A2003:014

Homeland Security and R&D in the United States

Magnus Karlsson

itps
SWEDISH INSTITUTE
FOR GROWTH POLICY
STUDIES

Homeland Security and R&D in the United States

Magnus Karlsson, Science & Technology Attaché
Swedish Institute for Growth Policy Studies
Embassy of Sweden, Washington DC

SWEDISH EMERGENCY MANAGEMENT AGENCY

VINNOVA

SCIENCE · TECHNOLOGY · MEDICINE · Swedish Foundation for Strategic Research

itps SWEDISH INSTITUTE FOR GROWTH POLICY STUDIES

ITPS, Swedish Institute for Growth Policy Studies
Studentplan 3, SE-831 40 Östersund, Sweden
Telephone: +46 (0)63 16 66 00
Fax: +46 (0)63 16 66 01
E-mail info@itps.se
www.itps.se
ISSN 1652-0483
Elanders Gotab, Stockholm 2003

For further information, please contact Magnus Karlsson
Telephone +1 202 467 2654
E-mail magnus.karlsson@itps.se

Foreword

Since the terrorist attacks in September 2001, the concern for homeland security in the United States has defined a market with a significant growth potential. Both public and private investments in science and technology are increasing, and new institutions and policies are emerging in the area of homeland security. These developments will have an impact on researchers, firms and policy-makers also in Sweden, creating opportunities for collaboration, business and information sharing.

The purpose of this report is to create an overview of the structure and funding of homeland security R&D in the United States. The report is relevant for the Swedish science and technology, and security communities and can serve as a basis for further collaboration between Sweden and the United States.

The report has been sponsored by the Swedish Emergency Management Agency, the Swedish Agency for Innovation Systems and the Swedish Foundation for Strategic Research.

Stockholm, December 2003
Sture Öberg

Contents

Executive Summary

- The 9/11 terrorist attacks had a profound impact on America and marked the starting point for a comprehensive reformation of institutions and policies related to homeland security by the Bush administration. Most important was the creation of the new Department of Homeland Security (DHS) that begun operations in March 2003.
- The National Strategy for Homeland Security (July 2002) launched a national R&D effort and set the direction for how new technologies for analysis, detection of attacks, and countering chemical, biological, radiological, and nuclear weapons will be used to help prevent and minimize the damage from future terrorist attacks.
- The purpose of this report is to create an overview of the emerging structure and funding of homeland security R&D in the U.S. The new landscape will take shape during 2003 and will have implications for the Swedish S&T, policy-making and security communities.
- Total homeland security spending will reach 41 BUSD in 2004. The amount set aside for homeland security R&D will be about 3.2 BUSD (compared with almost 68 BUSD for national security and defense R&D).
- DHS R&D portfolio will be about 1 BUSD in 2004 (up 50 percent from 2003). This budget will be spent on research (18 percent), development (66 percent) and on facilities and equipment. The DHS S&T Division will set priorities and coordinate homeland security R&D throughout the federal government.
- The S&T Division will conduct internal research (through a system of national laboratories), support industry and academia (through the Homeland Security Advanced Research Projects Agency – HSARPA) and support educational activities (through university-based Centers of Excellence and fellowship programs).
- Prioritized S&T areas are countermeasures for biological, chemical, radiological and nuclear threats, explosives detection, threat and vulnerability analysis, critical infrastructure protection (a new Cybersecurity R&D Center will be established during 2003), standards for homeland security related equipment and mechanisms for rapidly producing prototyps and deployment of new technologies. The first call for proposals was sent out in May 2003. Foreign entities may participate.
- The National Institutes of Health (NIH) will be responsible for biodefense R&D with a proposed budget of 1.6 BUSD for 2004. Most of these funds will be allocated to the National Institute of Allergy and Infectious Diseases (NIAID). DHS will have a priority-setting role. NIH will administer this research using the existing funding mechanisms.

- Priorities will be to expand basic research for responding to emerging diseases and bioterrorism events, increase the number of candidate drugs and vaccines under research, and expand clinical research projects to support Phase I and II clinical trials of candidate drugs and vaccines.
- Project BioShield has been proposed by President Bush to develop and make available modern, effective drugs and vaccines to protect against biological and chemical attacks. About 6 BUSD will be invested over 10 years. The idea is that the government should guarantee a market for innovative counter terrorism technologies.
- Universities and research institutes are establishing homeland security R&D programs, individually or by creating regional alliances (for example in the mid-Atlantic, New England, Northern California, San Diego and Virginia regions).
- Balancing security and openness is a key concern debated by the research community. Three issues have been discussed in particular: (1) the access to certain biological agents, (2) the control of foreign students and researchers, and (3) the handling of sensitive information.
- Conclusion: Swedish actors should consider agreements and other instruments at the policy-level to promote mutually beneficial exchange of information and people with the U.S. in the field of homeland security. The specific opportunities for Sweden to make these connections will be further explored in a separate report.
- In the preparation of this report, staff from the Swedish Ministry of Foreign Affairs, the Swedish Trade Council and the Defence Department at the Embassy of Sweden has contributed with valuable comments and insights.

1 Homeland Security in the United States

1.1 Responding to 9/11

The terrorist attacks on September 11, 2001 had a profound impact on America and created a political and military response on a global scale. These events also marked the starting point for a comprehensive restructuring and reformation of institutions, policies and legislation related to homeland security by the Bush administration. Right after the attacks, President Bush created the Office of Homeland Security with Tom Ridge, former Governor of Pennsylvania, as Director. The next major step was taken in mid-2002 when the President proposed the establishment of a new Department for Homeland Security (DHS), partly as a response to criticism that he did not take enough action on the issue. A National Strategy for Homeland Security was also released (see table 1-1).

The new department was created by the Homeland Security Act of 2002 (PL 107-296) which was enacted on November 25 after much political controversy. Headed by Secretary Ridge, DHS begun operations on March 1, 2003 with the transfer of about 180000 federal employees in over 20 agencies into the new department (see Appendix A). The event marked the largest reorganization of the federal government since the 1940s and it will take years for the new organization to be complete. DHS has three main tasks as part of its mission: (1) Prevent terrorist attacks within the United States, (2) Reduce America's vulnerability to terrorism and (3) Minimize the damage from potential attacks and natural disasters.

Table 1-1 Some events of restructuring homeland security institutions and policies after September 11, 2001.

September 2001	America attacked by terrorists
October 2001	The Office of Homeland Security (OHS) was created with Tom Ridge as Director
October 2001	Bush signed anti-terrorism legislation (Patriot Act)
March 2002	The Homeland Security Advisory System was established
June 2002	Bush proposed the creation of a new Department for Homeland Security (DHS)
July 2002	A National Strategy for Homeland Security was released by OHS
November 2002	The Homeland Security Act of 2002 was enacted
January 2003	DHS was formally created
March 2003	DHS began operations, Charles McQueary was assigned Under Secretary for S&T

The focus on homeland security has had and will have deep implications for American society. One of the key concerns is to achieve security in a way that preserves a vibrant economy. According to Secretary Ridge, security must be achieved in a rational and thoughtful manner and without corrupting productivity or competitiveness. To maintain both economic vitality and security several elements are required, according to Ridge, including innovation in security related technologies, active participation by the private sector and partnerships among government, private industry and academia (CoC 2002).

1.2 Science and technology

Science and technology (S&T) have created a fundamental change in society during the last decades. For the first time in history, it is possible for individuals and small groups to threaten the lives of large groups of people. Today's terrorists exploit technology for their weaponry (explosives, chemicals, biological agents, radiological devices and so on) and for managing their operations (for example using the Internet, mobile phones and computers). At the same time, science and technology can be used to counter terrorism, supporting such functions as sensing the presence of weapons, data mining, identifying individuals, communicating information and the development of vaccines. In his address to the nation on June 6, 2002, President Bush declared, "In the war against terrorism, America's vast science and technology base provides us with a key advantage".

In the National Strategy for Homeland Security from July 2002, the federal government launched a systematic effort to build a "national R&D enterprise for homeland security sufficient to mitigate the risk posed by modern terrorism" (OHS 2002). This strategy set the direction for how new technologies for analysis, detection of attacks, and countering chemical, biological, radiological, and nuclear weapons will be used to help prevent and minimize the damage from future terrorist attacks. The strategy identified eleven major initiatives in the science and technology area (see table 1-2).

Table 1-2 Eleven major S&T initiatives in the National Strategy for Homeland Security.

1	Develop chemical, biological, radiological, and nuclear countermeasures
2	Develop systems for detecting hostile intent
3	Apply biometric technology to identification devices
4	Improve the technical capabilities of first responders
5	Coordinate research and development of the homeland security apparatus
6	Establish a national laboratory for homeland security
7	Solicit independent and private analysis for science and technology research
8	Establish a mechanism for rapidly producing prototypes
9	Conduct demonstrations and pilot deployments
10	Set standards for homeland security technology
11	Establish a system for high-risk, high-payoff homeland ecurity research

Source: OHS 2002

Even though there are high expectations on science and technology to solve the comprehensive challenges of homeland security and counterterrorism, Secretary Ridge points out that it is important to be realistic about what can be achieved: “We're never going to design a fail-safe system. We will never eliminate the threat. We will never be in a position where we can virtually guarantee that nothing will happen. It's impossible.” (Ridge 2003).

At the same time, it is obvious that a great deal can and must be done. In a recent survey, about 80 percent of 700 federal, state and local agencies responded that current technologies are not adequate for the levels of threat facing the nation today (NCPC 2002).

In the closest future, it can be expected that science and technology take second stage behind more pressing issues such as border and transportation security and immigration. The focus will be on technology transfer and speed. The first task for the new department and its S&T Division is to identify technologies that already exist: “it is more important to find good technologies quickly than to wait to find perfect ones over time” according to Under Secretary Charles McQueary (New 2003).

1.3 About this report

Because of these changes and efforts, we will see a changing R&D landscape in the United States with new priorities, institutions and resources in the area of homeland security. The attention to homeland security and the amount of money injected into the sector will stimulate the creation of new technologies and methods (that will have spill-over effects into other areas), establish new and strengthen existing Centers of Excellence in the U.S. and new companies will emerge to exploit research results and contribute to economic growth. The new landscape will start to take shape during 2003 and it will have implications also outside the U.S., including implications for the Swedish S&T and security communities.

The purpose of this report is to create an overview of the emerging structure and funding of homeland security R&D in the United States. Some of the main questions that the report seeks to answer are:

- How large is federal government funding and what agencies are responsible for performing and financing R&D?
- What will the new science and technology organization look like under the Department for Homeland Security?
- What are the main homeland security R&D areas and how will priority-setting work in the new environment?
- What are the main R&D institutions and organizations related to homeland security?

The findings in this study are likely to be relevant for Swedish policy-makers, research councils and coordinators, researchers and companies dealing with homeland security issues. The report seeks to support these actors to create partnerships, find funding, build networks, identify contact points, explore business opportunities and learn from U.S. policy-making. The specific opportunities for Sweden to make trans-Atlantic connections in the homeland security area will be further explored in a separate report.

1.4 Homeland security publications

A number of public and private organizations have published reports with homeland security analysis and recommendations since 2001. Some of them specifically discuss science and technology issues. See for example *Protecting the American Homeland* by the Brookings Institution (Brookings 2002 & 2003), *Making the Nation Safer* by the National Research Council (NRC 2002*), America – Still Unprepared, Still in Danger* by an independent task force sponsored by the Council on Foreign Relations (CFR 2002), *Defending the American Homeland* by the Heritage Foundation (Heritage 2002), *Planning to Win: A Report on Homeland Security from the Aspen Strategy Group* (Aspen 2002) and several annual reports from the so called Gilmore Commission (see for example Gilmore 2002). A compendium analyzing some of these and other relevant reports have been put together by the RAND National Security Research Division (RAND 2003).

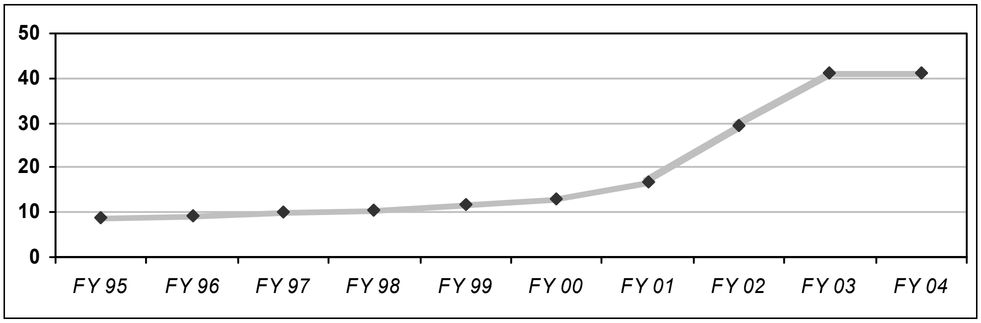
The key strategy documents from the Bush administration are the *National Strategy for Homeland Security*, and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (OHS 2002 & 2003). A good assessment of ongoing homeland security R&D efforts by federal agencies was compiled by the President's Council of Advisors on Science and Technology (see PCAST 2002 and Appendix B). A comprehensive analysis of the 2004 budget proposal relevant for science and technology can be found in AAAS 2003a and additional budget data in CRS 2003. In AAAS 2002, a number of scholars discuss the changing science and research environment in the light of national and homeland security.

2 Homeland Security R&D in Context

2.1 Federal homeland security spending

It is estimated that the total homeland security spending by the federal government for FY (fiscal year) 2003 will reach over 41 BUSD. This means an increase of nearly 150 percent since FY 2001.

Chart 2-1 Federal homeland security spending (in BUSD) from FY 1995 – 2004 (proposed).



Source: O'Gara 2003.

The proposed budget for FY 2004 is of the same amount but it is expected to be revised upwards during the year due to new demands for homeland security spending. Chart 2-1 shows federal homeland security spending over a tenyear period. From this total amount, the proposed budget for the Department of Homeland Security (DHS) for FY 2004 is 36.2 BUSD. Half of that amount (18 BUSD) will be spent to secure borders and transportation systems.

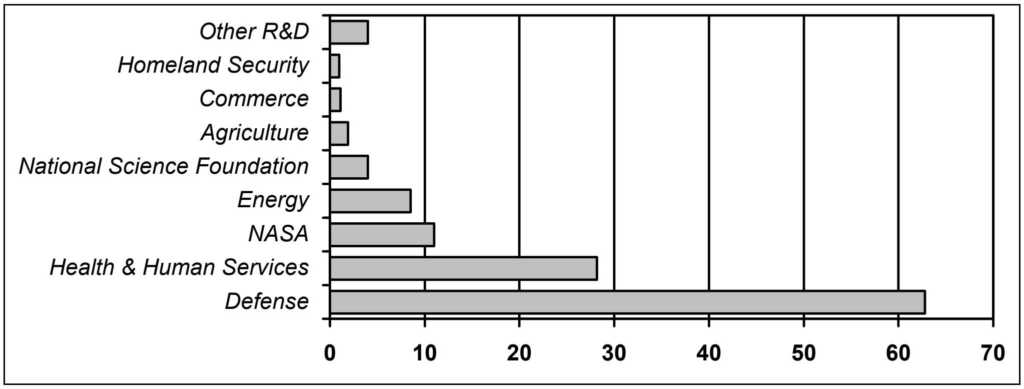
Federal funding for homeland security R&D is a small part of the overall budget but has increased substantially in the last three years. It is estimated that the FY 2004 budget request for all federal R&D to combat terrorism is about 3.2 BUSD (OSTP 2003a). This request includes 1.6 BUSD R&D funding through the Department of Health and Human Services and 1.0 BUSD (up 50 percent from FY 2003) at the Department of Homeland Security.

Combating terrorism will remain a top R&D priority in FY 2005 according to a memo from the administration outlining its R&D investment criteria for the future (OSTP 2003b).

2.2 Related R&D spending

Homeland security R&D spending is small compared to the total R&D enterprise. In 2002, the United States invested an estimated 292 BUSD in R&D, which represented 2.8 percent of its Gross Domestic Product. The largest share of money came from industrial firms (66 percent) and the federal government invested about 81 BUSD (28 percent). The main federal R&D funding sources were the Department of Defense (DoD), the Department of Health and Human Services (HHS), the National Aeronautics and Space Administration (NASA), the Department of Energy (DoE) and the National Science Foundation (NSF). Together these top-five funders accounted for 95 percent of the annual federal investment in R&D. Chart 2-2 shows the proposed federal R&D budget for FY 2004.

Chart 2-2 R&D in the FY 2004 budget by Agency (budget authority in BUSD).



Source: AAAS 2003a.

Homeland security R&D is also small compared to national security (defense) R&D. The defense R&D budget request for FY 2004 is 67.5 BUSD, which represents 55 percent of the total R&D spending of the federal government (more than five times as much as the EU member states together). The DoD accounts for most of this budget and is by far the largest supporter of R&D in the U.S. The FY 2004 request for DoD R&D represents a 7 percent increase over FY 2003, entirely targeted to the development of new weapon systems. However, while the development and engineering part of the proposed budget is increasing, the basic and applied research part is declining steeply (down 8 percent). This means reduced funding for universities, which traditionally absorb one third of these funds. Table 2-1 shows the breakdown of defense R&D on different types of activities estimated for FY 2004. DARPA plays a major role in defense R&D and will receive 3 BUSD of the amount proposed for DoD Science and Technology. This is up 10 percent from 2.7 BUSD in FY 2003.

Table 2-1 National security and defense R&D budget proposal for FY 2004 in BUSD.

Defense R&D	67.5
DoE & DHS R&D	4.7
DoD indirect R&D support	1.0
DoD R&D, technology & engineering	61.8
1) System development and engineering	51.6
2) "Science & Technology"	10.2
• Basic research	1.3
• Applied research	3.7
• Technology development	5.2

Sources: AAAS 2003a, Foster 2003.

Second after DoD in R&D spending is HHS. The proposed budget for FY 2004 is 28.2 BUSD and most of it will be directed towards the National Institutes of Health (26.9 BUSD, up 2.7 percent from FY 2003). The largest increase (17 percent, up to 4,3 BUSD) within NIH goes to the National Institute of Allergy and Infections Diseases (NIAID) due to specific initiatives in the area of biodefense research (see below).

Appendix B lists R&D entities or activities that are relevant to homeland security from several government departments and agencies.

2.3 The security market

Part of the federal budget for homeland security will translate into business opportunities for security companies, system providers and system integrators. See O'Gara 2003 for a recent analysis of the homeland security market (and their prioritized list of investment opportunities in table 2-2). Major security firms are setting up homeland security business units to access as many government contracts as possible. Start-up and small firms are also looking at federal contracts to compensate for the commercial market downturn. Venture capitalists are pushing start-up firms to determine how to sell to the government, particularly in the information technology market, according to the National Venture Capital Association. With security issues a top priority in most government and private sectors, the security industry is expected to grow. The private sector is estimated to spend at least 40 BUSD on security services and products during 2003 (Shetty 2003, Vaida 2003).

Table 2-2 A list of opportunities in homeland security, prioritized according to investment attractiveness.

1	Cargo-screening technologies for weapons of mass destruction (WDM) at ports
2	First responder equipment
3	Multimodal cargo security - tracking and authentication
4	Screening technology for aviation security
5	Physical security upgrades
6	Airport security upgrades
7	Homeland security training
8	International trade security compliance
9	Interoperable communications for first responders
10	Research on biological countermeasures

Source: O'Gara 2003.

3 R&D at the Department of Homeland Security

3.1 Outline and resources

When the new department was created by the Homeland Security Act in November 2002, the final legislation differed from the original proposal by President Bush (introduced in June 2002, White House 2002a) in two respects related to R&D:

1) Congress established an Under Secretary for Science and Technology reporting directly to the Secretary of Homeland Security (Tom Ridge). The under secretary will head the Division for Science and Technology and serve as the scientific and technical advisor to the Secretary. Dr. Charles E. McQueary, a mechanical engineer and retired president of General Dynamics, was assigned to this post on March 19, 2003.
2) The original proposal would have transferred 1.5 BUSD in bioterrorism R&D programs to DHS from the Department of Health and Human Services (HHS). The final bill kept these programs at HHS but the Secretary of DHS was given authority to set priorities for these funds.

A Homeland Security Transition Planning Office (TPO) was established in mid-2002 and a specific TPO team was focusing on the science and technology transition, mapping out logistical options and reorganization details for the new R&D structure. The main reorganization steps to be taken during 2003 are outlined in the Homeland Security Reorganization Plan submitted to Congress by the President in November 2002 (White House 2002b).

Table 3-1 R&D in the Department of Homeland Security (budget authority in MUSD).

	FY 2002 actual	**FY 2003 estimate**	**FY 2004 budget**	**Change FY 03-04**
Science and Technology	147	521	801	54%
Border and transportation security	95	110	172	56%
Coast Guard	19	23	23	0%
Information analysis and infrastructure protection	5	15	5	-67%
Total	**266**	**669**	**1001**	**50%**

Source: AAAS 2003a

The budget for FY 2004, released February 3, 2003 proposed 36.2 BUSD for the entire department. Included in this total was an R&D portfolio of 1.0 BUSD that would turn DHS into one of the major R&D funding agencies in addition to receiving by far the largest percentage of increase in R&D compared to other agencies. The R&D portfolio will include transfer of programs from other agencies as well as newly created R&D programs and performing organizations. The breakdown of these R&D resources on the different divisions or "directorates" within DHS and figures on how the R&D portfolio has evolved since FY 2002 are shown in table 3-1.

The majority of this R&D budget will be spent on development (66 percent). Basic and applied research makes up for 5 and 13 percent of the budget respectively, while the remaining 16 percent will be invested in facilities and equipment (CRS 2003b).

3.2 DHS Science and Technology Division

Most DHS R&D programs will be run from the S&T Division. This means that 80 percent (about 800 MUSD) of the total DHS R&D budget will be under its control. The Division, under the leadership of Under Secretary McQueary, has the responsibility of setting homeland security R&D goals and priorities, coordinating homeland security R&D throughout the federal government, funding its own homeland security R&D, facilitating the transfer and deployment of technologies for homeland security, and advising the DHS Secretary on scientific and technical matters. The estimated FY 2004 budget for different R&D areas in the S&T Division is presented in table 3-2 together with the appropriations bills progress through Congress.

Table 3-2 R&D portfolio of DHS Division of S&T: FY 2004 budget (revised since the February release), the House HS Bill (approved June 24) and the Senate HS Bill (approved July 24) in MUSD.

Research areas	**FY 2004 rev. budget**	**FY 2004 House**	**FY 2004 Senate**
Biological countermeasures	365	293	264
Radiological/nuclear countermeasures	137	130	131
Chemical countermeasures	55	52	55
High-explosives countermeasures	10	10	10
Threat and vulnerability assessments	90	86	98
Conventional missions R&D to assist DHS	55	112	64
Rapid prototyping /TSWG	30	80	70
Standards for homeland defense technologies	25	39	25
Emerging threats	22	21	22
Critical infrastructure protection	5	5	72
University programs and fellowships	10	35	55
Salaries and expenses (House Bill)	-	39	-
Total	**803**	**900**	**866**

Sources: AAAS 2003a & 2003b.

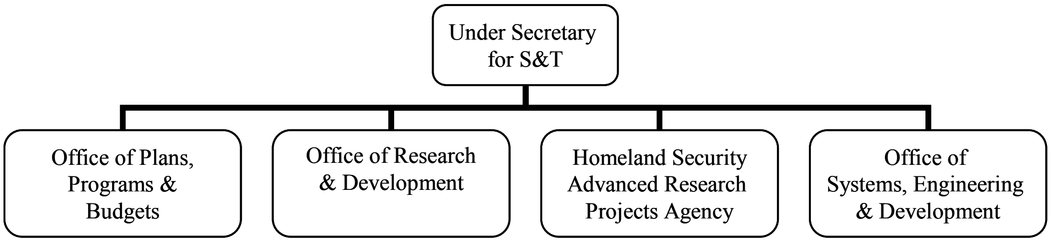
Existing R&D programs in the Department of Defense (DoD), the Department of Energy (DoE), and the Department of Agriculture (USDA) with an estimated value of 521 MUSD in FY 2003 have been transferred to DHS. The majority of these funds come from the newly created National Bioweapons Defense Analysis Center at DoD, which will be responsible for nearly the entire 365 MUSD biological countermeasures portfolio under DHS.

Parts of the Lawrence Livermore National Laboratory (LLNL), such as its Advanced Scientific Computing Research program, are taken over from DoE. In addition, DoE R&D programs focusing on microbial pathogens, national security, nuclear smuggling and other programs within Nonproliferation & Verification R&D move to DHS. The Plum Island Animal Disease Center, Long Island, New York is taken over from USDA.

The S&T Division has three primary activity areas: intramural, industrial and educational activities (see DHS 2003).

1) There is an internal R&D capability consisting of scientists and engineers concentrating on homeland security issues. Key components are the Office of National Laboratories and the Homeland Security Laboratories consisting of components from several DoE laboratories and multiple federal laboratories, respectively.
2) DHS is soliciting innovative ideas from industry and academia, by developing and demonstrating them through a program known as the Homeland Security Advanced Research Projects Agency (HSARPA). The industrial activities will also include efforts to quickly move developed and prototyped technologies at the laboratories into testing and deployment.
3) The S&T Division is supporting those who wish to enter into careers and perform research in fields that are important to the homeland security R&D enterprise. DHS will fund postgraduate and postdoctoral fellowship programs, and create scholarships. In addition, the department will establish Centers of Excellence in academic institutions. HSARPA will engage the academic community through grants and contracts in support of its programs.

Chart 3-1 The organization of the DHS Science and Technology Division.


Under Secretary for S&T
Office of Plans, Programs & Budgets
Office of Research & Development
Homeland Security Advanced Research Projects Agency
Office of Systems, Engineering & Development

Source: DHS 2003.

The organization of the S&T Division is shown in chart 3-1. The Office of Plans, Programs and Budget partners with operational end-users to identify requirements, create strategic initiatives, prioritize investments, and ensure both short-term and long-term goals are met in accordance with national policies. The Office of Research and Development executes the intramural programs in research, development, testing, and evaluation; supports university and fellowship programs; and provides an enduring R&D capability dedicated to homeland security. HSARPA engages industry, academia, government, and other sectors in innovative research and development, rapid prototyping, and technology transfer to meet operational needs. The Office of Systems Engineering and Development executes the transition of large-scale or pilot systems to the field through a rapid, efficient and disciplined project management process.

3.3 R&D in other DHS divisions

One fifth of the FY 2004 DHS R&D budget (200 MUSD) will remain outside the S&T Division.

The Division of Border and Transportation Security will integrate the newly created Transportation Security Administration (TSA) and its aviation security R&D program. The proposed budget for this program is 172 BUSD for FY 2004. In the current plan, the S&T Division will gradually take over the responsibility for these activities over the next couple of years.

The Division for Information Analysis and Infrastructure Protection will have a small R&D budget for FY 2004 (5 MUSD) when the National Infrastructure Simulation and Analysis Center (NISAC) is transferred from DoE. NISAC is a partnership between Los Alamos and Sandia laboratories.

The Division of Emergency Preparedness and Response has no R&D programs within its budget. The S&T Division will fund R&D to improve the ability to respond to disasters.

The Coast Guard is transferred from DoT but will remain an independent entity. Their R&D portfolio of 23 MUSD for FY 2004 will thus become part of DHS.

4 DHS Support Agencies

The reorganization of government departments and agencies are expected to continue for some time. The Homeland Security Act of 2002 stipulated the establishment of several support agencies to the Department of Homeland Security. They are expected to take shape gradually during 2003. The major new support agencies are described below (see AAAS 2003a).

4.1 Homeland Security Advanced Research Projects Agency

The new R&D unit, Homeland Security Advanced Research Projects Agency (HSARPA) is created under the S&T Division of DHS. It is modeled after the existing Defense Advanced Research Projects Agency (DARPA) in DoD. The responsibilities of HSARPA are to award grants for basic and applied research with the purpose to promote revolutionary improvements in homeland security technologies. Ideas from both academia and industry will be considered. HSARPA will be responsible for the entire spectrum of R&D at DHS and have a budget of about 350 MUSD for FY 2004. HSARPA R&D cuts across the other funding categories and its budget is already included in the total S&T budget. Dr. David Bolka, with a background from the U.S. Navy and the telecommunications industry, has been appointed Director of HSARPA. Deputy Director will be Jane Alexander.

The agency will develop and test potential technologies and accelerate the development and deployment of the technologies. HSARPA will administer a specific Acceleration Fund to support innovative homeland security R&D in businesses, Federally Funded Research and Development Centers (FFRDC) and universities. There are indications that the majority of activities will be in development and advanced prototyping and the initial task will be to address immediate gaps in high-priority operational areas, such as protecting critical infrastructure and securing national borders.

HSARPA will address the following crosscutting portfolio areas: cyber, biological, chemical, radiological & nuclear, and high-explosives defense. The new agency will be different from DARPA in the sense that 90 to 95 percent of its resources will be placed against identified DHS needs, roadmaps and requirements. Five to ten percent will be used for revolutionary research for breakthrough, new technologies and systems. It will be similar to DARPA in terms of program management, active technical leadership, wide range of contracting options and a common technology base with Department of Defense.

HSARPA will work with the Technical Support Working Group (TSWG) to make Broad Agency Announcements (BAAs) and create its own website for registering products for DHS purchase. At least 2.5 percent of contracts will be reserved for small businesses as part of the Small Business Innovation Research (SBIR) program (Alexander 2003). The first HSARPA Research Announcement was issued in September 2003 and included a focus on sensors capable of detecting biological and chemical agents.

4.2 Office for National Laboratories

An Office for National Laboratories will be set up by the DHS S&T Division. The purpose is to coordinate DHS interactions with national laboratories (mainly from the Department of Energy) with expertise in homeland security. The idea is to make sure that ongoing activities are utilized and to sponsor new R&D activities at these labs.

The Office has the authority to establish a semi-independent DHS headquarter laboratory within an existing lab or FFRDC. Five such “labs within labs” have been proposed at the following facilities.

- Lawrence Livermore National Laboratory (Administered by University of California), Livermore, CA.
- Los Alamos National Laboratory (Administered by University of California), Los Alamos, NM.
- Sandia National Laboratories (Administered by Sandia Corporation, which is a subsidiary of Lockheed Martin Corp.), Albuquerque, NM.
- Oak Ridge National Laboratory (Administered by UT-Battelle, LLC), Oak Ridge, TN.
- Pacific Northwest National Laboratory (Administered by Battelle Memorial Institute), Richland, WA.

4.3 Other organizational entities

A Homeland Security Science and Technology Advisory Committee consisting of 20 members will be established by the Under Secretary, representing first responders, citizen groups, researchers, engineers, and businesses to provide science and technology advice to the Under Secretary.

A Homeland Security Institute will be established as a Federally Funded Research and Development Center (FFRDC) to act as a think tank for risk analyses, simulations of threat scenarios, analyses of possible countermeasures and strategic plans for counterterrorism technology development.

A system of university-based Homeland Security Centers of Excellence will be developed in response to the Homeland Security Act. The centers will pursue research opportunities in a wide variety of fields related to homeland security and their activities will be coordinated with relevant federal agencies and private institutions. The first call for academic white papers was sent out in July by DHS in a Broad Agency Announcement (BAA). The call focuses on social sciences and more specifically on risk-based economic modeling on the impact of terrorism. White papers should have been submitted in August. Proposals will be evaluated by DHS together with Oak Ridge Associated Universities (ORAU) and the first award announcement is expected in November 2003. Information about the BAA can be found at www.orau.gov/dhsuce/.

5 DHS R&D Priority Areas

5.1 Main R&D areas and activities

The following specific R&D areas and activities for the S&T Division were outlined by Under Secretary McQueary in mid-2003 (McQueary 2003).

Development of **biological countermeasures** to reduce the probability and impacts of a bioterrorist attack. This portfolio includes the following components:

- Develop and implement a Biological Warning and Incident Characterization System (BWIC). The system will consist of three major components: (1) a nationwide bio-surveillance system that looks for early biological indicators of the exposure to biological agents, (2) development of a public health surveillance system together with HHS and its Centers for Disease Control and Prevention (CDC) to detect early adverse health events in the population, and (3) environmental monitoring networks in selected cities that can detect agents directly. A pilot version of this system will be available in FY 2004.
- Continue the National Biodefense Analysis and Countermeasures Center (NBACC) initiated in FY 2003. The center will leverage the expertise of America's cutting-edge medical and biotechnical infrastructure to focus on the biological agent threat. The analytical capabilities of the NBACC will be functional in FY 2004 and coordinated with NIH and the Food and Drug Administration (FDA).
- Work closely with USDA (U.S. Department of Agriculture) in areas of animal disease research and diagnostics. The Plum Island Animal Disease Center of USDA will be transferred to DHS in mid-2003.

The **chemical countermeasures** portfolio will address five specific areas: (1) system studies will be used to prioritize efforts amongst the many possible chemical threats and targets, (2) new detection and forensic technologies will be developed and demonstrated, (3) protective systems that integrate physical security, detection devices, information management and consequence management strategies will be developed and tested in selected facilities such as airports and subways, (4) the S&T Division will cooperate with the Information Analysis and Infrastructure Protection, and the Borders and Transportation Security Divisions to reduce the vulnerability posed by large volume of toxic industrial materials used, stored and transported within the U.S., and (5) work with CDC to coordinate public health response and management of detected events.

Detection of **high explosives** and mitigation is the prime focus of the Transportation Security Administration (TSA). DHS will build on TSA R&D to develop more effective explosives detectors, including reliable standoff detection capability of large quantities of explosives, especially in vehicles.

Radiological and nuclear countermeasures will by addressed with a systems approach that emphasizes early detection, effective intervention capabilities at the federal, state and local levels, development of mitigation technologies and science-based consequence management programs, and effective training at all levels of response.

The **Threat and Vulnerability, Testing and Assessment (TVTA)** program will create advanced modeling and information and analysis capabilities that can be used by the organizations in DHS to fulfill their missions and objectives. The program includes: (1) the development of advanced computing, information and assessment capabilities in support of threat and vulnerability analysis, detection, prevention and response, (2) R&D activities in the area of cybersecurity focusing on areas not currently addressed by the federal government. TVTA infuses new technologies and capabilities into DHS on a regular basis based on strategic five-year road maps.

The **Critical Infrastructure Protection (CIP)** program has three primary goals: (1) develop, implement and evolve a rational approach for prioritizing protection strategies and resource allocations using modeling, simulation and analysis to assess vulnerabilities, consequences and risks, (2) propose and evaluate protection, mitigation, response and recovery strategies and options, and (3) provide realtime support to decision makers during crisis and emergencies.

The **standards program** will provide consistent and verifiable measures of effectiveness of homeland security related equipment and systems in terms of basic functionality, appropriateness for the task, interoperability, efficiency and sustainability. The S&T Division will facilitate the development of guidelines together with both users and developers. The program will develop performance measures, testing protocols, certification methods and a reassessment process appropriate for each threat countermeasure and for the integrated system. This effort will include working with the private sector to establish a network of homeland security certification laboratories.

DHS and the Technology Administration (TA) at the Department of Commerce have signed an agreement to establish cyber-protection standards. A formal working relationship will be established between DHS S&T Division and TA’s National Institute of Standards and Technology (NIST) including research programs for the detection of chemical, biological and other threats. NIST is also working to develop “interoperability” standards for first responders and is doing work on cybersecurity, radiation measurements and biometrics among other initiatives.

The S&T Division will provide **support to other DHS components**, including working with the TVTA and CIP programs described above. The purpose is to assist and enhance their technical capabilities through integrated R&D. R&D in potentially high payoff technologies will be emphasized.

The purpose of the **rapid prototyping program** is to identify the significant capabilities that exist in the private sector for the rapid development and prototyping of technologies in support of the homeland security mission. The S&T Division will work together with the Technical Support Working Group (TSWG) of the Department of Defense to create a technology clearinghouse to encourage and support innovative solutions to enhance homeland security and to engage the private sector in rapid prototyping. Note: TSWG is the U.S. national forum that identifies, prioritizes, and coordinates interagency and international R&D requirements for combating terrorism. The TSWG rapidly develops technologies and equipment to meet the high-priority needs of the combating terrorism community, and addresses joint international operational requirements through cooperative R&D with major allies.

A **homeland security fellowship/university program** will be established to support strategic R&D partnerships with the academic community, including the creation of a fellowship program at DHS in cooperation with the American Association for the Advancement of Science. Fellows will spend one year at the Office of Research and Development within the S&T Division. The fellowship program will begin September 2003 and the first 102 awardees of this program were selected at the end of July. See www.orau.gov/dhsed/ for the 2004 competition.

Finally, the **emerging threats program** will support the exploration of innovative, crosscutting, out-of-the-box approaches for anticipating and responding to new and emerging threats. The program will also establish and support studies and analyses by the new Homeland Security Institute.

5.2 Cybersecurity R&D Center

One of the priority homeland security areas of the U.S. government is cybersecurity; the protection of the critical electronic infrastructure of information networks and systems. It is recognized that active R&D programs are necessary to produce new cybersecurity tools and techniques to ensure the performance of this infrastructure and improve the ability to defend it against cyber and physical terrorism. The overall strategy for securing cyberspace was outlined by the White House in the National Strategy to Secure Cyberspace in February 2003 (White House 2003a).

In line with these intentions, DHS intends to create a Cybersecurity R&D Center to provide a focus for R&D activities in the field and to leverage efforts underway in the defense, intelligence, academia and private laboratory communities. The center will be established with FY 2003 funds and it will be the centerpiece of the DHS research agenda for Information Analysis and Infrastructure Protection (IAIP). According to DHS S&T Under Secretary McQueary, the department has requested 7 MUSD for cybersecurity in FY 2004. Major partners will be the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST) and the Defense Advanced Research Projects Agency (DARPA).

The center will have four primary roles and functions: (1) Promote and coordinate cybersecurity research, innovation and evaluation. It will develop strategic R&D programs, create testing and evaluation programs, and develop test beds and measurement performance standards. (2) Provide communication and coordination between various public and private organizations, and foster national and international cooperation in creating a robust and defensible cyber infrastructure. (3) Support the operational needs of IAIP. (4) Cooperate with NSF to foster educational programs together with participating universities.

The center is created partly in response to concerns by Congress (the House Committee on Science) regarding lack of focus and budget allocation in this field. Both the Cyber Security Research and Development Act of 2002 (PL 107-305) and the Homeland Security Act established new programs and authorized new funds for cybersecurity R&D, but agencies have "not responded effectively" so far, according to House Science Committee chair Sherwood Boehlert (HCS 2003).

5.3 Initial call for research proposals

DHS issued the first in what is expected to be a series of Homeland Security Broad Agency Announcements (BAAs) or "calls for research proposals" in May 2003. The intent of the BAA was to identify technologies and approaches that provide near-, mid-, and long-term solutions that enhance the capabilities of the U.S. government to combat or mitigate terrorism. The focus is on research, development and prototyping. The areas covered by the BAA are listed in table 5-1. This list provides a good indication of the initial R&D interests of DHS. The call closed in June and generated more than 3300 proposals.

The DHS BAA was released by the Technical Support Working Group (TSWG) under the provisions of the Federal Acquisition Regulation (FAR). Research contracts are selected and awarded based on full and open competition under the provisions of the Competition in Contracting Act of 1984 (PL 98-369). The awards under this BAA are planned in late FY 2003 and in FY 2004. Foreign contractors, governments and universities can submit responses to BAAs. A threephase process will be used to evaluate the proposals. In the first phase, a onepage proposal will be reviewed. The government will notify the offeror if a submittal has been accepted and set a new deadline for submittal of a phase two application – a 12 page White Paper. The full application (not more than 50 pages) will be evaluated in the final phase of the selection process (TSWG 2003). See also www.tswg.gov, www.bids.tswg.gov and www.fedbizopps.gov.

Table 5-1 Technology R&D requirement areas in the first DHS Homeland Security Broad Agency Announcement (BAA), May 2003.

CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR COUNTERMEASURES (CB)

Unspecified Requirement - CBRNC

Low-Cost Personal Decontamination System (Chemical)

Statistical Design Tool for Sampling Contaminated Buildings

Low-Cost Personal Decontamination System (Biological)

CBR Mitigation in Mass Transit Terminals

Low Cost Shelter in Place Training and Tools for Public Buildings

Advanced Distributed Learning (ADL) Delivery Architecture and Services

Rapid Education for Medical Professionals

Chemical Agent Risk Assessment Tool

Next Generation Structural Fire Fighting Protective Ensemble

Standoff Maritime Radiological Gamma/Neutron Detector

Transportable Emergency Water Treatment and Distribution

Real-Time Radioisotope Identification and Reporting

Radiation Pager with Integrated Dosimetry, GPS, and 2-way Communications

Efficient Detection of High-Z materials in Cargo

Facility Toxic Industrial Chemical Warning Monitor

Biological Aerosol Threat Warning Detector

Facility Biological Toxin Aerosol Warning Monitor

Portable Biological Toxin Warning Sensor

Characterization of Biological Backgrounds in Facilities

Large-Scale Restoration of Biologically Contaminated Urban Areas

Rapid Semi-Empirical Tool for Estimating Air Flow in Facilities

Direct Detection Assay for Botulinum Toxin

Distributed Real-time Monitoring of Decontamination Conditions

Expedient Mitigation of a Radiological Release

Radiological Decontamination Technologies for Post-event Restoration

Rapid Field Identification of Agricultural Bioterrorism Agents

EXPLOSIVES DETECTION (ED)

Remote Detection of Large Vehicle Bombs

Deployed Screening Equipment Optimization

IMPROVISED DEVICE DEFEAT (IDD)

Integrated Spatial Recognition

INFRASTRUCTURE PROTECTION (IP)

Secure Video Teleconferencing and Document Transfer

Evaluation Test Beds for Information Discovery and Analysis Systems

Confidence Level Capability within Semantic Graphs

Conflicting Data and Data Pedigree within Semantic Graphs

Statistical Data Mining of Network Traffic

Modeling of Computer Networks

INVESTIGATIVE SUPPORT AND FORENSIC (IS)

Unspecified Requirement - Investigative Support and Forensics

Age Determination of Biological Evidence

Hyperspectral Imaging System for Forensic Examination

Cockpit Voice Recorder Transcription and Timing Tool

Long Range Non-Line-Of-Sight Wireless Video Transmission System

Real Time Remote Detection of Threat

Data Recovery from Damaged or Erased Advanced Storage Media

PERSONNEL PROTECTION (PP)

MANPADS Countermeasures

PHYSICAL SECURITY (PS)

National Rail System Passenger/Baggage Screening

Sea Mine Detection System

Underwater Loudhailer

Breach Control Barriers for Public Access Areas

Secure Authenticated Mobile Awareness System

Improved Mass Transit Surveillance and Early Warning System

Source: TSWG 2003.

6 Biodefense Programs and Initiatives

6.1 NIH biodefense R&D program

The anthrax letter attacks of October 2001 revealed major inadequacies in the existing methods for fighting bioterrorism. President Bush responded by a vast increase of the budget for biodefense in 2002. The next year (FY 2003) 5.9 BUSD was allocated for defending against biological terrorism in three areas: (1) Improve state and local health systems. (2) Improve capabilities to respond in the event of a bioterrorist incident. (3) Biodefense research and development.

The National Institutes of Health (NIH) budget proposal for biodefense R&D FY 2004 amounts to 1.6 BUSD. Most of these funds will be allocated to the National Institute of Allergy and Infectious Diseases (NIAID). The DHS Secretary will have a priority-setting role, but no funding authority, for human health-related R&D on terrorist threats. NIH will administer the research grants using the existing funding mechanisms.

The number one priority is to support research needed in the war on terrorism. This includes research on agents with bioterrorism potential and applied research and development of vaccines. Key priorities will be to: (1) Expand basic research to provide and maintain the R&D capacity necessary for identifying and responding to emerging diseases and bioterrorism events. (2) Increase the number of candidate drugs and vaccines under research. (3) Expand clinical research projects to support Phase I and II clinical trials of candidate drugs and vaccines.

Table 6-1 NIAID High Priority Biodefense Products.

1	High titer/concentrated Vaccinia Immune Globulin (VIG) or replacement product based on monoclonal antibodies (Mabs)
2	Botulinum antitoxin including: safe and effective alternatives to toxoid vaccine, monoclonal antibodies, and polyclonal antibodies
3	Development of an alternative vaccine against smallpox that could be delivered to those at high risk of serious complications to the current vaccinia vaccine (e.g., MVA)
4	Second generation anthrax vaccines (e.g., rPA)
5	Ebola and Marburg hemorrhagic fever vaccines
6	Tularemia vaccines
7	Plague vaccines
8	Rift Valley Fever vaccines
9	Cell culture (e.g. Vero cells) based vaccines for influenza
10	Antivirals for smallpox and viral hemorrhagic fevers
11	Arenavirus and specific viral encephalitis vaccines (e.g., Tickborne encephalitis viruses, West Nile virus, Eastern equine encephalitis virus, Western equine encephalitis virus)

Source: National Institute of Allergy and Infectious Diseases.

According to the NIAID strategic plan, a number of agents ("select agents") that are recognized as having bioterrorism potential will be the focus of initial research activities. Table 6-1 outlines high-priority biodefense product areas that are the focus of NIAID R&D. The scientific needs and areas of research emphasis have been divided into six sections: biology of the microbe (the basic biology and disease-causing mechanisms of pathogens), host response (understanding the complex parameters of innate and adaptive immunity), vaccines, therapeutics, diagnostics and the creation of the necessary research resources (including the establishment of several regional Centers of Excellence for Bioterrorism and Emerging Diseases Research) (NIAID 2002, AAAS 2003a).

6.2 Project BioShield

It is a fact that effective countermeasures do not exist for many of the biological threats deemed most dangerous by the Centers for Disease Control and Prevention (CDC). In his State of the Union Address at the end of January 2003, President Bush announced Project BioShield to address these issues. According to the proposal, 6 BUSD will be invested over 10 years to develop and make available modern, effective drugs and vaccines to protect against biological and chemical attacks. The idea behind the proposal is that the government should guarantee a market for innovative counter terrorism technologies deemed not to have a viable commercial market on their own.

The plan consists of three basic parts: (1) The creation of a permanent funding authority to stimulate the development of "next generation" medical countermeasures to allow the government to buy vaccines and drugs for smallpox, anthrax, botulinum toxin and other dangerous pathogens such as Ebola and plague. DHS and HHS will collaborate to identify critical countermeasures by evaluating likely threats and new opportunities in biomedical R&D. (2) Speeding up NIH development capabilities by giving the Director of the National Institute of Allergy and Infectious Diseases (NIAID) increased flexibility to award contracts and more rapid hiring of technical experts. (3) Giving the Food and Drug Administration (FDA) the ability to make promising, but yet unlicensed, treatments quickly available in emergency situations.

It is expected that the proposed investment into American biotechnology and pharmaceutical R&D to counter terrorism will have consequences for the usual civilian R&D carried out by the same organizations: "the breakthroughs resulting from Project BioShield are likely to have important spillover benefits in diagnosing and treating other diseases, and in strengthening our overall biotechnology infrastructure" (White House 2003b).

Some parts of the proposal are seen as controversial. Critics say that biotech and pharmaceutical companies will require even more incentives than contained in the proposal. Other incentives being considered include the protection from litigation, tax and intellectual property incentives (CRS 2003c). The House approved the proposal in July, but it remains stalled in the Senate as of August 2003.

7 R&D Coordination and Oversight

7.1 R&D priority-setting and coordination

The coordination mechanisms for homeland security R&D have been complex and according to some analysts both fragmented and inadequate, also before 9/11. It has been argued that R&D has been under-funded, not well prioritized, fragmented across many departments, wastefully duplicated and not clearly related to security requirements (CRS 2002b).

The interagency coordination, priority setting and the conduct of counterterrorism and homeland security R&D programs has been the subject of analysis and recommendations (see the publications discussed above) during the last couple of years. Still in April 2003, a Congressional Research Service report urged DHS to clarify its R&D procedures. It was unclear how DHS will set priorities for its support agencies such as HSARPA and the Homeland Security Institute, according to the report. Moreover, it remains to be demonstrated how DHS will influence R&D activities outside the department, for example at NIH, and how will other relevant R&D agencies with no formal role in DHS's R&D priority-setting process be handled. Finally, it is necessary to specify the interaction with other counterterrorism coordination mechanisms within the administration (CRS 2003b).

The following is a summary of interagency coordination for counterterrorism R&D and the agencies involved in 2002 before DHS was established (CRS 2002b).

The **National Security Council (NSC)** had a Preparedness Against Weapons of Mass Destruction Group – Subgroup on R&D (chaired by OSTP, TSWG was a member)

The **Office of Homeland Security (OHS)** had the Homeland Security Council (HSC). The Council had a (1) Policy Coordinating Committee (PCC) on R&D (led by OSTP Assistant Director for National Security), (2) PCC on Public Health Preparedness, and a (3) Homeland Security Advisory Council with Senior Advisory Committees (included PCAST members).

The **Technical Support Working Group (TSWG)** that coordinated and funded R&D for technologies to combat terrorism that where useful to more than one agency (headed by Department of State and DoD)

The **Office of Science and Technology Policy (OSTP)** had responsibilities for (1) Immigration Policy, (2) Border Technology, and (3) a Counter-Nuclear Smuggling Working Group (linked to OHS).

OSTP was also a member of (1) the Non-Proliferation and Arms Control Technology Working Group (led by the Department of State), (2) the Counter Proliferation Program Review Committee (chaired by DoD), and (3) the Interagency Group to develop guidelines for select agent regulations (together with HHS and USDA).

Moreover, the OSTP Assistant Director for National Security was also the OHS Senior Director for R&D. OSTP had relationships with the National Academies of Science, Engineering and Medicine. OSTP had its own FFRDC that did counter-terrorism work: the RAND Science and Technology Policy Institute (STPI).

The **National Science and Technology Council (NSTC)** was managed by OSTP and had an Antiterrorism Task Force with five working groups: (1) Radiological, Nuclear and Conventional WG, (2) Biological and Chemical Preparedness WG, (3) Rapid Response WG, (4) Social, Behavioral and Educational Sciences WG, and (5) Protection of Vulnerable Systems WG.

The **President's Council of Advisors on Science and Technology (PCAST)** under OSTP had a Panel on Combating Terrorism (which is a member of the Senior Advisory Committee of the Homeland Security Advisory Council).

Table 7-1 Members of the Homeland Security Advisory Council (HSAC).

HSAC Chair: Joseph J. Grano, chairman and CEO of UBS Paine Webber and a veteran of the U.S. Special Forces.

Vice Chair: William H. Webster, former director of the FBI and CIA.

Richard A. Andrews, Senior Director, National Center for Crisis and Continuity Coordination.

Kathleen M. Bader, Business Group president with Dow Chemical Co.

David Arthur Bell, chairman and CEO of the Interpublic Group of Companies.

Jared Cohon, president of Carnegie Melon University.

Ruth David, president and CEO of ANSER, Inc.

Lee Herbert Hamilton, director of the Woodrow Wilson International Center for Scholars.

Michael Leavitt, governor of the State of Utah.

James T. Moore, commissioner of the Florida Department of Law Enforcement.

James Rodney Schlesinger, chairman of the Board of Trustees of the MITRE Corp.

Sidney Taurel, chairman, president and CEO of Eli Lilly and Co.

Lydia Waters Thomas, president and CEO of Mitretek Systems, Inc.

Anthony Williams, mayor of the District of Columbia.

Ex Officio members of the HSAC

Norman R. Augustine, represents the Panel on Science and Technology of Combating Terrorism, on the President's Council of Advisors on Science and Technology (PCAST).

Vance D. Coffman, chairman and CEO of Lockheed Martin Corp., represents the National Security Telecommunications Advisory Committee (NSTAC).

Richard K. Davidson, chairman and CEO of Union Pacific Corp., represents the National Infrastructure Advisory Committee (NIAC).

Christopher J. Furlow will serve as Executive Director of the Homeland Security Advisory Council.

Source: Department of Homeland Security.

7.2 Homeland Security Advisory Council

The new Homeland Security Advisory Council (HSAC) has been established with the purpose to provide advice and recommendations to the Secretary on matters related to homeland security. The 18-member Council is comprised of leaders from state and local government, first responder communities, the private sector, and academia. HSAC members were named on June 25 (see table 7-1) and the council had its first meeting on June 30, 2003. HSAC replaced the President's Homeland Security Advisory Council (PHSAC) that was dissolved on March 31, 2003.

7.3 National Science and Technology Council

A revised structure at the National Science and Technology Council (NSTC) is under implementation. A new Committee on Homeland and National Security has been established with the purpose to coordinate security-related science and technology activities across federal agencies. Headed by John H. Marburger, Director, Office of Science and Technology Policy (OSTP), the committee will be co-chaired by Shana Dale from OSTP, Michael Wynne from Department of Defense and Charles McQueary from DHS. There will be six subcommittees: (1) National Security & Intelligence R&D, (2) Radiological and nuclear, (3) Medical countermeasures, (4) Standards, (5) Social, Educational & Behavioral (joint with the NSTC Committee on Science) and (6) Infrastructure (joint with the NSTC Committee on Technology).

7.4 Congressional oversight

The House Select Committee on Homeland Security, formally organized in February 2003, has the authority to coordinate all House oversight of the Department of Homeland Security. The Select Committee has 50 members and includes the chairs of relevant oversight committees.

As of mid-2003, Senate oversight remains with the Government Affairs Committee.

8 R&D Institutes, Universities and Partnerships

Research institutes and universities are positioning themselves to get federal homeland security funding. Apart from new educational and research programs, their strategies include setting up new facilities and forming partnerships and alliances. Here are some examples:

The University of Pennsylvania established the **Institute for Strategic Threat Analysis and Response (ISTAR)** following the 9/11 attacks. Broadly-based multidisciplinary teams and faculty members conduct studies of the causes and consequences of strategic threats both nationally and internationally. Moreover, in Pennsylvania, four state and private universities have formed the **Pennsylvania Keystone Alliance** to serve as the state's research and educational partnership for homeland security. The alliance includes the University of Pennsylvania, the University of Pittsburgh, Penn State University and Carnegie Mellon University. These schools are also members of the nine-member **Mid-Atlantic Universities Consortium** for Homeland Security. The other members are University of Maryland, Johns Hopkins University, Princeton University, Rutgers University and the University of Delaware.

The **MIT Committee on the Protection of Human Life and Infrastructure** was formed in October 2001 to assess the institutional assets and capabilities for addressing homeland security. Key areas of strength at MIT were identified: transportation security, chemical and biological defense, international relations, computational modeling and cognitive systems, network and computer security, and risk management. In a separate initiative, initial work has been done to establish a homeland security alliance for universities from all of **New England**.

The **Bay Area in Northern California** is promoted by the Bay Area Science Infrastructure Consortium (BASIC). The region offers a strong R&D infrastructure relevant for homeland security issues: (1) Five leading research universities (Stanford University and University of California at Berkeley, Davis, San Francisco and Santa Cruz). (2) Five national research laboratories (E. O. Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, NASA Ames Research Center, Sandia National Laboratories and Stanford Linear Accelerator Center). (3) International independent research centers, such as Electric Power Research Institute and SRI International. (4) Companies that represent the largest global concentration of industry in biotechnology and information technology, as well as venture capital. According to BASIC, the Bay Area is leading the next wave of innovation – the integration of bio, nano and information technologies and medical research.

The **San Diego Regional Network for Homeland Security** was established in 2002 by San Diego State University and University of California, San Diego. Involving interested public and private organizations, the network seeks to evaluate regional first response capability and needs, and develop strategies to fill the gaps – either through regional partnerships leveraging local resources or by working together to pursue funding opportunities at the state and federal level.

The **Virginia Institute for Defense and Homeland Security (IDHS)** was created in February 2003. It is an interdisciplinary consortium of universities collaborating with industry to conduct collaborative basic and applied research. It will emphasize R&D in the fields of information technology and telecommunications, biodefense, sensor systems and risk assessment and management. Virginia's Center for Innovative Technology (CIT) will house IDHS and help bring together the 14 universities and industry representatives.

Michigan's Big Three universities – Michigan State University, the University of Michigan and Wayne State University – are exploring the establishment of a joint antiterrorism research institute. Activities at the universities today include a bioterrorism preparedness initiative, training programs at the newly created Global Community Security Institute and social research that focus on the roots of terrorism.

A somewhat different action was taken in **New Mexico** when the New Mexico Institute of Mining and Technology and New Mexico State University teamed up to buy the small town of Playas with DHS money. The town and the surrounding land were bought for 5 MUSD and will be turned into a national first-responder training facility. Apart from emergency response training, the town will be used for bioterrorism research.

A homeland security institute has been created by the **University of Nevada, Las Vegas** in 2003. The university collaborated with Bechtel Nevada, which runs the National Counterterrorism Range Complex at the Nevada Test Site. The institute will focus on training students and first responders to deal with biological and chemical weapons attacks.

Purdue University, Indiana, also established a homeland security institute recently. The objectives will be based on the national strategy for homeland security. The institute will create teams of researchers from several disciplines to tackle specific types of terrorist threats.

Ohio State University has established a consortium (National Academic Consortium for Homeland Security) of more than 50 universities and research institutions to form a clearinghouse to collect and disseminate the work of homeland security experts and research information.

9 Concerns: Balancing Security and Openness

A critical issue is the possible impacts of counter terrorism security measures on R&D activities. The key question in this debate is how to ensure an open science and technology environment while maintaining the security of the homeland. Three issues have been discussed in particular; (1) the access to certain biological agents, (2) the control of foreign students and researchers, and (3) the handling of sensitive information (Marburger 2002, CRS 2002a, see also the more general discussion of these dilemmas in AAAS 2002).

Select agents and laboratory security. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 was signed by the President in June 2002 (PL 107-188). The Act specifies that HHS shall maintain a list of biological agents and toxins that have the potential to pose a severe threat to public health and safety ("select agents") and require that all laboratories in possession of these agents register with the department.

There is a concern that these measures will create barriers for legitimate research when it becomes more difficult to get access to these agents. For example, researchers must go through specific background checks by the Department of Justice according to the law. Another unintended consequence is higher costs for scientific institutions that have to invest in security and tracking measures. This will be a problem for many academic laboratories.

International students and researchers. A number of measures to control entry for foreign students and researchers have been implemented since 2001. A more thorough screening process of visa applicants and an automated tracking system: Student and Exchange Visitor Information System (SEVIS) have been established. These measures have resulted in more time consuming procedures and longer waiting times for applicants. For example, scholars with research related to the sensitive technologies currently listed on the U.S. Technology Alert List are forwarded to the State Department in Washington DC for further screening.

It is widely recognized that the U.S. benefit greatly from international students and researchers, and now there is a concern that some of the best scientists will go elsewhere. This might cause a loss of foreign technical workers in areas of short supply among U.S. citizens.

Sensitive S&T information. The Homeland Security Act of 2002 stipulated that procedures must be created to safeguard "homeland security information that is sensitive but unclassified". This was the first use of a category of information not previously officially defined considered sensitive but unclassified. These measures will limit, and have already limited, the access to information by the reclassification of already released material and by the withdrawal of information from federal agency web sites etc.

The provision has created concerns in the research community that the new category can be misused to restrict the flow of information that does not present a true threat to national security. At the same time, it is recognized that open access to fundamental research data is critical to continued scientific advancement, including the successful conduct of research related to homeland and national security. See also CRS 2003a for a discussion on sensitive information and other federal security controls on S&T information.

10 Concluding remarks

The concern for homeland security is shared by most countries in the world but the forces currently at work in the United States and the changes that are brought about are unmatched. So are the challenges for the administration to create a new institutional structure that is efficient and "future safe" in dealing with current and emerging threats and vulnerabilities. The provision of new and innovative technologies plays an important role in this endeavor.

This report has provided an overview or a "snap shot" of the evolving R&D landscape (structure, funding and coordination) in the area of homeland security in the U.S. With a five-year outlook, we can expect the following:

- The development of a significant market for homeland security products and services. This market will include procurement of technologies in the prototype-stage, under development in university labs and by research firms.

- The restructuring of players in the market (government, universities and industry) who seek to create a clear homeland security profile. This will include mergers, partnerships and new initiatives.

- Centers of excellence will be appointed or created in the domain of homeland security. Increased funding will further world-leading R&D at these institutions.

- Specific focus on technology transfer and the development of methods for rapid commercialization of research results. These schemes will accelerate technology development also in other areas.

- Entrepreneurship activities in start-up and small companies driven by increased R&D funding and market demand. Venture capital will contribute to later-stage funding.

- The development of new technologies, tools and methods for countering terrorism, particularly with a focus on NBC (nuclear, biological and chemical) threats. Spin-off technologies from the homeland security space into other areas, such as biotechnology and information technology.

The technology-leading role of the U.S. and its determination in the war on terrorism will make it a forerunner in the area of homeland security R&D. However, the U.S. cannot do it alone. To achieve its goals, partnerships and collaboration with other countries will be necessary.

As mentioned in this report, the developments in the U.S. will have implications for Sweden and its science and technology, policy-making and security management communities. There are several reasons for Sweden to seek further collaboration and to establish channels for the exchange of information and people with the U.S. in this area. Swedish authorities can benefit from the exchange of information regarding planning and coordination, Swedish researchers can tap into R&D funding and benefit from partnerships with U.S. institutions and Swedish firms can become more involved in the growing homeland security market.

Some possibilities that should be considered at the policy-level are agreements and other instruments promoting mutually beneficial exchange, including the following more specific examples:

- Exchange of information between the Department of Homeland Security (DHS) and the Swedish Emergency Management Agency (SEMA) regarding general coordination and planning of homeland security and emergency management issues. A more operative exchange might include the Swedish Rescue Services Agency (SRV). Both countries are putting new institutional structures in place to address homeland security issues and both have the mission to reduce vulnerabilities and increase the capacity to deal with emergencies when they occur.

- A more specific exchange between DHS (including the S&T Division) and SEMA (including the Research & Analysis Department) regarding issues related to R&D coordination and prioritization. From a science and technology perspective, both DHS and SEMA have priority-setting roles and they are responsible for the coordination and planning of R&D activities for homeland security purposes.

- Exchange between DHS (including HSARPA) as well as NIH (National Institutes of Health) and relevant Swedish R&D funding agencies, such as the Swedish Agency for Innovation Systems, the Swedish Research Council and the Swedish Foundation for Strategic Research, as well as institutes performing R&D, such as the Swedish Defence Research Agency. Issues might include research coordination and planning, exchange of researchers and participation in joint-projects.

- Support for Swedish researchers at universities and institutes, as well as Swedish companies and R&D firms, to participate in DHS S&T solicitations and technology procurement activities.

The specific opportunities for Sweden to make trans-Atlantic connections in the homeland security area will be further explored in a separate report.

References

AAAS (2002) *Science and Technology in a Vulnerable World,* American Association for the Advancement of Science.

AAAS (2003a) *AAAS Report XXVIII – Research & Development FY 2004*, American Association for the Advancement of Science.

AAAS (2003b) *AAAS R&D Funding Update July 14, 2003*, American Association for the Advancement of Science.

Alexander, *Jane A. (2003) Homeland Security Advanced Research Projects Agency*, Presentation July 31, 2003.

Aspen (2002) *Planning to Win: A Report on Homeland Security from the Aspen Strategy Group*, The Aspen Institute.

Brookings (2002) *Protecting the American Homeland – a Preliminary Analysis*, Brookings Institution Press, Washington DC.

Brookings (2003) *Protecting the American Homeland – One Year On, Brookings Institution Press*, Washington DC.

CFR (2002) *America – Still Unprepared, Still in Danger – Report by an Independent Task Force*, The Council on Foreign Relations.

CoC (2002) *Creating Opportunity out of Adversity, Proceedings of the National Symposium on Competitiveness and Security*, December 2002.

CRS (2002a) *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development and Higher Education*, Congressional Research Service RL31354, April 8, 2002.

CRS (2002b) *Federal Research and Development Organization, Policy, and Funding for Counterterrorism*, Congressional Research Service RL31576, September 19, 2002.

CRS (2003a) *"Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy,* Congressional Research Service RL31845, April 2, 2003.

CRS (2003b) *Homeland Security and Counterterrorism Research and Development: Funding, Organization, and Oversight*, Congressional Research Service RS21270, April 19, 2003.

CRS (2003c) *Project BioShield*, Congressional Research Service RS21507, April 28, 2003.

DHS (2003) *Overview of Science and Technology Division*, Department of Homeland Security, July 2003.

Foster, Robert (2003) *DoD Science and Technology*, Presentation, Department of Defense, April 30, 2003.

Gilmore (2002) *Implementing the National Strategy, Fourth Annual Report to the President and the Congress*, The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (the Gilmore Commission), December 2002.

HCS (2003) *Hearing on Cybersecurity Research and Development*, Science Committee, U.S. House of Representatives, May 14, 2003.

Heritage (2002) *Defending the American Homeland: A Report of the Heritage Foundation Homeland Security Task Force*, The Heritage Foundation.

Marburger, *John H. (2002) Statement of the Honorable John H. Marburger, Director Office of Science and Technology Policy, Before the Committee on Science, U.S. House of Representatives*, October 10, 2002.

McQueary, *Charles E. (2003) Statement of Under Secretary Dr. Charles E. McQueary, Department of Homeland Security, S&T Directorate before the House Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, and Research and Development*, May 21, 2003.

NCPC (2002) *Building the Homeland Security Network: What will it Take?,* The Wirthlin Report, special issue by the National Crime Prevention Council, August 2002.

New, William (2003) *Decision on Homeland Security Centers Draws Interest on Hill*, National Journal's Technology Daily, May 21, 2003.

NIAID (2002) *NIAID Strategic Plan for Biodefense Research* – Responding Through Research, National Institute of Allergy and Infectious Diseases, February 2002.

NRC (2002) *Making the Nation Safer: The Role of Science and Technology in Counter-terrorism*, National Research Council.

O'Gara (2003) *The Homeland Security Market: Corporate and Investment Strategies for the Domestic War against Terrorism*, The O'Gara Company LLC, May 28, 2003.

OHS (2002*) National Strategy for Homeland Security, Office of Homeland Security*, July 2002.

OHS (2003) *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, Office of Homeland Security*, February 2003.

OSTP (2003a) *Combating Terrorism: Research and Development Funding in the President's 2004 Budget, Office of Science and Technology Policy*, January 1, 2003.

OSTP (2003b) FY 2005 *Interagency Research and Development Priorities, Office of Science and Technology Policy*, June 5, 2003.

PCAST (2002) *Report on Maximizing the Contribution of Science and Technology within the New Department of Homeland Security*, the President's Council of Advisors on Science and Technology, September 2002.

RAND (2003) *Homeland Security – A Compendium of Public and Private Organizations' Policy Recommendations*, White Paper, RAND National Security Research Division.

Ridge, Tom (2003) *Remarks by Secretary of Homeland Security Tom Ridge to the Media Security and Reliability Council*, Press Release, Department of Homeland Security, May 27, 2003.

Shetty, Deepak (2003) *Homeland Security Budget – Is it Worth the Wait?,* Frost & Sullivan, March 2003.

TSWG (2003) *Combating Terrorism Technology Support Office, Technical Support Working Group (TSWG), Department of Homeland Security (DHS) – Broad Agency Announcement (BAA),* DAAD05-03-T-0024, May 14, 2003.

Vaida, Bara (2003) *Venture Capitalists Urge Small Tech Firms to Enter Government Market*, National Journal's Technology Daily, April 14, 2003.

White House (2002a) *The Department of Homeland Security*, the White House, June 2002.

White House (2002b) *Department of Homeland Security Reorganization Plan*, the White House, November 25, 2002.

White House (2003a) *National Strategy to Secure Cyberspace, the White House*, February 2003.

White House (2003b) *President Details Project BioShield, News Release, Office of the Press Secretary*, February 3, 2003.

Appendix A: DHS Organization

The following agencies will become part of the Department of Homeland Security. Organizational outline as of March 1, 2003 (Department of Homeland Security).

The Border and Transportation Security Division

- The U.S. Customs Service (Treasury)
- The Immigration and Naturalization Service (part) (Justice)
- The Federal Protective Service (GSA)
- The Transportation Security Administration (Transportation)
- Federal Law Enforcement Training Center (Treasury)
- Animal and Plant Health Inspection Service (part) (Agriculture)
- Office for Domestic Preparedness (Justice)
- **The Emergency Preparedness and Response Division**
- The Federal Emergency Management Agency (FEMA)
- Strategic National Stockpile and the National Disaster Medical System (HHS)
- Nuclear Incident Response Team (Energy)
- Domestic Emergency Support Teams (Justice)
- National Domestic Preparedness Office (FBI)

The Science and Technology Division

- CBRN Countermeasures Programs (Energy)
- Environmental Measurements Laboratory (Energy)
- National BW Defense Analysis Center (Defense)
- Plum Island Animal Disease Center (Agriculture)

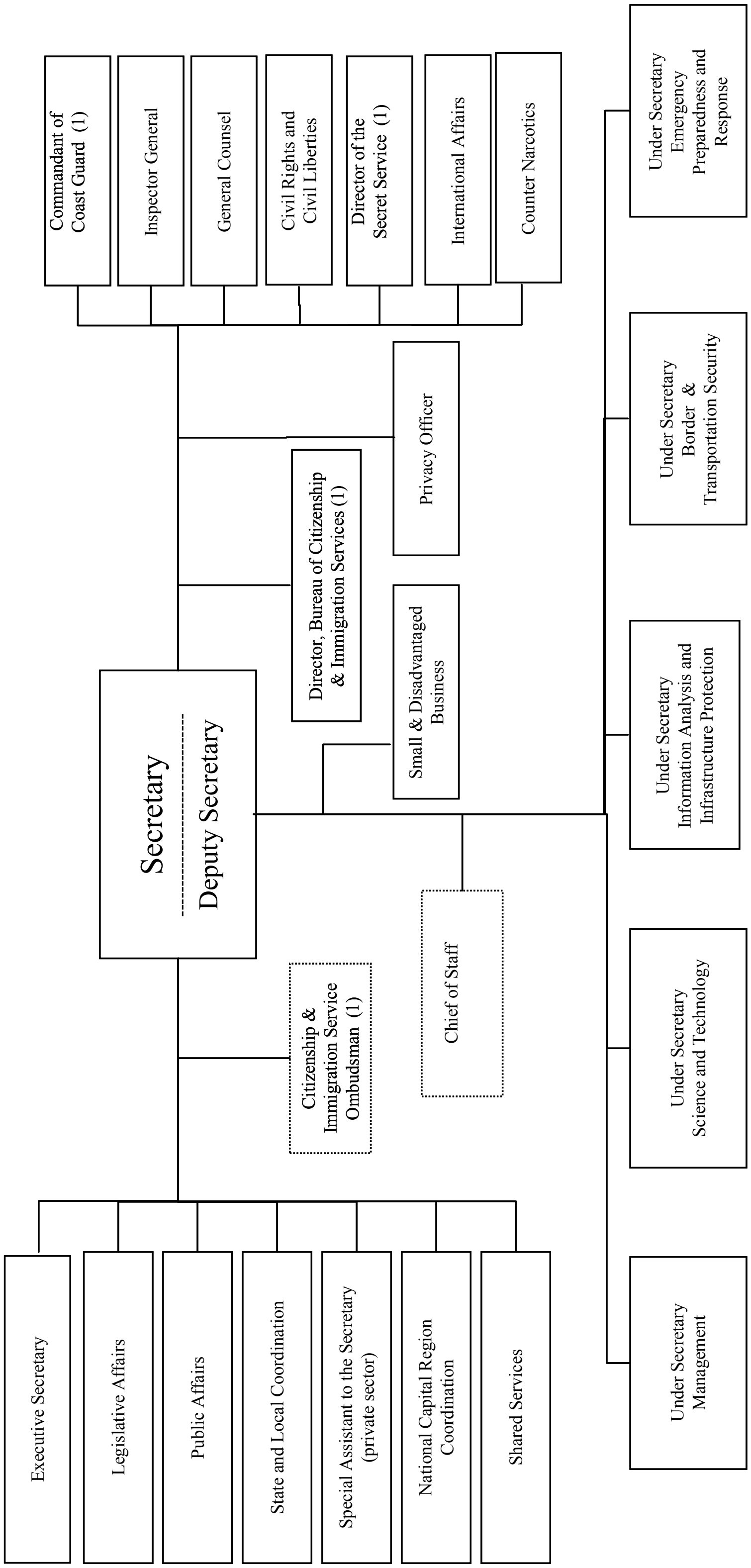
The Information Analysis and Infrastructure Protection Division

- Critical Infrastructure Assurance Office (Commerce)
- Federal Computer Incident Response Center (GSA)
- National Communications System (Defense)
- National Infrastructure Protection Center (FBI)
- Energy Security and Assurance Program (Energy)

Other agencies to be located in DHS

- The Secret Service
- The Coast Guard

Department of Homeland Security


Secretary
Deputy Secretary
Executive Secretary
Legislative Affairs
Public Affairs
State and Local Coordination
Special Assistant to the Secretary (private sector)
National Capital Region Coordination
Shared Services
Citizenship & Immigration Service Ombudsman (1)
Chief of Staff
Small & Disadvantaged Business
Director, Bureau of Citizenship & Immigration Services (1)
Privacy Officer
Commandant of Coast Guard (1)
Inspector General
General Counsel
Civil Rights and Civil Liberties
Director of the Secret Service (1)
International Affairs
Counter Narcotics
Under Secretary Management
Under Secretary Science and Technology
Under Secretary Information Analysis and Infrastructure Protection
Under Secretary Border & Transportation Security
Under Secretary Emergency Preparedness and Response

Note (1): Effective March 1st, 2003

Appendix B: Federal R&D Related to Homeland Security

The programs described below comprise a partial listing of R&D entities or activities that are relevant to homeland security. Most of them will remain outside the Department of Homeland Security but the need to coordinate programs and priority setting has been pointed out by many analysts. This list was compiled in mid-2002 (PCAST 2002).

Department of Agriculture (USDA)

National Veterinary Services Laboratories: These labs are responsible for diagnosis for domestic and foreign animal diseases, diagnostic support for disease control and eradication programs, import and export testing of animals, and laboratory certification for selected diseases. Many of the diseases they diagnose at the facilities are listed as select agents by both the Centers for Disease Control and Prevention (CDC) and USDA. This laboratory was the main diagnostic lab used during the anthrax outbreak. These labs contain the other biosafety level 3 lab (in addition to Plum Island).

The Food Safety and Inspection Service (FSIS): FSIS serves as the front line for detection of diseases and health risks in domestic meat, poultry, seafood and eggs. FSIS tests for microbiological, chemical, and other types of contamination and conducts epidemiological investigations in cooperation with the CDC based on reports of food borne health hazards and disease outbreaks. Food safety did not appear to be considered as a priority for homeland defense.

FoodNET: Run by CDC’s Emerging Infections Program, and similar to PulseNET, FoodNET monitors food disease outbreaks and works collaboratively with USDA, the Food and Drug Administration (FDA) and several states.

USDA ARS and CSREES: Intra- and extramural research programs which support research on food safety, microbes and pathogens that can be used in bio- and agro-terrorism.

Department of Commerce

National Institute of Standards and Technology (NIST):

- **Building and Fire Research Laboratory:** This lab studies building materials; computer-integrated construction practices; fire science and fire safety engineering; and structural, mechanical, and environmental engineering. Products of the laboratory's research include measurements and test methods, performance criteria, and technical data that support innovations by industry and are incorporated into building and fire standards and codes.

- **Structures Division:** This division promotes construction productivity and structural safety by providing measurements and standards to support the design, construction, and serviceability of constructed facilities. The Division performs and supports laboratory, field, and analytical research in the areas of structural evaluation and standards, structural systems and design, construction metrology and automation, and earthquake hazards reduction.

  NIST has legislative authorities to initiate and conduct structural and fire investigations to provide technical analysis of the causes of fire or structural failure. A team of NIST-led experts is currently investigating the technical causes for the collapse of the World Trade Centers, for example. The funding for the NIST-led technical investigation of the WTC collapses will is provided through the Federal Emergency Management Agency (FEMA).

- **Indoor Air Quality and Ventilation Group:** This group develops computer simulation programs and measurement procedures to better understand air and contaminant transport phenomena in buildings. The results of this research are providing valuable methods to evaluate ventilation characteristics and indoor pollutant concentrations in buildings.

  Expertise in ventilation systems developed a sophisticated computer model to understand different ways in which airflow may have transported anthrax spores in the Hart Senate Office Building. The results of the modeling were used in planning sampling within the building and in developing decontamination strategies. NIST's expertise could be applied to the anthrax spore problem quickly because it has long worked to improve indoor air quality by developing computer-modeling programs to show how pollutants, smoke, and contaminants are transported through indoor air.

Department of Defense (DOD)

Components of the Defense Advanced Research Projects Agency (DARPA): DARPA's charter is to prevent technological surprise from harming U.S. national security by sponsoring revolutionary and innovative high-payoff research. Examples of this mission relevant to homeland security are:

- **Medical Surveillance Program**: The Air Force's Lightweight Epidemiology Advanced Detection and Emergency Response System (LEADERS) uses key components of DARPA's Enhanced Consequence Management Planning and Support System. A commercialized version of the DARPA bio-surveillance program, LEADERS, provided medical surveillance for signs and symptoms of a biological attack for the state of New York within 24 hours of the attack on the World Trade Center. The CDC also used LEADERS to monitor for specified syndromes from hospitals within in the New York City area and report them back in real-time to the CDC in Atlanta via the Internet.

- **BioSensors Program**: To detect the presence of a threat agent, DARPA is investing in the development of advanced Biosensor Defense Systems that are robust, autonomous, fast, and sensitive to any known bacterial or viral organism, as well as to novel natural or engineered biowarfare agents. Two example systems are the TIGER and BioTOF sensor systems.

- **Medical Diagnostics and Countermeasures Program:** In the event of a biological attack, the U.S. will need to identify those who have been exposed to a biological warfare agent and to distinguish them from the "worried well," as well as from those with natural diseases that might require different treatment. Therefore, identifying disease markers that can serve as rapid indicators of exposure is one of the focus areas of the Advanced Medical Diagnostics Program.

- **The Unconventional Pathogen Countermeasures (UPC) Program:** Broad-spectrum countermeasures for threat pathogens are being developed, including anti-viral and antibiotic drug discovery and development, as well as new approaches to vaccinations. Three UPC projects have shown promise in initial evaluations and are transitioning to the U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID) for further development: a drug designed to attack the DNA of bacteria, viruses and malaria; a family of drugs that target a common and critical enzyme in anthrax and other bacteria; and a protein fragment that blocks the effects of toxins released by bacteria

- **Genetic Sequencing of Biological Warfare Agents Program:** The validated threat agent organisms whose sequences had not yet been characterized were sequenced and analyzed via modern, high-throughput sequencing technologies. The organisms we sequenced and analyzed are: *Coxiella burnetti (Q fever), Rickettsia typhi (typhus), Burkholderia mallei (glanders)*, Brucella suis (brucellosis), *Clostridium perfringens (gas gangrene), and Franciscella tularensis* (tularemia). Additionally, several more strains and variants of orthopoxviruses related to smallpox are being sequenced, and an orthopoxvirus database was established in collaboration with the CDC and USAMRIID.

- **Immune Building Program:** The goal of this program is to make military buildings far less attractive targets for attack by chemical or biological warfare agents by reducing the effectiveness of such attacks via active and passive response of heating, ventilation, and air conditioning systems, and other building infrastructure (e.g., neutralization and filtration).

- **Information Assurance and Survivability Programs:** This suite of programs was created to raise strong barriers to cyber attack and provide commanders with technology to see, counter, tolerate, and survive sophisticated cyber attacks.

Armed Forces Radiobiology Research Institute (AFRRI): The DOD's principal and only organizational element charged with prosecuting the mandates of the Medical Radiological Defense Research Program (MRDRP); medical nuclear/radiological defense. The current program is highly focused on developmental and applied research in four areas that include prevention and treatment of radiation injuries, biological dosimetry, medical effects of combined exposure to radiation and chemical or infectious agents, and medical effects of chronic exposure to depleted uranium (DU). The second mandate of AFRRI is the training of DoD medical personnel in the management and treatment of radiation injuries; Medical Effects of Ionizing Radiation Course. The third mandate of AFRRI is its medical nuclear response team; Medical Radiobiology Advisory Team. The fourth mandate is consultation to the Office of the Secretary of Defense, Joint Chiefs of Staff and the Commanders-in-Chief of the regions of the world.

The program's combined personnel and physical elements constitute a nationally unique resource capable of conducting a wide variety of studies into the biological effects of ionizing radiation and development of effective medical countermeasures.

Components of the Defense Threat Reduction Agency (DTRA): DTRA's mission is to safeguard the United States and its friends from weapons of mass destruction (chemical, biological, radiological, nuclear and high explosives) by reducing the present threat and preparing for the future threat.

- **Chemical and Biological Defense Program (CBDP):** The objective of the CBDP is to enable our forces to survive, fight and win in a chemically or biologically contaminated warfare environment. The CBDP provides for the procurement and development of systems to enhance the ability of personnel to deter and defend against CB agents. The CBDP's six major areas cross cut all military/civilian applications for defense against CB attacks: (1) individual protection; (2) collective protection; (3) medical defense; (4) modeling and simulation; (5) contamination avoidance; (6) decontamination. The Program supports and manages program testing (at the Dugway Proving Ground).

- **Biological Warfare Defense Program (BW):** The BW conducts research and development of novel technologies against a broad application of many different threat agents. Examples of projects with civilian applications in the detection systems program: Portal Shield ACTD biological and chemical detection network, Long range Bio Stand-off Detector, Joint Biological Remote Early Warning System, Joint Chemical Agent Detector.

- **Joint Service Technology Panel for Chemical and Biological Defense (JSTPCBD):** This panel makes sure that efforts between DARPA's CBW programs are coordinated with those of the National Institutes of Health and other interested researchers.

- **Technical Support Working Groups (TSWG); Technology Development Division:** By accelerating state-of-the-art technologies that improve force application/protection modeling capabilities, provide enhanced weapons and sensors for defeat of WMD-related facilities, and optimize capabilities for use by Special Operations Forces, DTRA enhances the survivability and operability of U.S. military equities. The agency evaluates the lethality of conventional, biological, chemical, and other advanced weapons against a broad spectrum of target types in war fighting and terrorist scenarios.

U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID): The USAMRIID conducts research to develop strategies, products, information, procedures, and training programs for medical defense against biological warfare threats and naturally occurring infectious diseases that require special containment. USAMRIID, an organization of the U.S. Army Medical Research and Materiel Command (USAMRMC), is the lead medical research laboratory for the U.S. Biological Defense Research Program. The Institute plays a key role in national defense and in infectious disease research as the largest biological containment laboratory in the DOD for the study of hazardous diseases. Medical products developed to protect personnel against biological attack include drugs, vaccines, diagnostic capabilities, and various medical management procedures.

Components of the Naval Medical Research Center (NMRC):

- **Biological Defense Research Directorate:** This directorate's investigator staffs are recognized leaders in the rapid and confirmatory diagnosis of infectious diseases through analysis of a wide variety of clinical materials. The directorate explores basic and applied microbiological, immunological and related scientific research methodologies for the development of medical diagnostics to bioweapons. Research personnel have designed, developed, and tested a broad variety of methodologies, which have allowed for swift and accurate disease diagnosis essential for substantive medical protection. In addition, researchers have been instrumental in the advancement and refinement of confirmatory diagnostic methods utilizing polymerase chain reaction (PCR) methodologies in tandem with innovative, state of the art biosensor technologies.

- **Infectious Disease Directorate (IDD):** The overarching research goal in IDD is to minimize the impact of infectious diseases by preventing infection; and in most cases, the best approach to achieve that goal is through the development of efficacious vaccines. IDD departments have the unique research capability of developing a new vaccine from the conceptual stage through construction, "test tube" evaluation, animal model testing, human safety and immunogenicity testing, to final field trials in a large number of volunteers for efficacy evaluation. NMRC-IDD also serves as the organizational umbrella under which the Navy's participation in the **Department of Defense Global Emerging Infection Systems (DoD-GEIS)** initiative is coordinated. Along with other DoD agencies, Navy researchers participate in efforts for the GEIS Program objectives:
    - Detection and Monitoring: Detect and monitor emerging pathogens, the diseases they cause, and the factors influencing their emergence to protect military readiness, the health of DoD beneficiary populations and other national interests.
    - Response: Enhance the prompt implementation of all prevention and control strategies for emerging infections to include improving communication of information about emerging agents.
    - Training and Capacity Building: Leverage DoD and international public health infrastructures to support surveillance, assessment, response, and prevention of emerging agents through training, networking, and other forms of assistance.
    - Systems Research, Development and Integration: Integrate public health practices and improve capabilities in clinical medicine, military medicine, laboratory science, epidemiology, public health, and military medical research to facilitate rapid identification and response to emerging infections.

Department of Energy (DOE)

Pacific Northwest National Laboratory National Security Division: Pacific Northwest's mission in national security supports the U.S. government's objectives against the proliferation of nuclear, chemical and biological weapons of mass destruction and associated delivery systems. The lab conducts work in national security programs for the DOE, DOD, and most other federal agencies. The Remote Sensing and Electro-Optics Technical Group provides synergistic capabilities in image analysis, optical and electro-optical system analysis and development, and data fusion/integration, analysis, and visualization.

Remote Sensing Test and Evaluation Center: This Center includes the Remote Sensing Laboratory, the HAZMAT Spill Center, and the Special Technologies Laboratory. The Remote Sensing Laboratory provides integration and flight services for unique research sensors that require airborne testing and data collections to further scientific understanding. The HAZMAT Spill Center on the Nevada Test Site supports field-testing of effluent detection sensors for the nonproliferation and Verification R&D program. In addition, Bechtel Nevada provides for facility maintenance, equipment upgrades needed to support sensor testing, and system calibration.

New Brunswick Laboratory (NBL): A center of excellence in the measurement science of nuclear materials, NBL is the U.S. government's Nuclear Materials Measurements and Reference Materials Laboratory and the National Certifying Authority for nuclear reference materials and measurement calibration standards. As an internationally recognized federal laboratory, NBL provides reference materials, measurement and interlaboratory measurement evaluation services, and technical expertise for evaluating measurement methods and safeguards measures in use at other facilities for a variety of federal program sponsors and customers.

DoE Office of Security: The Nonproliferation and National Security Institute: This Institute, located along with Sandia National Laboratory on Kirtland Air Force Base, trains protective-force personnel in the skills required to protect against terrorist threats directed at U.S. nuclear facilities. Its curriculum includes more than 100 courses in five major topical areas: information security, materials control and accountability, personnel security, program and planning management (including curriculum development and instructional techniques), and protection program operations. The Institute encompasses a number of new academies and training centers: Emergency Operations Training Academy (EOTA), Counterintelligence Training Academy (CITA), and Foreign Interaction Training Academy (FITA).

Fossil Energy and Energy Supply: Program elements within these DOE programs could be reoriented to focus on research priorities identified in the NRC report, Making the Nation Safer: The Role of Science and Technology in Counter-terrorism (NRC 2002).

Fossil Energy R&D, Central Systems, Advanced Systems: Currently the Advanced Systems program supports demonstration projects for integrated gasification combined cycle, pressurized fluidized beds, and turbines. The program should be focused on the physical and cyber security of the electric transmission system, with a particular emphasis on supervisory control and data acquisition (SCADA) systems, as well as developing integrated multi-sensor warning systems (MWS) and other tools for the real-time monitoring for reliable detection of an attack.

Department of Health and Human Services (HHS)

Components of the Centers for Disease Control and Prevention (CDC): The CDC's responsibility, on behalf of the HHS, is to provide national leadership in the public health and medical communities in a concerted effort to detect, diagnose, respond to, and prevent illnesses, including those that could occur as a result of bioterrorism or any other deliberate attempt to harm the health of our citizens.

- **Epidemic Intelligence Service (EIS):** EIS trains personnel to respond to naturally occurring and bioterrorism outbreaks and other disaster situations to aid state and local officials in the identification of potential causes and implement appropriate solutions. EIS was established during the Cold War in response to the threat of biological warfare.

- **Public Health Prevention Service (PHPS):** This Service provides specialists who can provide on-site programmatic support to extend the manpower of state and local public health staff in responding to naturally occurring and bioterrorism events.

- **Metropolitan Medical Response System (MMRS):** MMRS helps communities prepare for coordinated response of medical, epidemiological and public health experts in response to an attack or disaster. So far, 97 cities nationwide have received assistance.

- **Epidemiological and Laboratory Capacity (ELC); Laboratory Response Network (LRN):** The LRN is a network of governmental (local, state and federal) laboratories that have been trained by the CDC to process samples by well-established and validated procedures. These laboratories must adhere to the LRN standard protocols for testing and must successfully complete periodic proficiency testing challenges sent from CDC. The LRN was formed as a self-organized group through the efforts of the CDC and the Association of Public Health Laboratories (APHL).

- **Surveillance Programs for Food Borne Pathogens:** PulseNet and eLEXNET: The CDC's Food Safety Office mission is to prevent illness, disability and death due to domestic and imported food borne diseases, whether they occur naturally or as acts of terror. They collaborate with and support other CDC organizations with focus on attainment of food safety program plans, goals and objectives. They work in partnership with the FDA, EPA, USDA, state and local health departments, and other public and private organizations to strengthen regulations and policies for prevention of food borne diseases.

- **Human Health Surveillance Programs: Emerging Infections Program (EIP) – Health Alert Network (HAN):** CDC has helped establish sentinel disease detection systems that involve local networks of clinicians and other health care providers. To ensure rapid communication and access to critical health information, CDC is implementing the national HAN, in partnership with the National Association of County and City Health Officials (NACCHO), the Association of State and Territorial Health Officials (ASTHO), and other health organizations. The HAN will establish communications, information, distance-learning, and organizational infrastructure for a new level of defense against bioterrorism and other health threats, linking all public health agencies at the local, state, and federal levels via: (1) continuous, high-speed connection to the Internet, (2) broadcast communications, and (3) satellite- and Web-based distance learning.

- **National Pharmaceutical Stockpile (NPSP):** Once the cause of a terrorist-sponsored outbreak was determined, specific drugs, vaccines, and antitoxins might be needed to treat the victims and to prevent further spread. CDC has developed of a stockpile of pharmaceuticals to be able to reach victims of an incident anywhere in the continental U.S. within 12 hours. This system was proven for the first time when tons of medical supplies reached New York City within seven hours of deployment following the attack on the World Trade Center.

HHS/Food and Drug Administration

Center for Drug Evaluation and Research (CDER): CDER is working with other federal agencies to make sure adequate supplies of medicine and vaccines are available to the American public. They are working to provide the most current information on drug preparedness and response to the public in response to a bioterrorism attack through drug information; vaccine information; and information of prescribing and buying medicine.

Center for Biologics Evaluation and Research (CBER): CBER plays an integral role in the expeditious development and licensing of products to diagnose, treat or prevent outbreaks from exposure to the pathogens that have been identified as bioterrorist agents. These products must be reviewed and approved prior to the large-scale productions necessary to create and maintain a stockpile. Staff must guide the products through the regulatory process, including the manufacturing process, pre-clinical testing, clinical trials, and the licensing and approval process.

Center for Food Safety and Applied Nutrition (CFSAN): CFSAN is responsible for regulating the foods that are not under the jurisdiction of USDA for human consumption safety.

Department of Justice (DOJ)

Border Research and Technology Center (BRTC): A program within the National Institute of Justice, The Border Research and Technology Center (BRTC), operated by Sandia National Laboratories, is located in San Diego, California. BRTC works with the Immigration and Naturalization Service, the U.S. Border Patrol, the U.S. Customs Service, the Office of National Drug Control Policy, the U.S. Attorney offices, and law enforcement agencies to strengthen technology capabilities and awareness on the Nation's borders.

One of its most recognized assistance activities has been the implementation of SENTRI (the Secured Electronic Network for Travelers' Rapid Inspection). BRTC also works on joint ventures to identify technologies that will stop fleeing vehicles and is currently participating in a project to detect heartbeats of people concealed in vehicles or other containers. BRTC's technology partners include Sandia, and the Space and Naval Warfare Systems Center–San Diego (SSC-SD).

Office of Law Enforcement Technology Commercialization (OLETC): A program within the National Institute of Justice, this program is designed to develop and deploy an active, broad based national program to assist in the commercialization of innovative technology for use by the law enforcement and corrections community. OLETC's primary objective is to bring research and private industry together to put affordable, market-driven technologies into the hands of law enforcement and corrections personnel.

Office of Law Enforcement Standards (OLES) (DOJ funded activity at NIST): The mission of OLES is to serve as the principal agent for standards development for the criminal justice and public safety communities. OLES has been instrumental in the development of numerous standards and the issuance of various technical reports that have had significant impact on both of these communities. Through its programs, OLES helps criminal justice and public safety agencies acquire the high quality resources they need to do their jobs. To accomplish this task, OLES:

- Develops methods for testing equipment performance;
- Develops methods for examining evidentiary materials;
- Develops standards for equipment and operating procedures;
- Develops users' guides;
- Develops standard reference materials; and
- Performs other scientific and engineering research as required by the criminal justice and public safety communities.

National Science Foundation (NSF)

The NSF supports research related to terrorism and homeland security objectives. Its revised mission statement after Fall 2001 reflects the use of federal funds for research in areas such as detection and decontamination of biological or chemical warfare agents, cybersecurity, and continuing social responses to anti-terrorism. Examples of grants recently funded include:

Chemical and Biological Terrorism

- will use gas chromatography and polymer sensors ("electronic noses") to identify chemical warfare agents.
- will explore the use of activated hydrogen peroxide to destroy chemical and biological warfare agents on contaminated surfaces.
- will develop guidelines to use ozone as an alternative to toxic chemicals to decontaminate spaces contaminated with anthrax.
- will examine disinfectants such as ultraviolet and gamma irradiation for decontaminating anthrax from objects in closed spaces.
- will attempt to find inhibitors of "anthrax lethal factor" (a lethal toxin produced by anthrax bacteria and responsible for inhalational anthrax fatalities), which can help develop novel anthrax drugs.
- will investigate the environmental impact of 9/11 by studying the chemistry and mineralogy of sediments of New York Harbor.

Cyber Security

- will review trends in cyber security research and identify problems that need to be addressed in the national cyber security research agenda.

SWEDISH EMERGENCY MANAGEMENT AGENCY

VINNOVA

SCIENCE • TECHNOLOGY • MEDICINE Swedish Foundation for Strategic Research

ITPS, Swedish Institute for Growth Policy Studies
Studentplan 3, SE-831 40 Östersund, Sweden
Telephone: +46 (0)63 16 66 00
Fax: +46 (0)63 16 66 01

info@itps.se
www.itps.se
ISSN 1652-0483

itps SWEDISH INSTITUTE FOR GROWTH POLICY STUDIES