environmental Measurements Laboratory
FAR	Federal Acquisition Regulation

Contents

FTE	Full Time Equivalent
FY	Fiscal Year
HSA	Homeland Security Act of 2002
HSI	Homeland Security Institute
HS-Center	Homeland Security-Center for Excellence
HSARPA	Homeland Security Advanced Research Projects Agency
HSSTAC	Homeland Security Science and Technology Advisory Committee
IAIP	Information Analysis and Infrastructure Protection
IND	Improvised Nuclear Device
IPT	Integrated Product Team
IRCM	InfraRed CounterMeasure
IT	Information Technology
MANPADS	Man-Portable Air Defense Systems
NSF	National Science Foundation
ORD	Office of Research and Development
OIG	Office of Inspector General
OTA	Other Transactions Authority
OWMDO-IM	Office of Weapons of Mass Destruction Operations-Incident Management
PIADC	Plum Island Animal Disease Center
PPB	Office of Plans, Programs, and Budget
RDD	Radiological Dispersal Device
RDT&E	Research, Development, Test and Evaluation
S&T	Science and Technology Directorate
SED	Office of Systems Engineering and Development
START	Scientific and Technical Advisory and Response Teams
USC	University of Southern California
USDA	Department of Agriculture
TSA	Transportation Security Administration
TSWG	Technical Support Working Group
TVTA	Threat and Vulnerability, Testing and Assessment
WMD	Weapons of Mass Destruction

Introduction

The Science and Technology Directorate (S&T) was created to support the strategic mission of the Department of Homeland Security (DHS) by conducting, stimulating, and enabling research; and developing, testing, evaluating, and transferring homeland security capabilities to federal, state, and local operational end-users. The S&T will:

- Partner with operational end-users to identify requirements, and develop capabilities to counter threats and enhance mission operations;
- Engage government, academic, and private sectors in innovative research, development, rapid prototyping, and systems engineering and development;
- Provide a rapid, efficient, and disciplined process for systems engineering and development;
- Provide DHS with an enduring research and development complex dedicated to homeland security.

The S&T is unique in that no other federal organization has the statutory mandate to merge these responsibilities under one organizational framework.

We conducted this survey to further our knowledge of the S&T. Particularly important were the following:

- The methodology for transferring and integrating the functions and resources from legacy agencies responsible for conducting research and development into the S&T;
- How the S&T offices and divisions are working or intend to work with other DHS entities and non-DHS entities to protect critical infrastructure; and
- The S&T's ability to communicate information with entities within DHS and other federal, state, local, and private sector partners.

Additionally, we endeavored to determine the obstacles the S&T faces in “standing-up” the organization and areas or issues that could result in future Office of Inspector General (OIG) reviews.

Results in Brief

On March 1, 2003, portions of programs, activities, and laboratories from three agencies – Department of Defense (DoD), Department of Energy (DoE) and Department of Agriculture (USDA) – merged to become the S&T. The S&T is known as the “technology arm” of the DHS. Some aspects of this merger were made easier because S&T was able to borrow some business processes from DoD’s Defense Advanced Research Projects Agency (DARPA), which has a federal research and development mission. In addition, S&T hired key personnel who had prior work experience with DARPA. However, the merger was not completely without its challenges. The S&T has had to contend with a set of administrative and logistical challenges similar to those encountered by other startup ventures, including: (1) the inability to hire personnel quickly who can work in a secure environment, (2) the lack of centralized space, and (3) the lack of consistent Information Technology (IT) systems and procurement support. These difficulties are partially the result of being dependent on services provided by other federal agencies and other DHS directorates that are themselves not fully staffed.

We identified several areas that may warrant future evaluation, including: (1) the procedures for selecting persons to participate in both the Homeland Security Centers of Excellence program and the Scholars and Fellows program; (2) the level of coordination between S&T and other DHS directorates to formulate an integrated strategic plan and reduce the possibility for duplication when selecting new technologies for further research and development; (3) the governing doctrine between the S&T and the laboratories that it oversees, to make sure that responsibilities for facilities management and security are clearly defined; (4) the procedures and controls in place for managing Other Transactions Authority (OTA),¹ and (5) the ability of friendly foreign scientists and students to contribute to S&T programs.

¹ Other Transactions Authority exempts the S&T from having to follow the procurement rules found in various federal procurement regulations and is intended to greatly shorten the time it takes to procure goods and services.

Background

In response to the recognized need for a coordinated, national approach² to protect the homeland against potential terrorist attacks, the United States Congress enacted the Homeland Security Act of 2002 (HSA), resulting in the creation of the DHS. The primary strategic objectives of the DHS are:

- To prevent terrorist attacks within the homeland;
- To reduce the vulnerability of the homeland to terrorism; and
- To minimize the damage and assist in the recovery from terrorist acts that occur within the homeland.

To sustain these strategic objectives, the S&T was created as the primary research and development arm of the DHS. The S&T organizes scientific, engineering, and technological resources of the United States to facilitate the rapid identification, development, and implementation of new, cost effective technologies in support of the homeland security mission. The S&T has three primary activity areas: (1) intramural, (2) extramural, and (3) educational. Intramural activities involve in-house research and development consisting of a group of scientists and engineers focusing on homeland security issues. Extramural activities involve soliciting innovative ideas from industry and academia. Educational activities involve providing scholarships and fellowships to those who wish to enter into careers and perform research that are important to the homeland security research and development enterprise. S&T fulfills its mission through its four major components, namely, the Office of Plans, Programs, and Budget (PPB); the Homeland Security Advanced Research Projects Agency (HSARPA); the Office of Research and Development (ORD); and the Office of Systems Engineering and Development (SED).

Purpose, Scope, and Methodology

The objective of our survey was twofold. First, we set out to gain a basic understanding of the S&T. This included learning the missions of the S&T offices, defining the operational relationships between its offices and divisions,

² Before the DHS was created in November 2002, protecting the homeland was primarily a federal responsibility and was mainly coordinated through the military, the intelligence agencies, and Department of State. Since the September 11, 2001, terrorist attack, this has become a national rather than a federal responsibility, because the federal government alone cannot protect the homeland. This responsibility has now become a national responsibility, requiring close coordination among federal, state, and local governments and the private sector.

diagramming S&T's organization and business processes, and identifying the obstacles impeding S&T's ability to become fully operational. Second, our survey provided us an opportunity to identify issues suited for future OIG inspections or audits. We reviewed and analyzed documentation pertinent to the DHS and the S&T directorate including program guidance, policy memorandums, briefing packages, meeting notes, Internet websites, various news articles, and the HSA.

We interviewed the S&T Under Secretary, the Chief of Staff, and several key S&T officials.

We conducted our fieldwork from December 2003 to January 2004. This survey was conducted under the authority of the Inspector General Act of 1978, as amended.

The Budgetary Programs and Organizational Elements of the Science and Technology Directorate

Guided by the requirements of the HSA, S&T is the principal directorate within DHS charged with leading the federal government's civilian efforts in the research and development of technologies in support of homeland security. Included among these technologies are those geared toward: (1) preventing the importation of chemical, biological, radiological, nuclear, and related weapons and materials; and (2) detecting, preventing, protecting against, and responding to terrorist attacks. In addition to its research and development function, S&T is also charged with supporting the Under Secretary for Information Analysis and Infrastructure Protection by assessing and testing homeland security vulnerabilities and possible threats (Appendix A). S&T accomplishes this mission through an approved fiscal year (FY) 2004 personnel complement of 140 Full-Time Equivalents (FTE) that manages its intramural and extramural research and development and educational programs through an extensive network of contacts at other federal agencies, public and non-profit laboratories, universities, and the private sector.

The Budgetary Programs of S&T

S&T budget statistics are reported in Appendix B. The S&T budget was \$553 million for March through September in FY 2003 and \$918 million in FY 2004. Of the \$918 million in funding approved for FY04, about \$874 million, or 95.2

percent, will be spent on research and development programs, while the rest will cover personnel expenses. The FY 2004 budget request is designed to support homeland security by helping the nation maintain its technical superiority in science and technology. As new technologies are developed with this funding, S&T intends to share them with other federal, state, local and private sector partners. Highlights of S&T's FY 2004 budget include:

- \$198.5 million to develop and implement integrated systems to decrease the probability and effects of a biological attack on this country's civilian population and agricultural system.
- \$127 million to develop radiological and nuclear countermeasures that prevent the importation, transportation, and subsequent detonation of a radiological or nuclear device within our borders.
- \$93 million to develop technologies and systems to enhance DHS's ability to analyze threat information, assess and test vulnerability assessments for infrastructure protection, detect and mitigate sophisticated cyber threats, enhance the interoperability of new technologies, and determine hostile intent.
- \$88 million for the construction of a National Biodefense Analysis and Countermeasures Center, which is to be the principal DHS component of the Fort Detrick Interagency Biodefense Campus in Maryland.
- \$75 million for the Rapid Prototyping/Technical Support Working Group (TSWG)³ to provide a competitive method to evaluate technologies during their initial phases of development.
- \$70 million to develop academic programs that support students by building learning and research environments in key areas such as bioforensics, cybersecurity, disaster modeling, and psychological and behavioral analysis.

³ TSWG is the U.S. national forum that identifies, prioritizes, and coordinates interagency (Departments of State, Defense, Energy, Homeland Security, and Federal Bureau of Investigation) and international research and development requirements for combating terrorism.

The Organizational Elements of S&T

The S&T inherited programs, activities, and laboratories from three legacy agencies. Most came from DoE, while the others came from the DoD and USDA. The following list identifies the programs, activities, and laboratories that were merged to form the S&T:

- The chemical and biological national security and supporting programs and activities of the nonproliferation and verification research and development program (DoE)
- The life sciences activities related to microbial pathogens of the biological and environmental research program (DoE)
- The nuclear smuggling programs and activities within the proliferation detection program of the nonproliferation and verification research and development program (DoE)
- The nuclear assessment program and activities of the assessment, detection, and cooperation program of the international materials protection and cooperation program (DoE)
- The advanced scientific computing research program and activities at Lawrence Livermore National Laboratory (DoE)
- The Environmental Measurements Laboratory (DoE)
- The National Bio-Weapons Defense Analysis Center (DoD)
- Plum Island Animal Disease Center (USDA)

Merging these programs, activities, and laboratories has been an ongoing process and has created challenges similar to those encountered by other startups. Fortunately, not all of S&T is without precedent. Less than ten percent of S&T's mission involves conducting non-requirements driven research and development of new technologies. To provide us with an example of what non-requirements driven research and development means, an S&T executive provided the hypothetical example of the development of a mass bio-button network of sensors. In such a network, small bio-buttons would be passed out to millions of commuters. During their return trip home, people who received buttons during their commute into work would toss the bio-buttons into receptacles to be analyzed later as they exited their commuting destination. The purpose of the bio-buttons would be to sense where and when the button was exposed to a potential biological contagion. With thousands of people wearing these so-called bio-buttons, such a network of sensors could be useful in the early warning and detection of a massive biological attack on the nation. Currently, such a technology does not exist, nor are there any current requirements or concept of

operations for such a technology – the kind of technology that is so cutting edge that it will “knock your socks off.” The execution arm of S&T responsible for conducting this kind of research is the Homeland Security Advanced Research Projects Agency (HSARPA). HSARPA is modeled after a similar agency within the DoD known as the DARPA.

The S&T has recruited several key personnel from DARPA. These personnel have been able to draw from their overall knowledge of the DoD’s Research, Development, Test and Evaluation (RDT&E) program to assist the S&T in becoming fully operational. As part of this overall knowledge, these personnel continued to use RDT&E program nomenclature (Appendix C):

- Basic Research 6.1
- Applied Research 6.2
- Advanced Technology Development 6.3
- Demonstration and Validation 6.4
- Engineering and Manufacturing Development 6.5
- Management Support 6.6
- Operational Systems Development 6.7

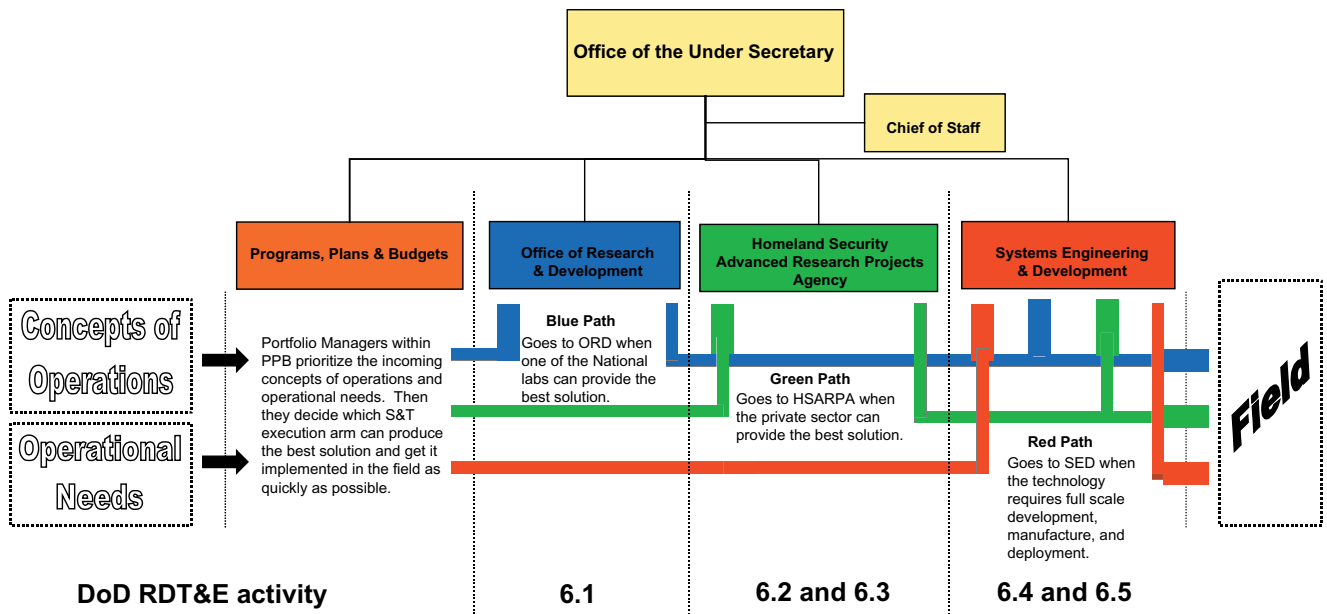
This RDT&E program nomenclature can be seen in the overall organizational structure of the S&T. Recruiting DARPA personnel and incorporating RDT&E program nomenclature into its overall organizational structure and into its business model has helped make the startup phase for S&T somewhat easier. Despite being able to borrow some RDT&E program nomenclature and business methodologies, it is important to reiterate that the merging process has not been without challenges. The S&T has had to contend with a myriad of administrative and logistical issues that include: (1) the inability to hire personnel quickly who can work in a secure environment, (2) the limited space in its central office, and (3) the lack of consistent IT systems and procurement support. These difficulties are partially the result of S&T’s dependence for these services on other DHS directorates that are in themselves not fully staffed and other federal agencies. One senior executive with significant private sector experience characterized the S&T as a “startup within a merger.”

Like DARPA, the S&T was endowed by Congress with Other Transactions Authority (OTA). The statutory OTA plays an important role in S&T’s ability to quickly implement new technologies in the field. OTA does this by providing a legal basis for exempting S&T from nearly all federal procurement rules and regulations. We were told that Congress’ intent was to substantially reduce the

normal procurement cycle for complex systems and advanced technologies, which under the existing federal procurement process can take as long as three to five years.

Presented below is the most recent organizational chart supplied by the S&T, dated October 1, 2003, with a graphical presentation of RDT&E program nomenclature integrated into the S&T organizational chart and business model as depicted by the OIG:

**Chart 1 – The Science and Technology Directorate
Business Processes of the
Science and Technology Directorate**



One of the intended benefits of S&T’s business model is its relative simplicity and ability to assign projects based on criticality and national priorities to the best-suited S&T execution arm for further research and development. As outlined in the above chart, portfolio managers within the PPB first vet incoming concepts of operations and operational needs that have applications for homeland security. The portfolio concept and the personnel that manage them are discussed later in this survey. Portfolio managers in conjunction with an Integrated Project Team (IPT) examine incoming concepts of operations and operational needs against

short-term and long-term goals in accordance with national priorities. The IPT concept is discussed in more detail later in this survey. After determining where these incoming concepts of operations and operational needs fit within national priorities, the portfolio managers submit recommendations to senior S&T management as to which technologies should be selected for further research and development. Once final decisions on which technologies to further research and develop are made, portfolio managers continue to work closely with end-users to refine the technology's concept of operation or to better understand the operational needs of the end-user. After the technology's concept of operation or the end-user's operational needs have been fully determined and prioritized, the portfolio manager, in conjunction with the rest of the IPT, decide which S&T execution arm can provide the best solution for getting the technology implemented in the field as quickly as possible. This decision is primarily based on the maturity of the selected technology, i.e., how close the technology is to production. If the technology requires extensive research and development before it can go into production, then it is assigned to the Office of Research & Development (ORD). If the technology requires minimal research and development and can be brought quickly to proof-of-concept, then it is assigned to HSARPA. If the technology is mature enough to go immediately into a pre-production demonstration or a pilot program, or if it is a production phase solution ready for validation and field test, then it is assigned to the Systems Engineering & Development (SED) execution arm of the S&T.

S&T's organizational structure and business model, coupled with having OTA, supports the rapid identification, development, and implementation of new technologies that are a high priority for implementation in the field. This can be seen in how S&T chose to address the immediate potential threat that shoulder-fired missiles, known as MANPADS, i.e., Man-Portable Air Defense Systems, pose to U.S. commercial aircraft. Congress approved \$60 million for the counter MANPADS program in FY 2004, with approximately an additional \$61 million likely to be approved for FY 2005. Initially, the counter MANPADS program was a portfolio in the PPB. However, with the prospect of new funding, S&T senior executives, in consultation with the counter MANPADS portfolio manager, decided to turn the counter MANPADS portfolio into a full-fledged program and moved it into the SED to be administered.

This organizational and OTA procurement flexibility enabled the S&T to announce contract awards to three separate companies for the first phase of the counter MANPADS initiative approximately three months after soliciting white papers from prospective contractors. According to the manager of the counter

MANPADS program, having OTA substantially shortened the time it took to reduce the 24 contractors that submitted white papers to a more exclusive group of five contractors that were allowed to continue with the bidding process. These five contractors were asked to submit more detailed proposals on how they would actually counter the threat that MANPADS pose to commercial aircraft. Rather than have them submit lengthy technical and cost proposals, OTA allowed S&T to require the five remaining contractors to present their proposals during a tight, five-hour oral presentation. All of these presentations were scheduled and conducted within one week and within several hours after the last presentation the three winning contractors were selected.

The Office of the Under Secretary

The Under Secretary for S&T reports directly to the Secretary of DHS and is responsible for carrying out the S&T mission as prescribed by the HSA. The Under Secretary is responsible for leading the S&T into functioning as a technological clearinghouse by encouraging and supporting research, development, testing, evaluation and timely transmission of new technologies to federal, state, and local operational end-users in the field to make the homeland more secure. In addition to leading the day-to-day operations of the S&T, the HSA states that the Under Secretary is responsible for administering: (1) the Homeland Security Science and Technology Advisory Committee (HSSTAC), and (2) the Homeland Security Institute (HSI).

As the sponsor of the HSSTAC, the Under Secretary is responsible for appointing all 20 members of the committee. He appointed the committee members in February 2004. In addition to scientists, engineers, and medical researchers, committee membership includes emergency first responders, representatives from organizations or associations of emergency first responders, and representatives from citizen groups, including those representing economically disadvantaged communities. All members will serve in a pro-bono capacity. The HSSTAC is designed to provide the Under Secretary with a direct end-user perspective and to make recommendations with respect to the utility of activities conducted by the S&T, as well as identify research areas of potential future importance. By statute, the HSSTAC will meet at least four times a year. The HSSTAC's first meeting was scheduled for February 26, 2004.

The HSA also provides for the establishment of the HSI and requires it to be administered as a separate and distinct entity from the S&T. The HSI is to function as a federally funded research and development center. The law also

gives the Under Secretary considerable discretion in assigning responsibilities to the HSI. The program manager in charge of establishing the HSI on behalf of the Under Secretary described it as being “an operations-driven think-tank that will provide studies and analyses for the DHS similar in scope to those that organizations such as the Rand Corporation, Institute for Defense Analyses, Center for Naval Analyses, to name a few, have provided the DoD for many years.” The program manager expects the HSI to have a personnel complement of 150 FTE and will provide the Under Secretary with independent analysis on such topics as vulnerabilities of the nation’s critical infrastructures, economic and policy analyses of approaches to enhance security, metrics designs, and methods to evaluate federal government security programs.

There are two immediate organizational units that provide direct support for the Under Secretary: the Chief of Staff and the Office of Weapons of Mass Destruction Operations and Incident Management (OWMDO-IM). The Chief of Staff is the Under Secretary’s principal advisor for daily administrative matters such as financial and strategic planning, facilities, and acquisition support that are essential to ensure that the S&T fulfills its mission. The Chief of Staff serves also as the principal S&T liaison to other DHS elements like the Management Directorate, Legislative Affairs, Public Affairs, General Counsel, and the Inspector General. Additionally, the Chief of Staff is responsible for assuring the dissemination and implementation of policies and directives throughout the S&T.

The OWMDO-IM is staffed with response experts who provide architecture for the Scientific and Technical Advisory and Response Teams (START). The OWMDO-IM is primarily a “virtual” entity, but can insert START teams at or near the incident site for analysis and advisory support to state and local governments, or to Disaster Field Offices. START is staffed with highly technical scientists from other S&T offices, and serving in the START is considered to be a collateral duty. During crisis and near-crisis events, personnel from the OWMDO-IM are assigned to work in the Homeland Security Operations Center. Part of the process is making recommendations to the Director of the Interagency Incident Management Group during crisis operations. They are expected to ensure a “scientist-to-responder” link, by translating complex scientific and technical information into terms that are easier to understand for non-technical audiences on the ground. In addition to first responders, the work conducted by OWMDO-IM personnel assists executive management in decision-making. To illustrate, personnel from OWMDO-IM are able to direct various national

laboratories to conduct “plume modeling exercises”⁴ for possible scenarios involving the dispersion of chemical, biological, or radiological contaminants near certain potential terrorist targets. Upon receiving the results, the OWMDO-IM can report the results within one hour in non-technical terms to executive management. Executives are then better able to make decisions regarding the type of medical remedies and equipment that first responders need when responding to any hypothetical catastrophic situation.

Office of Programs, Plans, & Budget

The PPB plays a central role in S&T’s business model. The Portfolio Managers in PPB lead the interaction with S&T’s customers. They also play an important role in prioritizing and selecting which incoming concepts of operations and operational needs are ultimately chosen for further research and development. One senior executive described PPB as being a type of “conduit” for customers to communicate their technical and operational needs to S&T.

The PPB interacts with customers through portfolio managers. An S&T portfolio can be defined as a compilation of subject material under one type of threat that has implications for existing or future research and development initiatives. The PPB employs 16 portfolio managers who oversee the same number of portfolios, with some having multiple sub-portfolios (Appendix D). In addition to being on the front-line of S&T customer interaction, portfolio managers are responsible for setting timelines and priorities to satisfy customer needs. In addition to portfolio managers, an IPT is made up of program managers from similar programs within the other three S&T operational elements, namely ORD, HSARPA, and SED. The role of portfolio managers is to provide the IPT with strategic guidance, while program managers provide the IPT with an assessment of the technical capability of their own individual S&T element and the public and private sectors to actually bring a new technology to production and eventually get it implemented in the field. By understanding the technical capability of the three S&T execution arms, portfolio managers can better decide which of them is best suited for beginning the research, development, and production cycle for the selected new technology. In the MANPADS illustration discussed previously that involved a mature technology that had been used in executive aircraft for years, knowing

⁴ When a chemical is released from a device, the plume can travel great distances, depending largely on the wind conditions at the time of detonation. Plume modeling can be used to predict how far the plume will travel and how many people the device may have contaminated.

the technical capabilities of the three S&T execution arms assisted the portfolio managers in making the decision to select the SED as the lead operational element for administering the counter MANPADS program.

It is through portfolio managers and their leadership positions on IPTs that the PPB is able to exert a considerable amount of influence on the technology selection process. In addition to leading IPTs, another avenue for influence that the PPB has on the selection process comes from its unique relationship with the Information Analysis and Infrastructure Protection (IAIP) Directorate. The IAIP is the lead directorate within the DHS for formulating the national infrastructure protection plan. As part of this responsibility, the IAIP maintains a Protective Measures Target List that catalogues and prioritizes the nation's critical infrastructure and key assets. The PPB has one portfolio and parts of another dedicated to working on IAIP matters. One senior executive described these portfolios as "where the S&T and IAIP are joined at the hip." It is here where the S&T supports IAIP by researching and developing new tools to conduct vulnerability and risk assessments. In turn, it is here where the IAIP communicates to the S&T which critical infrastructure and key assets are considered Tier I, i.e., the highest priority, requiring the greatest protection, and Tier II, i.e., lower priority, requiring less protection. In the ideal environment, the relationship between S&T and IAIP would be such that the IAIP would be equipped with state-of-the-art modeling and visualization tools capable of anticipating and mitigating against future terrorist attacks, while the S&T would be equipped with the terrorist threat picture facing the nation, ensuring that it focuses its attention on researching and developing new technologies designed to safeguard Tier I critical infrastructure and key assets, rather than on those designed to safeguard Tier II critical infrastructure and key assets.

In addition to utilizing the terrorist threat picture formulated by the IAIP, the PPB also utilizes a type of matrix system when selecting new technologies for further research and development. Along the horizontal x-axis of the matrix is a list of traditional portfolios, e.g., Border & Transportation Security, Emergency Preparedness & Response, Coast Guard, Secret Service, etc. Along the vertical y-axis of the matrix is a list of technical portfolios, e.g., Chem-Bio, Rad-Nuclear, Cyber, etc. As portfolio managers receive input from contacts within the technical and traditional portfolios, they record incoming concepts of operations and operational needs by populating corresponding cells within the matrix. Concepts of operations and operational needs that are requested by multiple portfolios in the matrix system receive a higher priority. Once a particular technology resulting from a concept of operation or operational need is selected for development, the

portfolio manager in conjunction with the rest of the IPT decide which of the three S&T execution arms is best suited for beginning the research, development, and production cycle for the selected new technology.

Office of Research and Development

The Office of Research and Development (ORD) reports to the Under Secretary for S&T. Sections 308(c) and 309 of the Homeland Security Act prescribe the R&D mission. Generally, this is known as the intramural activity of the S&T. The intramural activities are all S&T requirements that the senior S&T leaders determine cannot be fulfilled by the private sector and must be carried out by national or university laboratories. Generally, the R&D receives projects that have needs for technologies that are not mature and need extensive research and development. ORD's duties include research, development, testing, and evaluation; university and fellowship programs; and enduring research and development capability dedicated to homeland security.

The ORD manages and acts as the steward for the federal and national laboratories that are responsible for providing research and development activities for the protection of the homeland. The S&T has direct stewardship over the Plum Island Animal Disease Center (PIADC) and the Environmental Measurements Laboratory (EML). A reorganization plan required by the HSA mandated that the PIADC be transferred from the Department of Agriculture to the DHS S&T on June 1, 2003. PIADC was used to conduct basic and applied research and diagnostic activities to protect the health of livestock on farms across America from foreign disease agents. Its role is to lead research and development to prevent, respond to, and recover from the intentional introduction of animal diseases.

The HSA also mandated that the EML be transferred from the Department of Energy to DHS S&T. The EML mission is to advance and apply the science and technology required for preventing, protecting against, and responding to radiological and nuclear events in the service of homeland and national security. EML is responsible for using its expertise in radiation and radioactivity measurements to improve the science and technology available to the nation's responders.

The S&T also works with laboratories that are owned and operated by other federal agencies. These laboratories are⁵:

- Lawrence Livermore Laboratory, (DOE)
- Los Alamos National Laboratory (DOE)
- Sandia National Laboratory (DOE)
- Oak Ridge National Laboratory (DOE)
- Pacific Northwest Laboratory (DOE)
- United States Secret Service Laboratory (DHS)
- Transportation Security Laboratory (DHS)

Homeland Security Advanced Research and Projects Agency

The Homeland Security Advanced Research and Projects Agency (HSARPA) reports to the Under Secretary for S&T. HSARPA is the external research and development funding unit of DHS. HSARPA has three primary missions: (1) to interact with the private sector and universities to identify and develop revolutionary technologies that can be used to better secure the homeland, with an emphasis on satisfying the operational needs of customers, (2) fill DHS customers' operational needs for advanced technology by fostering emerging technologies to a developmental level where they can be demonstrated in a proof-of-concept, i.e., furnish a pragmatic technology, and (3) move technology out of the labs and into the field quickly by rapid prototyping/commercial adaptation of technologies. HSARPA receives operational needs from PPB and provides technology infusion to ongoing SED and other DHS components' programs, and may transfer large technology developments to SED for full-scale development and deployment.

As part of the rapid Prototyping program, HSARPA leverages its relationship with the TSWG. Rapid prototyping is used when a new technology needs to be in the field in less than one year. HSARPA contributed \$33 million to TSWG in FY2003 and another \$30 million in FY2004 to issue a Broad Agency Announcement (BAA) before HSARPA was staffed to do so. The contracts resulting from this BAA are managed by TSWG with coordination with HSARPA.

HSARPA conducts its roles in part by awarding procurement contracts, grants, cooperative agreements, or other transactions for research or prototypes to public

⁵ We also identified another laboratory within DHS, but not under S&T control. This laboratory was the U.S. Customs Laboratory and Scientific Service that does testing to determine the origin of agricultural and manufactured products.

or private institutions, businesses, federally funded research and development centers and universities.

Office of Systems Engineering and Development

The SED supervises and directs major acquisition programs and related activities. SED receives operational needs from PPB that have a “mature” technology, require little or no research and development, and are ready for a pilot program, pre-production integration and test, or systems development and demonstration. These projects are generally larger and involve more integration and test complexities than those handled by HSARPA. Also, HSARPA may transfer projects to SED when it needs to transition from a small project to a major initiative. SED develops solution-based systems, conducts rapid full-scale development and acceptance testing, and makes transition of cost-effective systems with a view to satisfying customer needs. The adoption of military technologies that are appropriate for homeland defense purposes, for instance, a commercial variant of InfraRed CounterMeasures (IRCM) equipment for use on civil aircraft, is one example of SED’s activities.

During its brief tenure, SED has worked on major DHS initiatives, such as the counter MANPAD program, which aims to protect commercial aircraft from human-portable anti-aircraft missiles. SED is also involved with Safety Interoperable Communications Program (SAFECOM) and Biowatch. Established in 2002, SAFECOM is the first umbrella program within the federal government to assist local, tribal, state and federal agencies improve public safety response through efficient interoperable wireless communications.

The Biowatch program involves the installation in several metropolitan areas across the country of detection devices to identify airborne pathogens like anthrax in time to hand out life-saving medicines to victims. SED is also assisting in the pilot programs with the Port Authorities of New York and New Jersey to test chemical, biological, radiation, nuclear and explosive detection equipment.

Other SED’s responsibilities include preparing the budget, determining the sequence of projects to be completed within the fiscal year, and ensuring they are executed according to law, regulation, and Departmental policies. In addition, SED proposes policies to ensure disciplined and efficient systems engineering and acquisition process for S&T.

Management's Response

Management generally concurred with the contents of this report. We incorporated some changes to the report based on their comments.

Issues for Future OIG Reviews

As we studied the S&T in order to understand its mission and how its offices and divisions operate in the fulfillment of the directorate's mission, we identified several issues that may be suitable for OIG follow-up reviews. These issues do not necessarily identify organizational weakness. Rather they highlight issues that either impede the S&T's ability to become fully operational or are areas that will further clarify the role of the IAIP as the nation's premier protector against terrorist attacks.

Procedures in the selection of the Fellowship Programs and Centers for Excellence Program require further review

To attract some of the nation's most talented scientists and engineers into its programs and build partnerships among laboratory and university researchers, S&T established two programs: the Homeland Security Centers of Excellence program and the Scholars and Fellows program. The budget for these programs increased from \$3 million in FY 2003 to \$70 million in FY 2004.

Among the initial 70 responses reviewed by DHS and outside advisors to establish the first Homeland Security Center for Excellence (HS-Center), 12 were selected to submit full proposals. During November 2003, DHS announced the selection of the University of Southern California (USC) as its first HS-Center. USC is entrusted with the task of studying risk analysis related to the economic consequences of terrorist threats and events.

Open to all U.S. citizens, the Fellowship program attracted 2,500 graduates, of which 102 were awarded scholarships. According to National Science Foundation standards, more than 100 experts from a variety of fields including physical, biological, social and behavioral sciences, engineering, mathematics, and computer science reviewed these applications. These scholars are pursuing academic programs that are consistent with the DHS mission.

We could review how S&T selects the HS-Centers, how it ensures that the Centers fulfill their assignments, and how the fellowship funds are allotted and used to achieve the homeland security purposes in integration with the rest of S&T's responsibilities.

The S&T must maintain close relationships with other DHS elements, especially with the IAIP

To successfully select the best new technologies that support a cohesive and integrated national plan for homeland security, it is critical for the S&T to have a clear understanding of: (1) the terrorist threat picture facing the nation, and (2) the current technical capabilities and ongoing research and development initiatives of other DHS elements. By having a clear understanding of these essential factors, the S&T will be better able to prioritize its investment decisions and avoid duplicating technology initiatives by other DHS components.

While many S&T executives agreed with the importance of maintaining a relationship with IAIP, personnel below them were not actively involved in obtaining terrorist threat information from IAIP and incorporating it into S&T's selection of new technologies for homeland security. On a different level, however, S&T personnel were actively pursuing working relationships with the IAIP to assist with developing the next generation of threat vulnerability and risk assessment tools for the IAIP. Although S&T personnel were attempting to support the IAIP in this manner, the relationship between S&T and IAIP may not be as close as it should be. S&T personnel attributed the relationship with their IAIP counterparts as not being as close as it should to the following factors: (1) IAIP management not being aware of what S&T programs have to offer, (2) difficulties working with the Chief Information Officer's delegates to the IAIP, and (3) IAIP staff being heavily focused on operational concerns and daily threat information.

Other DHS elements may be involved in research and development initiatives that diverge from the DHS strategic plan for new technology investment being developed by the S&T. For example, on January 21, 2004, the OIG was invited to the Transportation Security Administration (TSA) for a briefing and demonstration of the tools being developed by TSA to conduct threat vulnerability and risk assessments. According to the briefing, substantial funding already has been invested in developing such tools. The TSA demonstrated successfully a tool that utilized the Internet to promote interaction between end-users such as the New York City Port Authority and the TSA. However, TSA program

managers were not actively seeking to coordinate their research and development investments with the IAIP, and did not know whether S&T was active in the area of seaport security.

Section 302, subsections (2) and (12) of the HSA, requires the S&T to coordinate with other executive agencies, including those within the DHS, to develop an integrated national policy and strategic plan for identifying and procuring new technologies designed to safeguard the nation. Subsection (13) specifically requires coordination between S&T and other executive agencies to reduce duplication and identify unmet needs when selecting technologies to further review and develop, and subsection (3) specifically requires S&T to support the IAIP in assessing and testing homeland security vulnerabilities and possible threats. Given the emphasis on coordination between the S&T and other executive agencies in the HSA, a future review could identify and make recommendations to improve areas where this kind of coordination is not occurring.

S&T needs to assess the vulnerability of the foreign human capital factor in light of security requirements imposed on foreign students and other aliens with expertise in science and engineering.

The National Science Foundation Act of 1950 established the National Science Board, which is the governing board of the National Science Foundation (NSF). The NSF mission is to (1) promote the progress of science, (2) advance the national health, prosperity, and welfare, and (3) secure the national defense. On August 14, 2003, the National Science Board issued a report titled *The Science and Engineering Workforce Realizing America's Potential*. According to the report, it is more essential than ever to think about workforce development in a global context. Progress in science and engineering relies on knowledge and skills found throughout an international community. Also, according to the report, our nation needs the perspectives and talents of both the native-born and foreign-born for the best possible science and engineering workforce.

Foreign students enrolled at U.S. colleges and universities are encountering visa problems when entering the U.S. because of a government crack down after the September 11, 2001, terrorist attacks on our nation. Before September 11, 2001, it took students entering the U.S. about two weeks to get a student visa. Recent news articles stated that in 2003 foreign students had to wait approximately 6 months to receive their visas in order to enter the U.S. America needs to attract

the world's most accomplished students, scientists, and engineers and encourage them to share their capabilities with us.

On the other hand, over 583,000 foreign students attend U.S. colleges and universities. One third or more of all U.S. science and engineering doctoral degrees and 40 percent of PhD's in computer science go to foreigners. One-third or more of the research assistants in academic laboratories are foreigners. S&T will need to assess whether, and how, to accommodate these facts when funding academic research involving potentially highly sensitive homeland defense efforts, and balance the benefit gained from obtaining foreign students' intellectual skills with the cost of securing the country.

Prudent project management is key to S&T's success and to ensure that the nation maintains trust in S&T's efforts. This is especially true for S&T projects that depend on agreements with other federal entities.

S&T works closely with national laboratories, universities, and the private sector for research and development for creating new technologies to address terrorist threats. S&T owns two of these national laboratories: Plum Island and Environmental Measurements Laboratory. However, S&T also relies on laboratories owned and operated by other federal agencies, such as the Department of Energy, and universities to fulfill S&T's mission in regards to research and development.

Some of the national laboratories have come under public scrutiny because of problems disclosed at the laboratories. To illustrate, a local California newspaper published an article on security concerns at the University of California Lawrence Livermore National Laboratory. According to the article, the laboratory is not fit to effectively resist a terrorist attack because of (1) ineffective and unsafe security procedures, and (2) high attrition rates and inadequate training to handle radioactive materials. Also, the article discussed millions of dollars in unaccounted lab property.

According to a November 2003, newspaper article, a number of deficiencies exist at the Plum Island Laboratory that is owned and operated by DHS, and need to be fixed.

Prudent business practices warrant that management oversight procedures should be in place to protect S&T's interest in ensuring that laboratories deliver what is expected and that the government is protected. This is especially true for national laboratories and university facilities that S&T does not own, but depends on to satisfy S&T mission.

S&T should have provisions in their agreements with non-DHS entities that require protective security measures, and other factors for prudent oversight of S&T's projects. Also, S&T should have procedures in place to monitor the laboratories' compliance with these requirements.

S&T should ensure that proper controls are in place when using Other Transaction Authority.

The HSA of 2002 statutorily gave OTA to the DHS for research and development projects. OTA gives DHS, specifically the S&T Directorate, flexibility in engaging non-traditional vendors, including contractors that are reluctant to do business with the federal government because of its unique accounting requirements and inability to freely negotiate intellectual property rights. OTA authority allows the S&T Directorate to function more like a commercial partner and negotiate flexible agreements that protect the DHS's interest.

However, according to the HSA, the OTA is only in effect for a five-year period following the effective date of the HSA. Furthermore, not later than two years after the effective date of the HSA, and annually thereafter, the Comptroller General shall report to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate on: (1) whether the OTA attracts nontraditional government contracts and results in the acquisition of needed technologies, and (2) if such authorities were to be made permanent, whether additional safeguards are needed with respect to the use of such authorities.

If DHS fails to prove that the use of OTA attracted nontraditional government contracts and put the proper controls in place regarding the use of OTA, then OTA may not be renewed at the end of the 5-year period as prescribed in the HSA. This could have a devastating effect on S&T's ability to quickly implement new technology in the field.

We could conduct a review to determine if S&T's use of OTA has met the intent of Congress. The objective of the review could be to determine whether S&T's

use of OTA did attract non-traditional vendors and quickly implemented new technologies necessary to protect our nation. This review could also determine if sufficient management controls were in place to ensure that the benefits gained were commensurate with reasonable cost incurred.

S&T Major Responsibilities Outlined in the HSA	
No.	Statutory Responsibility
1	Advising the Secretary on research and development efforts and priorities in support of the DHS mission
2	Developing a national policy and strategic plan for coordinating the federal government's civilian efforts to identify and develop countermeasures to terrorist threats
3	Assisting in assessing and testing homeland security vulnerabilities and possible threats
4	Leading DHS and national research efforts to prevent importation of terrorist weapons and materials and preventing or responding to terrorist attacks
5	Establishing a system to transfer homeland security developments and technologies to federal, state, local, and private sector partners

Appendix B
 Budget and FTE Statistics for Fiscal Years 2003 and 2004

Budget and FTE Statistics for Fiscal Years 2003 and 2004				
Programs/Salaries & Expenses/Office of the Under Secretary	FY 2003		FY 2004	
	FTE	Budget (\$000)	FTE	Budget (\$000)
Biological Countermeasures	57	362,600	63	198,500
Nuclear & Radiological Countermeasures	4	75,000	22	127,000
Threat & Vulnerability, Testing and Assessment (TVTA)	7	36,100	18	93,500
National Biodefense Center		88,000
Rapid Prototyping/Technical Support Working Group (TSWG)	4	33,000	5	75,000
University & Fellowships Programs	1	3,000	2	70,000
Critical Infrastructure Protection		6,500
Chemical Countermeasures	2	7,000	10	52,000
Standards/State & Local Program	3	20,000	4	39,000
Conventional Missions	10	34,000
Emerging Threats	1	16,750	4	21,000
High Explosives Countermeasures	2	9,500
S&T Salaries & Expenses	39,000
Office of the Under Secretary	5,168
Total	79	553,450	140	918,168

RDT&E Program Nomenclature⁶		
No.	Title	Description
6.1	Basic Research	Supports research that produces new knowledge in a scientific or technological area of interest to the military.
6.2	Applied Research	Supports the exploratory development and initial maturation of new technologies for specific military application (or further developing existing technology for new military applications).
6.3	Advanced Technology Development	Supports larger scale hardware development and integration and experiments that can demonstrate capability in more operationally realistic settings.
6.4	Demonstration and Validation	Supports the initial development and demonstration of a product designed specifically to meet an agreed upon set of performance standards associated with a validated operational need.
6.5	Engineering and Manufacturing Development	Supports the continued development and refinement of a specifically designed product that has demonstrated it can meet performance requirements and development of the necessary manufacturing processes needed to build that product.
6.6	Management Support	Supports the overhead costs associated with managing the RDT&E activities and running facilities.
6.7	Operational Support Development	Supports the continued improvement and upgrading of products already in production.

⁶ Source: CRS Report for Congress, *Defense Research: A Primer on the Department of Defense's Research, Development, Test and Evaluation (RDT&E) Program*, updated July 14, 1999.

S&T Portfolios		
Port No.	Name	Description
Port-01	Biological Countermeasures	This portfolio provides the science and technology required to decrease the likelihood and potential impact of a biological attack on our civilian population, infrastructure, or agricultural system.
Port-02	Border & Transportation Security	This portfolio ensures that research, development, test and evaluation (RDT&E) activities in relation to the homeland security are consistent with the goals and objectives of the BTS, the S&T Directorate, and the National Security Strategy.
Port-03	Chemical Countermeasures	This portfolio provides the science and technology required to diminish the country's vulnerability to chemical attacks on our civilian population and infrastructure.
Port-04	Threats & Vulnerability, Testing & Assessments (TV/TA)	This portfolio enhances the intelligence and vulnerability analysis of the DHS.
Port-04a	TV/TA -- Physical Security	This program is expected to significantly improve the capabilities of our nation to physically protect its critical infrastructure and key assets.
Port-04b	TV/TA -- Critical Infrastructure Protection – Modeling, Simulation, and Analysis Program (CIP-MSAP)	The program has three essential goals: a) develop, implement, and evolve a rational approach for prioritizing CIP strategies and resource allocations using modeling, simulation, and analyses to assess vulnerabilities, consequences, and risks; b) propose and evaluate protection, mitigation, response, and recovery strategies and options; and c) provide real-time support to decision makers during crises and emergencies.

S&T Portfolios		
Port No.	Name	Description
Port-06	Cyber Security	The portfolio engages in research, development, testing, and evaluation activities along several different dimensions.
Port-07	ERP	
Port-07a	ERP – Technology Development for Emergency Preparedness and Response	The program identifies venues where significant improvements in capability can be facilitated by modern technologies, technology integration and/or advances in basic research.
Port-07b	ERP – State and Local Program	The State and Local Program provides the capability to obtain user requirements from State and Local Emergency Responders to advance the development, implementation, and reassessment of standards for Homeland Security Technologies that support their missions.
Port-07c	ERP – Safe Cities Program	This program supports the nation-wide regional security initiative under the aegis of DHS. Working directly with state and local emergency responders and law enforcement agencies, this program aims to obtain the best available science and technology to prevent, detect, and respond to “all-hazard” emergencies into existing command, control and communication infrastructures.
Port-08	Explosives	During fiscal year 2004, the portfolio will primarily address terrorist attacks against buildings and the general public.
Port-09	International Program	This portfolio supports the Under Secretary in encouraging and facilitating involvement of the world community on homeland security issues.

S&T Portfolios		
Port No.	Name	Description
Port-11	Radiological and Nuclear Countermeasures	This portfolio has a comprehensive strategy to deter a radiological and nuclear attack. It also provides the best available technologies, training, and information to aid in crisis response, incident management and recovery, and attrition.
Port-11a	Preplanned Product Improvements (P3I)	The two goals of this program are: a) to quickly develop and transition enhanced capability to deployed detectors/systems and b) to quickly include recent improvements in prototype technologies into the near commercial offerings of radiological and nuclear detectors/systems used in DHS operational environments.
Port-11b	Detection Technology Initiatives	The program conducts the underlying research and development to develop modern or enhanced technologies for the detection of nuclear and radiological materials.
Port-11c	Incident Management and Recovery	The primary goals of this program are to save human lives, and to minimize environmental and economic impacts.
Port-11d	Systems Architecture and Pilot Deployments	This program focuses on the development of radiological and nuclear countermeasure systems that improve the nation's capability to address the threat of terrorist use of a radiological dispersal device (RDD) or improvised nuclear device (IND) in the U.S.

S&T Portfolios		
Port No.	Name	Description
Port-13	Standards Program	
Port-13a	Biological Countermeasures	This program for biological countermeasures develops comprehensive standards for development, testing, and certification of effective detection, response, remediation, and forensics tools for specific bioagents.
Port-13b	BTS Biometrics	The program for biometrics develops comprehensive standards for the development, testing, and certification of effective technologies for identification, authentication and security of biometric data.
Port-13c	Certification/Attestation/ SAFETY Act Implementation	This program provides the ability for the DHS to perform the conformity assessments for specific homeland security technology tools.
Port-13d	Chemical Countermeasures	This program provides the science and technology required for reducing our country's vulnerability to chemical attacks on our civilian population and infrastructure.
Port-13e	Interoperability of Communication and Information	The program develops comprehensive standards for the development, testing, and certification of enabling technologies for interoperable and compatible detection and information exchange tools.
Port-13f	Conventional Missions Standards Program	The program offers the capability to provide standards, best practices and guidelines to assist conventional missions within DHS to operate effectively and consistently.

S&T Portfolios		
Port No.	Name	Description
Port-13h	IAIP Critical Infrastructure Protection	This program provides the capability for the provision of security standards, best practices and guidelines to protect the nation's critical infrastructure.
Port-13i	IAIP Cyber Security	The program develops comprehensive standards for the development, testing, and certification of effective technologies for the authentication of persons attempting to access information systems and the security of data critical to the needs of homeland security.
Port-13j	Modeling, Simulation and Analysis	The program develops comprehensive standards for the validation and verification of modeling, simulation and analysis tools.
Port-13k	Radiation/Nuclear Countermeasures	The program develops comprehensive standards for the development, testing, and certification of effective detection, response, remediation, and forensics tools for radiological and nuclear materials.
Port-13l	Training	This training program develops comprehensive standards for the development, testing, and certification of effective responders at all levels. It has the ability to provide guidance to local/state/federal homeland security entities regarding the appropriate testing and certification for all levels of emergency responders.

S&T Portfolios		
Port No.	Name	Description
Port-15	Threat and Vulnerability Testing & Assessments	
Port-15a	Advanced Scientific Computing Research and Development	This program supports advanced scientific computing research and development in four technical areas-Simulation Technologies, Discrete and Stochastic Algorithms, Large-Scale Data Integration and Information Extraction, and Computer Science and Mathematics Foundations- and will demonstrate the value of these capabilities to DHS operational assets via pilot projects.
Port-15b	Behavioral Research Program	The three goals of this program are: a) to understand terrorism behavior to the level that enables disruption of both organized and individual terrorist activities, b) to create a reliable method for accurately interpreting indications of threat, both directly communicated and intercepted, and c) to understand the impact and public acceptance of DHS activities to obtain their cooperation.
Port-15c	Biometrics Program	The program's goal is determination of rapid biometrics feasibility which will be conducted on both individual biometrics and fusion approaches.
Port-15d	Integrated Feasibility Experiment (IFE)	The objective of this program is to develop and demonstrate the ability to track terrorists coming across our borders using a quick-start project followed by aggressive research and experimentation effort that is grounded and shaped by the use of real data.

S&T Portfolios		
Port No.	Name	Description
Port-15f	Threat—Vulnerability Integration System Prototype	The program enables analysts to rapidly search, integrate, and gain insight from information that lies buried in terabytes and petabytes of digital information that are overwhelming by today’s standards.
Port-15g	Threat – Vulnerability Mapping and Warning Systems R&D	This program is responsible for advancing the Threat-Vulnerability, intelligence and information analysis, and warning capabilities of the Homeland Security.
Port-15h	Information Analysis -- WMD Assessments Programs	The program establishes an end to end national capability, built on the technical expertise of the Homeland Security community of resources, to assess the validity of communicated threats for all weapons of mass destruction (WMD), to create a comprehensive strategic and current awareness of WMD material flows and illicit trafficking through distributed sensor and information systems integration, to characterize the capabilities of adversaries through integrated analytic and technical teams, and rapidly characterize composition and sources of WMD materials.
Port-16	Secret Service	This portfolio has twin missions- protection and investigations. In addition to protecting our nation’s leaders and visiting world leaders, and also has sole jurisdiction for investigating counterfeit U.S. currency.

Carlton I. Mann, Chief Inspector, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Frank A. Parrott (Team Leader), Senior Inspector, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

M. Faizul Islam, Ph.D., Senior Inspector, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Bradley J. Harp, MBA, Inspector, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Department of Homeland Security

Under Secretary, Science and Technology Directorate, Department of Homeland Security

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to Department of Homeland, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.