Order Code RL31202

Federal Research and Development for Counter Terrorism: Organization, Funding, and Options

Updated January 3, 2002

Genevieve J. Knezo
Specialist, Science and Technology Policy
Resources, Science, and Industry Division

Federal Research and Development for Counter Terrorism: Organization, Funding, and Options

Summary

Before the September 11 terrorist attacks national expert commissions questioned whether the federal government was prepared adequately to conduct and use research and development (R&D) to counter terrorism. They cited inadequate planning, conflicting information about agency funding; the absence of coordination mechanisms to set agency priorities and eliminate duplication; and the need to use resources of government, academia, and industry efficiently and effectively to develop needed scientific and technological information. Since September 11, two levels of counter terrorism R&D coordination have started to evolve. One is at the interagency R&D policymaking level and the other is at the programmatic level for specific areas of R&D. The Office of Homeland Security (OHS), created on October 8 by Executive Order 13228, does not list R&D among its major responsibilities, but R&D is a topic of one of the interagency Policy Coordination Committees attached to the Homeland Security Council (HSC). Legislation was introduced to statutorily authorize a homeland security agency that would coordinate R&D. The Director of the Office of Science and Technology Policy (OSTP) was not named to participate in OHS activities, but he reports that his office is temporarily filling the HSC interagency R&D policy coordination role. The President gave OSTP two specific counter terrorism R&D-related functions – to help develop policy for foreign student visas/identification of "sensitive" courses and to help develop advanced technology for immigration/visa control. The OSTP chairs the National Security Council's (NSC) Preparedness Against Weapons of Mass Destruction R&D Subgroup, which has responsibility to identify gaps and duplication in R&D relating to chemical, biological, nuclear, and radiological threats. Some advocate expanding the NSC mission beyond foreign policy and defense to include economic and cyber- threats.

Related counter terrorism R&D issues include the relationship between the NSC and the HSC R&D coordinating committee; the collection of reliable data about federal funding; the conduct of creative, risky R&D; the use of nontraditional funding mechanisms; the pros and cons of overcoming barriers to industrial collaboration; the balance between funding for counter terrorism R&D and for other fields of science; and mitigating any adverse effects controls placed on access to "sensitive" scientific information. Proposals have been made to expand the Technical Support Working Group and the Defense Advanced Research Projects Agency. The National Academy of Sciences has started to assist the government.

Bioterrorism R&D is dominated by the Defense and Health/Human Services departments. Each agency has intra-agency coordination mechanisms, but there is no formal interagency group. The interagency President's Critical Infrastucture Board has responsibility for information security R&D; OSTP was tasked to help it coordinate R&D priorities and the board was authorized to request federal agencies to fund priority R&D programs. When examining proposals for expanded counter terrorism R&D funding (which is estimated to have tripled to $1.5 billion for FY2002), Congress may consider whether adequate mechanisms are in place to develop priorities which best serve the nation's interests.

Contents

Introduction 1

Federal Agency Funding and Programs for Counter Terrorism R&D 2
- Definition of the Policy Issue 2
- Office of Management and Budget Funding Data 2
- Monterey Institute of International Studies Funding Data 7

Interagency Coordination of Federal Agency Counter Terrorism R&D Policy, Priorities, and Funding 7
- Definition of the Policy Issue 7
- Concerns About Coordination of Federal Counter Terrorism R&D 8
- Use of Existing Agencies 10
  - Technical Support Working Group (TSWG) 10
  - National Security Council 11
  - Office of Science and Technology Policy 12
    - OSTP's Limited Responsibilities to Implement Specific Counter Terrorism R&D Activities 13
    - OSTP-initiated Actions Relating to Counter Terrorism R&D . . 14
  - National Science and Technology Council 16
- Proposals for New Organizations With R&D Responsibilities to Combat Terrorism 17

Establishment of Office of Homeland Security 18
- Research and Development Coordination Function Assigned to the Homeland Security Council's Policy Coordination Committee 19
- Congressional Proposals to Authorize a Homeland Security Agency With Responsibilities for R&D 20

Other Counter Terrorism R&D Proposals 22
- Proposal to Create a RAND-like Independent Think Tank to Support the Office of Homeland Security 22
- An Enhanced DARPA or "Manhattan" Project for Counter Terrorism . . . 22
- Creative R&D for Counter Terrorism 23

Priorities for, and Coordination of, Bioterrorism and Information Security Counter Terrorism R&D 24
- Definition of the Policy Issue 24
  - Funding for Bioterrorism R&D and Information Security R&D 25
- Bioterrorism R&D 26
  - Options for Priority-setting and Organization 26
    - Proposals to Create a Government-Owned Facility for Bioterrorism R&D and Drug Production 28
  - Policy Actions 30
  - Congressional Options 31
    - NIH and CDC and Other Health Agencies 33
    - Department of Agriculture 35
    - Multi-agency Bioterrorism R&D 36

Information Security R&D 37
Options for Priority-setting 37
Options for Organization 38
Policy Actions 39
Congressional Options 42

National Academy of Sciences 43

Policy Options for Priority-setting and Coordination 45
Interagency Coordination at the Policymaking Level 45
Coordination at the Functional Program Level 49

Conclusion 51

APPENDIX 1, Administration's Goals for Counter Terrorism for Weapons of Mass Destruction 52

APPENDIX 2, Table on Research and Development Funding by Category as a Subset of Federal Funding to Combat Terrorism, Including Defense Against Weapons of Mass Destruction, FY1998-2001, by Monterey Institute of International Studies 54

APPENDIX 3, Table on Research and Development Funding by Agency and Category as a Subset of Federal Funding to Combat Terrorism, Including Defense Against Weapons of Mass Destruction, FY1998-2001, by Agency and Category, by Monterey Institute of International Studies, 2000 55

APPENDIX 4, Other Recommendations to Strengthen U.S. Science and Technology Infrastructure to Deal With National Security Threats, Made Primarily by the Hart-Rudman Commission 60
Proposals to Increase Federal R&D Funding 60
Science and Engineering Education 61
National Laboratories 61
Other Proposals to Strengthen U.S. Science Infrastructure 62
Enforce Independent Research and Development (IR&D) Rules 62
Create Interagency Space Working Group 62
Use More Open Source S&T Literature in Intelligence Analysis 62

APPENDIX 5, Abbreviations 63

List of Figures

Figure 1, AAAS Estimates of FY2002 Federal Counter Terrorism R&D 5

List of Tables

Table 1. Research and Development to Combat Terrorism, By Agency, FY2000-FY2001 (Request), Dollars in Millions 3
Table 2. Research and Development for Counter Terrorism R&D and for R&D Defense Against Weapons of Mass Destruction (WMD), FY2002 Request, By Subcategory and Agency (Dollars in Millions) 6

Federal Research and Development for Counter Terrorism: Organization, Funding, and Options

Introduction

In reports prepared before the September 11 terrorist attacks, nationally convened expert commissions, the General Accounting Office (GAO), and other authorities questioned whether the U.S. government was prepared adequately to conduct and use the research and development (R&D) that would generate scientific and technological advances to prevent and combat terrorism. Since September 11, federal responses and mechanisms have evolved. This report focuses on that issue, with an emphasis on governmental organization to determine appropriate R&D priorities, funding levels, and policy. Federal agency funding and organization for counter terrorism R&D are described and recommendations for improvement made in authoritative reports are summarized.

Recent policy actions and legislative initiatives relating to coordination activities of the Office of Science and Technology Policy, the Office of Homeland Security, and other bodies are discussed. Recommendations made by others about improving priority setting and organization of bioterrorism R&D and cyber terrorism R&D are covered as case studies because of their importance and the fact that they received considerable attention both before and after the September 11 attacks. The report also summarizes the activities of the National Academy of Sciences to aid the government in counter terrorism R&D.

The final sections identify issues to consider when assessing the evolving governmental structures to coordinate counter terrorism R&D. These include the relationship between R&D and the counter terrorism agenda developed since September 11; identification and coordination of program and policy activities that cut across many different agencies; development of coordination mechanisms that work effectively with federal agencies and have the confidence of Congress and the President; and cooperation among government, the scientific and technological communities, and industry.

Federal Agency Funding and Programs for Counter Terrorism R&D

Definition of the Policy Issue

There are conflicting estimates of agency funding, as well as reports of duplication, waste, and inadequate priority-setting for federally supported counter terrorism R&D.

Office of Management and Budget Funding Data

OMB's FY2001 *Annual Report to Congress on Combating Terrorism*[1] reported that $10.333 billion[2] was requested for combating terrorism (conventional and against weapons of mass destruction (WMD)) for FY2002. Of this, about $554 million – or 5% of the total – was for federal R&D to develop technologies to deter, prevent or mitigate terrorist acts. This includes work in "...antiterrorism (defensive measures to combat terrorism) and counter terrorism (offensive measures)...."[3] Of the terrorism R&D total, 80%, or $442 million, was for WMD. While OMB did not formally define WMD, it referred to some research against WMD as intended to meet "a broad range of increasingly complex needs to prevent, counter, or respond to nuclear, radiological, chemical, and biological terrorism."[4]

As shown in **Table 1**, the national security community is responsible for about 44% of R&D to combat terrorism – principally in the Defense Advanced Research Project Agency's (DARPA) Biological Warfare Defense program in the WMD category. The national security line also includes $40 million for the Technical Support Working Group (TSWG) – a State Department/DOD "interagency forum that identifies, prioritizes, and coordinates interagency and international R&D requirements for combating terrorism" and that conducts R&D specifically to develop new technologies and equipment to counter terrorism. TSWG also receives almost $20 million in funding transferred from other agencies.[5] (TSWG's functions are discussed in more detail below in the section on "Use of Existing Agencies.")

---

[1]OMB, *Annual Report to Congress on Combating Terrorism*, August 2001, authorized by Section 1051 of the FY1998 National Defense Authorization Act, P.L. 105-85 (which required information on executive branch funding to combat terrorism) and section 1403 of P.L. 105-26 (which required information on domestic preparedness).

[2]OMB, *Annual Report to Congress on Combating Terrorism*, p. 5. This funding is largely separate from funding that goes to protect critical infrastructures OMB defines critical infrastructures as "those physical and cyber-based systems essential to national security, national economic security, and public health and safety." According to OMB, data on these expenditures can be found in the Administration's *National Plan for Information System Protection*, pp. 2-3.

[3]OMB, *Annual Report to Congress on Combating Terrorism*, p. 14.

[4]OMB, *Annual Report to Congress on Combating Terrorism*, p. 30.

[5]OMB, *Annual Report to Congress on Combating Terrorism*, p. 28.

The emphasis of counter terrorism research supported by the National Institutes of Health (NIH) in the Department of Health and Human Services (DHHS) is on genomics, basic research and infrastructure, and design and testing of diagnostics, therapies, and vaccines. The Department of Energy's (DOE) work ranges across such areas as genomic sequencing, development of new DNA-based diagnostics, advanced

Table 1. Research and Development to Combat Terrorism, By Agency, FY2000-FY2001 (Request), Dollars in Millions[6]

Agency	FY2000 Actual	FY2001 Enacted	FY2002 Request
Agriculture	$37.3	$51.7	$41.6
Commerce	9.6	4.1	4.1
Energy	59.7	68.0	55.6
DHHS	109.7	116.1	128.2
Justice	45.2	42.9	23.9
National Security	190.0	234.9	242.7
State	7.0	5.0	6.2
Transportation	50.7	54.6	51.1
Treasury	2.1	1.2	1.2
Total	**511.3**	**578.5**	**554.6**

modeling and simulation,[7] and microfabrication technologies. The Department of Agriculture's (USDA) Agricultural Research Service conducts extensive research into plant, pest, and animal diseases from natural or inadvertent introductions. According to OMB, "much of this research can be of benefit whether the cause was naturally occurring, criminal, or terrorist induced, however, only $500,000 has been appropriated specifically for pathogen detection and identification of research needs directly related to terrorism."[8]

OMB also focused in detail on R&D funding for WMD and identified the Administration's six major WMD counter terrorism R&D goals (called "subcategories" in the next table). (See **Appendix 1** for a detailed description of these goals.) The OMB data show that the defense agencies spend the most on counter terrorism R&D for WMD, followed by the Department of Health and Human

---

[6]OMB, *Annual Report to Congress on Combating Terrorism*, p. 27.

[7]DOE "is developing models for evaluating effectiveness of response and mitigation measures, such as reducing vulnerability of installations and improving operations and procedures at key urban facilities (e.g. evacuation, sheltering, traffic control, train control in subways, control of air handling systems)." (OMB, *Annual Report to Congress on Combating Terrorism*, p. 36.)

[8]OMB, *Annual Report to Congress on Combating Terrorism*, p. 28.

Services, Department of Energy, the Department of Transportation, the Department of Agriculture, the Department of Justice, and then in much smaller amounts – the Department of State and the Department of the Treasury. The R&D "goal" area that receives the most funding is basic research, followed by vaccines and therapeutics, detection and measurement of WMD agents, personal protection and device disposition, information systems and modeling, and then personal and environmental decontamination. See **Table 2**.

The American Association for the Advancement of Science estimated that FY2002 appropriations for counter terrorism R&D total about $1.5 billion, about triple the reported funding level for FY2001. [9] See **Figure 1.**[10]

[9]According to AAAS, "Roughly half the final $1.5 billion comes from regular FY 2002 appropriations, and half from emergency appropriations out of a $40 billion post-September 11 emergency response fund." The legislation referred to is P.L. 107-38 and also H.R. 3338, the Department of Defense Appropriations Act, sent to the President on Dec. 20, 2001, which allocated expenditures for counter terrorism R&D in defense and other areas.

[10]Source: "Counter-Terrorism R&D in Final FY 2002 Appropriations, Federal Counter-Terrorism R&D Nearly Triples to $1.5 Billion in FY 2002," AAAS R&D Funding Update - Jan. 2, 2002.

Figure 1, AAAS Estimates of FY2002 Federal Counter Terrorism R&D

Special Table. Federal Counter-Terrorism R&D, including Weapons of Mass Destruction
Congressional Action on R&D in the FY 2002 Budget (final appropriations Dec. 26, 2001)
(budget authority in millions of dollars)

	FY 2000 Actual	FY 2001 Estimate	FY 2002 Approved	Change FY 01-02 Amount	Change FY 01-02 Percent
Agriculture	37	52	195	143	276.4%
(Agri. Research Service)	*36*	*49*	*191*	*143*	*294.6%*
(APHIS)	*1*	*3*	*3*	*0*	*0.0%*
Commerce (NIST)	10	4	10	6	151.8%
Department of Defense	190	235	353	118	50.1%
Department of Energy	60	68	194	126	184.7%
(NNSA)	*55*	*63*	*109*	*46*	*72.1%*
(Other Defense programs)	*5*	*5*	*85*	*80*	*1634.7%*
Environmental Protection Agency	0	0	70	*70*	- -
Health and Human Services	110	116	451	335	288.2%
(AHRQ)	*5*	*0*	*0*	*0*	- -
(CDC)	*32*	*37*	*130*	*93*	*256.0%*
(FDA)	*0*	*0*	*20*	*20*	- -
(NIH)	*43*	*50*	*293*	*244*	*489.9%*
(Office of Secretary)	*30*	*30*	*8*	*(23)*	*-75.0%*
Justice	45	43	71	28	65.3%
(FBI)	*15*	*7*	*7*	*0*	*0.0%*
(Office of Justice Programs)	*30*	*36*	*64*	*28*	*77.8%*
Nat'l Aeronautics and Space Admin.	0	0	33	*33*	- -
State	7	5	6	1	24.0%
Transportation	51	55	101	47	85.2%
(FAA)	*50*	*55*	*100*	*46*	*84.0%*
(FTA)	*1*	*0*	*1*	*1*	*700.0%*
Treasury	2	1	1	0	0.0%
Total Terrorism R&D	511	579	1,484	905	156.5%

OMB data from OMB's *Annual Report to Congress on Combating Terrorism*, August 2001.
FY 2002 Approved figures are AAAS estimates of R&D in enacted FY 2002 appropriations bills, including emergency funds appropriated in Public Law 107-38 and allocated in appropriations bills.
Figures include conduct of R&D and R&D facilities. Figures do not include non-R&D counterterrorism activities.
December 26, 2001- FINAL

Table 2. Research and Development for Counter Terrorism R&D[11] and for R&D Defense Against Weapons of Mass Destruction (WMD), FY2002 Request, By Subcategory and Agency (Dollars in Millions)[12]

Basic Subcategories for R&D[13]	Dept. Agri-culture	Dept. Com-merce	Dept. Energy	Dept. Health/ Human Services	Dept. Justice	National Security	Dept. of State	Dept. Trans-porta-tion	Dept. Trea-sury	Total
Total Agency Funding for Counter terrorism R&D	**$41.6**	**$4.1**	**$55.6**	**$128.2**	**$23.9**	**$242.7**	**$6.2**	**$51.1**	**$1.2**	**$554.6**
R&D Against Weapons of Mass Destruction, Part of the Total in the Row Above										
Basic Research+ Enabling Capacity	$7.0	$2.0	$16.4	$35.7		$172.7				$233.7
Personal and Collective Protection+ Device Disposition				[1.6] revised	17.0					[18.6] revised total
Detection and Measurement of WMD Agents			32.7	11.2	2.7	19.4		0.7		66.6
Personal+Envi-ronmental Decontam-ination			1.5							1.5
Vaccines, Therapeutics+ Treatments, Including Psychological Effects	34.6			81.3						115.9
Information Systems, Modeling, Simulation,+ Analyses			5.0						0.5	5.5
Total for R&D Against WMD	**$41.6**	**$2.0**	**$55.6**	**$129.8**	**$19.7**	**$192.7**		**$0.7**	**$0.5**	**$441.8**

[11]Defined by OMB as R&D activities "to develop technologies to deter, prevent, or mitigate terrorist acts." (OMB, *Annual Report to Congress on Combating Terrorism,* FY2001, p. 27).

[12]OMB, *Annual Report to Congress on Combating Terrorism,* FY2001, Part 4.

[13]As defined by the Administration.

Monterey Institute of International Studies Funding Data

The Monterey Institute of International Studies published data on funding for federal counter terrorism R&D that used slightly different concepts and categories and also used reports that agencies themselves produced. The Institute reported federal counter terrorism R&D funding for FY2001 (the latest year for which Monterey Institute data were available) that totaled about 40% more than the OMB data for FY2001. The largest percentage differences between the two sets of data were for R&D supported by the national security community and the Departments of Energy, Agriculture, and Commerce. Tables in **Appendix 2** and in **Appendix 3** give detailed data from this source for total counter terrorism R&D and, specifically for R&D to combat WMD, by agency and goal.

Interagency Coordination of Federal Agency Counter Terrorism R&D Policy, Priorities, and Funding

Definition of the Policy Issue

Interagency coordination and priority-setting for counter terrorism R&D are contentious issues and agency roles and functions are evolving following the September 11 terrorist attack. Tensions between centralization and decentralization are difficult to resolve. Some analysts recommend improved processes to determine priorities to meet short and long-term needs and criticize duplication of effort among agencies. They are concerned about the potential for wasteful duplication of resources as more funds are made available for counter terrorism R&D and agencies vie to share these resources. The National Security Council in the Executive Office of the President – which deals primarily with defense and foreign policy threats – has an R&D subgroup that focuses on chemical, biological, nuclear, and radiological weapons. The Office of Science and Technology Policy (OSTP) in the Executive Office of the President chairs this group.

OSTP's overall role in counter terrorism R&D policy relating to homeland security is still unclear. Counter terrorism R&D priority-setting and coordination were not listed among the primary functions of the Office of Homeland Security (OHS) and the Homeland Security Council (HSC) created by Executive Order 13228 on October 8, 2001. R&D was listed as one of the "functional areas" that will be coordinated at the interagency level by one of the Homeland Security Council's associated Policy Coordination Committees. The OSTP Director has said that his office will, for the time being, fill the R&D interagency policy coordination role for the HSC and OSTP and he has convened interagency meetings to inventory and identify gaps in federal agency counter terrorism R&D. Legislation has been introduced to authorize a Homeland Security Agency and give it specific responsibilities for R&D. Alternative coordination mechanisms have been proposed. These existing and proposed mechanisms are discussed in this section and the analysis

of options appears in the section of this report entitled, "Conclusions About Priority-setting, and Policy Options."

Concerns About Coordination of Federal Counter Terrorism R&D

Even before the terrorist attacks of September 11, 2001, several reports recommended a more focused, prioritized, and coordinated federal counter terrorism R&D program. Four of those reports – by GAO,[14] by the National Commission on Terrorism, (the Bremer/Sonnenberg report),[15] by the Advisory Panel To Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (the Gilmore Commission),[16] and by the Center for Strategic and International Studies (CSIS),[17] – recommended that the President develop a long-range strategy to set priorities for, and coordinate, counter terrorism R&D. These groups reasoned that the federal government was the major supporter of such work and needed a long lead time to develop national security-related products and that coordination would promote setting priorities and eliminate duplication. These reports' recommendations generally coincided with those made in a Department of Justice report that called for a long- term comprehensive R&D strategy and plan that sets national counter-terrorism priorities, tracks projects, defines near-and longer time technology needs, supports fundamental research in targeted technical sectors, and promotes technological breakthroughs.[18]

GAO reported in September 2001 that the management of federal R&D to counter terrorism was "limited by a lack of formal mechanisms to capture the entire

---

[14]GAO, *Combating Terrorism: Selected Challenges and Related Recommendations,* September 2001 (GAO-01-822). This report was prepared largely in response to section 1035 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (P.L. 106-398).

[15]National Commission on Terrorism, *Countering The Changing Threat of International Terrorism, Report of the National Commission on Terrorism,* Pursuant to P.L. 277, 105th Congress, June 2000, [http://www.fas.org/irp/threat/commission.html], **(Bremer/Sonnenberg Commission**). The online version of this report does not have page numbers. This is from Chapter 4, "Prepare to Prevent or Respond to Catastrophic Terrorist Attacks."

[16]Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Toward a National Strategy for Combating Terrorism,* December 14, 2000, [second of three reports] Written in cooperation with the Rand Corporation, (**Gilmore Commission**).

[17]Frank J. Cilluffo Sharon L. Cardash Gordon N. Lederman, *Combating Chemical, Biological, Radiological and Nuclear Terrorism: A Comprehensive Strategy* , CSIS, Dec. 14, 2000.

[18]GAO, *Combating Terrorism,* p. 85, referring to *Attorney General's Five-Year Interagency Counter Terrorism and Technology Crime Plan.* According to GAO this classified report was requested by Congress. It was first issued in 1998 and is updated annually. See GAO, *Combating Terrorism,* p. 124.

universe of government wide research and development efforts. The absence of a single oversight and coordinating entity to ensure against duplications further hinders coordination," according to GAO and had led to the use of informal mechanisms, which may not be effective.[19] "For example, the Defense Advanced Research Projects Agency was unaware of U.S. Coast Guard plans to develop methods to detect biological agents on infected cruise ships and, therefore, was unable to share information on its research to develop chemical and biological detection devices for buildings that could have applicability in this area."[20] Also, often different agencies contract with the same laboratories to do counter terrorism-related R&D and, reportedly, contractors charge them separately for the same work. GAO also cited how security classification and compartmentalization prevent the sharing of research information among agencies.[21] The report recommended that the executive branch "complete a strategy to coordinate research and development to improve federal capabilities and to avoid duplication of effort...."[22]

The National Commission on Terrorism, in a statutorily required report released in June 2000, recommended that the "President should establish a comprehensive and coordinated long-term research and development program for catastrophic terrorism."[23] A long lead time is needed to conduct R&D to develop technologies to cope with terrorist attacks, especially involving biological, chemical, or radiological weapons, it said. Therefore, "Given the urgency of near-term needs, long-term research and development (R&D) projects on technologies useful to fighting terrorism will be short-changed unless Congress and the President can agree on special procedures and institutional arrangements to work on research that is risky and has more distant payoffs."

The Gilmore report said there is "no comprehensive national plan – one that establishes clear priorities and precludes unnecessary duplication – for [research, development, test, and evaluation] RDT&E for-combating terrorism."[24] It recommended a comprehensive plan and long-range research for combating terrorism.

A fourth report, by the policy group the Center for Strategic and International Studies (CSIS), synthesized several recent CSIS reports on counter terrorism R&D. It stressed the need for the government to "Develop future year plans and coordinated program budgets" to manage counter terrorism R&D. Specifically it said "Each federal department and agency with a CBRN [chemical, biological, radiological, nuclear] counter terrorism mission should develop five year plans, and long-term research, development, testing, and evaluation (RDT&E) plans, that would

---

[19]GAO, *Combating Terrorism*, September 2001, p. 82-85.

[20]GAO, *Combating Terrorism*, September 2001, p. 83.

[21]GAO, *Combating Terrorism*, Sept. 2001, p 85.

[22]GAO, *Combating Terrorism*, September 2001, p. 17-18.

[23]Bremer/Sonnenberg report. The online version of the report does not have page numbers. This is from Chapter 4, "Prepare to Prevent or Respond to Catastrophic Terrorist Attacks."

[24]Gilmore Commission report, p. v, 37.

be coordinated by the [Senate confirmed] Assistant to the President or Vice President for Combating Terrorism," which it recommended creating.[25]

Interviews reported after September 11, 2001 with governmental officials and experts reiterated these problems. A *Science* magazine article, based on discussions with several experts, quoted Ernest Moniz, an MIT physicist and former chief scientist at the Department of Energy, saying that " 'there is no integrated system,' [and] 'to get one, you have to break a lot of china': interagency jealousies and congressional oversight by a bewildering number of committees."[26]

Use of Existing Agencies

Some proposals to improve coordination of counter terrorism R&D would make more use of existing organizations, such as the Technical Support Working Group, the National Security Council, the Office of Science and Technology Policy, and the National Science and Technology Council. Others would create new bodies. Summarized next are developments related to using existing bodies.

Technical Support Working Group (TSWG). The most visible part of the current federal apparatus for coordinating the planning and conduct of interagency counter terrorism R&D is the Technical Support Working group (TSWG), which operates under the policy guidance of the Department of State-chaired Interagency Group on Terrorism. It identifies, prioritizes, and coordinates interagency and international R&D for combating terrorism. It is mostly "...focused on near-term, requirements-driven, non-medical R&D with a focus on deployable technologies that will serve the needs of first responders."[27] It provides "a way for technologies to be developed when a single agency cannot invest sufficiently in a technology that would benefit multiple agencies...." The TSWG coordinated $60 million worth of R&D in FY2000.[28] This constitutes about 10% of current [before September 2001] federal funding for counter terrorism R&D and what GAO calls "... a minor share of all terrorism-related research and development being conducted across the federal government because numerous federal agencies also independently engage in research and development...specific to their respective agency missions for combating terrorism."[29] About 2/3 of TSWG's funding is from national security agencies and 1/3 comes from some of the more than 40 other agencies that participate in its activities. TSWG also addresses joint international operational requirements through cooperative R&D with the United Kingdom, Canada, and Israel, and has an outreach program, so that State and local agencies can benefit from new technology

---

[25]*Combating Chemical, Biological, Radiological and Nuclear Terrorism: A Comprehensive Strategy* , CSIS, Dec. 14, 2000, pp. vii - viii.

[26]Andrew Lawler, "The Unthinkable Becomes Real for a Horrified World," *Science*, Sept. 21, 2001, pp. 2181–2183, 2185.

[27]"Letter from Robin Cleveland, National Security Programs, OMB, to Stephen Caldwell, GAO, Sept. 4, 2001, in GAO, *Combtaing Terrorism*, Sept. 2001, p. 163.

[28]GAO, *Combating Terrorism*, September 2001, p. 82.

[29]GAO, *Combating Terrorism*, September 2001, p. 82.

developments. The group operates under the "technical oversight of the DOD Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. An Executive Committee chaired by the Department of State representative provides program direction. Members of the Executive Committee include representatives from DOD, DOE, and the Department of Justice (FBI)." DOD manages and executes the programs through the Combating Terrorism Technology Support Office.[30] TSWG has eight subgroups that focus on developing technology and prototyping efforts.[31] Each subgroup has many federal agency members – for instance, the CBW group membership numbers 15 major departments and agencies and many subunits within agencies.

The Gilmore Commission recommended that the TSWG, which also serves "as an adjunct of the 'Interagency Working Group on Counter Terrorism' under the National Security Council, ...become an adjunct to the National Office for Combating Terrorism" [a statutorily authorized cabinet-level body which it proposed creating] "in the same manner that it now serves in the NSC process and that it expand its coordination role for technical aspects of RDT&E for combating terrorism."[32] (For more details about the Gilmore Commission proposal, see below in the section on "Proposals for New Organization With R&D Responsibilities....")

National Security Council. The National Security Council (NSC) has core responsibility to coordinate defense and foreign policy-related counter terrorism R&D policy across the government. It has a Policy Coordinating Committee on Counter Terrorism and National Preparedness and a NSC-chaired Preparedness Against Weapons of Mass Destruction Group (PWMD), with eight subgroups, including a Research and Development Subgroup, which reports to the NSC chair. The PWMD group was chartered under National Security Presidential Decision Directive-1, dated February 2001, to address the government's preparedness to forestall or respond to terrorist incidents involving weapons of mass destruction (chemical, biological, radiological or nuclear). "All federal departments and agencies with interests, equities, or needs in research and development for combating terrorism are represented on the PWMD R&D Subgroup."[33] The subgroup works to coordinate ongoing R&D activities and to assist in the preparation and review of the President's

---

[30]GAO, *Combating Terrorism*, September 2001, pp. 79-82.

[31]Technical Support Working Group, *Program Overview 2000: Technical Support Working Group*, passim, preface, and p. 37. The eight TSWG subgroups deal with:

- blast mitigation stand-off detection of explosives,
- large vehicle bomb countermeasures,
- sentry point screening,
- advanced surveillance equipment,
- VIP protection,
- forensics, vulnerability assessment analysis tools,
- infrastructure protection, countermeasures for chemical and biological devices and agents in urban environments, and
- technical support for responders to terrorist incidents.

[32]Gilmore Report, pp. 36-37.

[33]Letter Cleveland to Caldwell, in GAO, *Combating Terrorism*, p. 164.

budget request for work on counter terrorism R&D and it makes recommendations to the PWMD. The R&D Subgroup is chaired by OSTP; a TSWG co-chair is a member of the Subgroup. While TSWG focuses on shorter term projects only of interest to its members, this NSC subgroup is long-range in nature and "...has a broad role in identifying long-range, large-scale research and development issues that involve preventing, countering, and responding to chemical, biological, radiological, or nuclear terrorist attacks." The PWMD R&D subgroup consults "with other NSC subgroup chairs to identify comprehensive R&D needs in preparedness for combating terrorism; identifying and prioritizing R&D gap-filling objectives; implementing a process for reporting progress toward achieving R&D objectives; and continuing the ongoing effort to achieve concordance of R&D objectives with agency programs."[34]

Office of Science and Technology Policy. The Office of Science and Technology Policy (OSTP) in the Executive Office of the President (EXOP), was established statutorily in 1976[35] to provide the President with advice on science and technology (S&T) issues. The law authorized that the OSTP be headed by a Director, who is presidentially nominated and confirmed by the Senate. It also named the Director as the President's Science and Technology Advisor. From time to time Presidents have named their science advisor an assistant to the President. This is not mandatory nor statutorily required. The current OSTP Director, Dr. John Marburger, was not named an assistant to the President. OSTP does not have a direct role in establishing national security or counter terrorism R&D strategy, but it plays a role in integrating national security R&D since, as mentioned above, it chairs the National Security Council's PWMD R&D Subgroup. GAO recommended that "to reduce duplication and leverage resources, ... the Assistant to the President for Science and Technology,"[36] [who, in the past, has been the Director of the Office of Science and Technology Policy], "[should] ...develop a strategic plan for research and development to combat terrorism, coordinating this with federal agencies and state and local authorities." This should be coordinated with the national strategy to combat terrorism that would have its focal point in the Executive Office of the President.[37]

The U.S. Commission on National Security/21st Century (the Hart-Rudman Commission), that was convened by the Secretary of Defense, reported in *Road Map for National Security: Imperative for Change the Phase III Report*, February 15, 2001.[38] It focused on actions to strengthen national security capability broadly (without focusing specifically on counter terrorism). It recommended creating a cabinet level National Homeland Security Agency (NHSA) with responsibility for planning, coordinating and integrating various U.S. government activities involved in

---

[34]Letter Cleveland to Caldwell, in GAO *Combtaing Terrorism,* p. 165.

[35]Title II of P.L. 94-282 (National Science and Technology Policy, Organization, and Priorities Act of 1976.)

[36]As pointed out, P.L. 94-282, did not create such an "assistant."

[37]GAO, *Combating Terrorism*, p. 87.

[38]U.S. Commission on National Security/21st *Road Map for National Security: Imperative for Change, the Phase III Report*, February 15, 2001, p. 30, Century (the **Hart-Rudman Commission**, convened by the Secretary of Defense).

homeland defense. Federal R&D resources should be doubled to strengthen the science base as a general national security defense. The Commission also urged that OSTP play a paramount role in collecting data about R&D and in developing policies to strengthen the science base and that the "president should empower his Science Advisor to establish non-military R&D objectives that meet changing national needs, and to coordinate budget development within the relevant departments and agencies." It also recommended that the National Science and Technology Council (NSTC), the interagency coordinating group managed by OSTP, should be strengthened to help identify additional creative, targeted large-scale governmental scientific and technological initiatives in key fields.[39] (See Appendix 4 in this report for more details.)[40]

OSTP's Limited Responsibilities to Implement Specific Counter Terrorism R&D Activities. As will be described in greater detail below in the section on the "Office of Homeland Security," the OSTP Director was not named a member of the Council that advises Office of Homeland Security or among the other officials who were identified to be invited to attend relevant meetings of the council, which included cabinet secretaries, and others, such as the Administrator of the Environmental Protection Agency. Also, the OSTP Director was not named to be a member of the Homeland Security Council Principals Committee, the senior interagency forum for homeland security issues that was created on October 29. Eleven Homeland Security Council Policy Coordination Committees (HSC/PCCs),[41] were established, one of which focuses on "Research and Development," but the OSTP Director was not named a member of the PCC on R&D. The eleven committees were tasked to "...manage the development and implementation of homeland security policies by multiple departments and agencies throughout the federal government and ...[to] coordinate those policies with State and local government. The HSC/PCCs shall be the main day-to-day fora for interagency coordination of homeland security policy" and are chaired by a "Senior Director" from the Office of Homeland Security. (OSTP is fulfilling some of these coordination responsibilities. See the next section.)

The OSTP Director was given responsibility to work in two specific R&D areas under Homeland Security Presidential Directive-2, that deals with "Combating Terrorism Through Immigration Policies," issued October 29, 2001. One was to develop, in cooperation with the Secretaries of State, Defense, Energy, and Education and the Attorney General, and academic institutions, a program to "end the abuse of student visas and prohibit certain international students from receiving education and training in sensitive areas, including areas of study with direct application to the development and use of weapons of mass destruction"[42] This would involve identifying sensitive courses of study, identifying "problematic applicants for student

---

[39]Hart-Rudman report, p. 34.

[40]Hart-Rudman Commission, Phase III report, p. 34.

[41]Homeland Security Presidential Directive-1, Subject: Organization and Operation of the Homeland Security Council, October 29, 2001.

[42]Section 3, "Abuse of International Student Status," Homeland Security Presidential Directive-2, Subject Combating Terrorism Through Immigration Policies," Oct. 29, 2001.

visas and denying their applications, and tracking students who receive a visa by looking at "the proposed major course of study, the status of the individual as a full-time student, the classes in which the student enrolls, and the source of the funds supporting the student's education." The plan is to be recommended to the Homeland Security Council by the end of December 2001.

A second responsibility mandated by Homeland Security Presidential Directive-2 required the Director of the OSTP, in conjunction with the Attorney General and the Director of Central Intelligence, to recommend by December 29, 2001, methods and resources needed to use advanced technology to help enforce U.S. immigration laws by facilitating the identification of, and denying access to, aliens who are suspected of engaging in or supporting terrorist activity. Recommendations are also to be made about using existing databases to detect, identify, locate, and apprehend potential terrorists. The Director of OSTP is to submit to the Director of OMB legislative remedies to overcome legal barriers to data sharing to achieve this objective. The OSTP director is to make recommendations on technologies and associated budgetary requirements to the President through the Homeland Security Council by the end of December 2001. The directive did not require explicit coordination between OSTP on this task with the National Security Council's PWMD R&D subgroup.

Executive Order 13231, issued October 16, 2001, gave the OSTP Director a third responsibility, related to cyber security R&D. As described below in the section on "Information Security R&D," the OSTP Director was made a member of the interagency President's Critical Infrastructure Board, which among other things was directed to coordinate with the OSTP Director to develop a federal R&D program to protect "information systems for critical infrastructure."[43] These activities are to be coordinated with NSC.

OSTP-initiated Actions Relating to Counter Terrorism R&D. Despite the lack of formal designation of responsibility, OSTP is undertaking some interagency coordination activities for counter terrorism and homeland security R&D. Even before he was confirmed, OSTP-nominee John Marburger met with more than a dozen major federal department and agency R&D/science chiefs to inventory and assess the strengths and weaknesses of their counter terrorism portfolios. At recent hearings before the House Science Committee Dr. Marburger testified that the NSC's PCC on Preparedness Against Weapons of Mass Destruction, which OSTP chairs, "...initiated briefings from agencies on their bioterrorism-related R&D programs and on specific projects...for detecting and tracking threats."[44] He also said that "OSTP has been asked to fulfill the research and development component of OHS for the time being," which he said previously was the position of "senior director for R&D[45] in the

---

[43]"Critical Infrastructure Protection in the Information Age," Executive Order 13231, issued October 16, 2001.

[44]Statement of Hon. John H. Marburger, "Science of Bioterrorism: Is the Federal Government Prepared?," Hearing before the House Committee on Science, Dec. 5, 2001.

[45]"An Interview With John Marburger: Terrorism, Money, Contacts Top Science Adviser's (continued...)

Homeland Security Council's Policy Coordination Committee on Research and Development.

The OSTP is working with the National Academies and RAND to develop a taxonomy and inventory of agency activities in "antiterrorism R&D" with the objective of identifying "gaps, duplication, and opportunities for collaboration." Dr. Marburger meet several times with representatives of federal agencies to identify their antiterrorism activities...." These meetings, according to Dr. Marburger, typically included representatives of the OMB, OHS, Domestic Policy Council, Office of the Vice President, and Cabinet Affairs.[46] Reportedly, within the last few weeks the Assistant to the President for Homeland Security called upon the OSTP Director for science and technical advice and to provide some "science coordination."[47] Dr. Marburger reported that OSTP coordinated the federal response relating to mail security and baggage inspection at airports in response to direct requests from the Director of Homeland Security[48] and that OSTP has been collaborating closely with the National Coordination Office for Information Technology R&D in the Commerce Department to identify counter terrorism experts.[49]

During his confirmation hearings in October 2001, Dr. Marburger said that in order to help obtain advice about counter terrorism, he would utilize the President's Council of Advisors on Science and Technology (PCAST),[50] which he co-chairs and which includes industrial and academic members.[51] PCAST would be enlisted to assess issues such as "how to better mobilize the creativity and energy of private-sector technology companies in both preventing and responding to terrorism."[52] For additional policy and program support, OSTP also plans to utilize both its own Federally Funded Research and Development Center, the Science and Technology Policy Institute, which is part of the RAND corporation, and, as warranted, the advice

---

[45](...continued)
Agenda,"*Science*, Nov. 23, 2001.

[46]Marburger Testimony, Dec. 5, 2001.

[47]Mooney, op. cit., and "Terrorism, Money, Contacts Top Science Adviser's Agenda," *Science*, Nov. 23, 2001, p. 1642-1644.

[48]Statement of Hon. John H. Marburger, "Science of Bioterrorism: Is the Federal Government Prepared?," Hearing before the House Committee on Science, Dec. 5, 2001.

[49]Testimony at Hearing on the "Response of the Technology Sector in Times of Crisis," Senate Committee on Commerce, Science, and Transportation, Subcommittee on Science, Technology, and Space, Dec. 5, 2001.

[50]Created by Executive Order 12882 in November 1993.

[51]See also, Bara Vaida, "Bush High-Tech Council To Discuss Terrorism at First Meeting," *GovExec.com*, Dec. 12, 2001.

[52]Audrey T. Leath, "Positive Hearing for OSTP Director Nominee Marburger," *AIP Bulletin of Science Policy News*, Oct. 11, 2001.

of the staff and scientists affiliated with the National Academies (National Academy of Sciences, National Academy of Engineering, and Institute of Medicine).[53]

Although OSTP is acting to fulfill R&D coordination activities relating to homeland security and counter terrorism R&D, the extent and amount of formal cooperation between the OHS and OSTP in this regard is still evolving. After his confirmation on October 24, 2001, the new OSTP Director reportedly eliminated two of the divisions that had existed previously – the divisions of national security and of environment – on the grounds that the office was too fragmented.[54] At least one critic, an official of the American Association for the Advancement of Science, is reported to have said that "eliminating the national security position 'is a big blow' to forging links to the powerful National Security Council...[on terrorism issues]."[55] Possible implications of this reported move will be discussed in the concluding sections of this report.

National Science and Technology Council. The National Science and Technology Council (NSTC) was established by Executive Order 12881 on November 23, 1993. This Cabinet-level council is the principal means for the President to coordinate science, space, and technology across the government. The President chairs the NSTC. Membership consists of the Vice President, the Assistant to the President for Science and Technology, who typically is the Director of the White House Office of Science and Technology Policy, cabinet secretaries and agency heads with significant science and technology responsibilities, and other White House officials. The OSTP manages the activities of the Council. The Council prepares research and development strategies for some topics and coordinates them across federal agencies.

The **NSTC's Committee on National Security** (CNS) is intended to provide a formal mechanism for interagency policy review, planning, and coordination as well as the exchange of information regarding national security-related research and development. It was active during the Clinton Administration.[56] So far during the Bush Administration, the NSTC's CNS has participated in "monitoring the research and development subgroup of the interagency Weapons of Mass Destruction Preparedness Group [PWMD subgroup of the National Security Council]. ...The CNS was briefed on and discussed the activities and progress of the R&D subgroup

---

[53]Interviews, October 2001.

[54]David Malakoff and Robert Koenig, "Counterterrorism: U.S. Science Agencies Begin to Lend a Hand," *Science*, Oct. 26, 2001, pp. 761-762; Chris Mooney, "Political Science: The Bush Administration Snubs Its Science Adviser," *The American Prospect*, December 3, 2001.

[55]Lawler, Andrew, "Marburger Shakes Up White House Office," *Science*, Nov. 2, 2001, pp. 973-974.

[56]Three Subcommittees and Interagency Working Groups were active during the last year of the Clinton Administration in 2000, including the Interagency Working Group on Critical Infrastructure Protection Research and Development, the Interagency Working Group on International Technology Transfer Issues and Policy, and the Interagency Working Group on Non-proliferation and Arms Control Technology.

on several occasions."[57] GAO, in its September 2001 report, said neither the OSTP nor the NSTC's CNS have created a national R&D strategy to combat WMD-related terrorism and do not coordinate individual agency projects.[58] "As result," the management of counter terrorism-related R&D is "self-governing and highly dependent on voluntary coordination mechanisms."[59]

As of November 2001, the chairmanship of the NSTC's CNS remains vacant and there has been no announcement regarding if and how the committee will be continued, which could be doubtful given the reported termination of OSTP's national security division. The links, if any, between the NSTC's CNS and the National Security Council's PWMD R&D Subgroup have not been made known. Also unclear is the relationship between the NSTC's CNS and the counter terrorism R&D interagency coordinating role to be played by the Homeland Security Council's Policy Coordination Committee for R&D. (See below under "Establishment of the Office of Homeland Security.")

OSTP's new director testified how he would use the NSTC to deal with counter terrorism as follows:

> Under the structure of the National Science and Technology Council, I am establishing an interagency Antiterrorism Task Force with several working groups to address broad categories of issues. The four categorical working groups focus on Biological/Chemical Detection and Response; Radiological/Nuclear/Conventional Detection and Response; Protection of Vulnerable Systems and Social, Behavioral, and Education Sciences. We are establishing the Technical Response Team as a fifth working group ...[to] establish small subgroups on an ad hoc basis to grapple with emergencies as they arise. The team will also serve as a clearinghouse for technical reviews of the many incoming proposals on technologies related to homeland security. It is important that these proposals be assessed for scientific merit and referred, as necessary, to the appropriate agency for further review.[60]

Proposals for New Organizations With R&D Responsibilities to Combat Terrorism

Several expert reports have called for the creation of a new counter terrorism agency, which would have specific responsibilities to coordinate federal counter terrorism R&D. The Gilmore Commission recommended that the President should establish a statutorily authorized cabinet level National Office for Combating Terrorism in the Executive Office of the President. It would have five major sections,

---

[57] *National Science and Technology Council, 2000 Annual Report,* http://www.ostp.gov/NSTC/html/nstc_ar.pdf.

[58] GAO, *Combating Terrorism: Selected Challenges and Related Recommendations,* September 2001 (GAO-01-822), p. 82.

[59] GAO, *Combating Terrorism,* p. 82.

[60] Marburger, Testimony, "Science of Bioterrorism..., op. cit., Dec. 5, 2001.

each headed by an assistant director. One section, that focused on Research, Development, Test, and Evaluation (RDT&E) and National Standards, would develop a comprehensive plan for long-range research for combating terrorism, "provide direction and priorities for research and development and related test and evaluation...for combating terrorism as well as for developing nationally recognized standards for equipment and laboratory protocols and techniques, with the ultimate objective being official certification."[61] It "would have budget and program and authority to review federal agency programs and budgets to ensure compliance with the priorities it established in the national strategy," [this is more budget approval authority than granted to the Office of Homeland Security]; would coordinate national laboratory R&D to deal with terrorism, and would gather and disseminate information about off-the-shelf research and technology to combat terrorism.[62] The commission also recommended a greater role for OSTP in setting federal R&D priorities and that the proposed Assistant Director for RDT&E and National Standards either enter into a formal relationship with OSTP or have appropriate members of the OSTP staff detailed to the Office for Combating Terrorism on a rotational basis.[63]

CSIS made a similar recommendation – that "Each federal department and agency with a CBRN counter terrorism mission should develop five year plans, and long-term research, development, testing, and evaluation (RDT&E) plans. These would then be coordinated by a Senate-confirmed Assistant to the President or Vice President for Combating Terrorism, who should support a holistic effort to use technology to improve domestic response preparedness and tie RDT&E efforts to practical deployment plans."[64]

Establishment of Office of Homeland Security

On October 8, 2001 the President established the Office of Homeland Security (OHS) by Executive Order 13228, and named Governor Tom Ridge to head it as the Assistant to the President for Homeland Security. The executive order creating the Office of Homeland Security did not include either R&D priority-setting or R&D coordination among the functions assigned to it, which included such things as "detection," "response and recovery," "prevention," and "incident management." However, the office clearly was assigned activities that explicitly or implicitly involve applications of science and technology.[65]

---

[61]Gilmore report, p. xi.

[62]Gilmore report, pp. 37-38.

[63]Gilmore report, pp. 37-38.

[64]CSIS, *Combating Chemical, Biological, Radiological and Nuclear Terrorism: A Comprehensive Strategy* , p. vii.

[65]For instance, with respect to "detection," it was given responsibility to coordinate activities to ensure that agencies have sufficient technological capabilities to collect intelligence data about terrorism, and to coordinate development of monitoring protocols and equipment for use in detecting the release of biological, chemical, and radiological hazards. Under the function

(continued...)

The OHS, located in the Executive Office of the President, has the "mission to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threat or attacks. The Office will coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks...." [66] Also, it will advise the Director of the Budget on programs that will contribute to the Administration's strategy. Although the Assistant for Homeland Security can review the budgets of homeland security-related programs submitted to the OMB and suggest legislation to help agencies fight terrorism, he currently has no statutory authority to modify or approve agency budgets.

Research and Development Coordination Function Assigned to the Homeland Security Council's Policy Coordination Committee

In addition to creating the Office of Homeland Security, Executive Order 13228 created a Homeland Security Council, whose purpose is to advise and assist the "President with respect to all aspects of homeland security." The Council is to "serve as the mechanism for ensuring coordination of homeland security-related activities of executive departments and agencies and effective development and implementation of homeland security policies."[67] The Director of the Office of Science and Technology Policy was not named a member of the Homeland Security Council, nor was he mentioned among those specific officials [department and agency heads] who would be "invited to attend Council meetings pertaining to their responsibilities."[68]

Homeland Security Presidential Directive - 1 regarding the "Organization and Operation of the Homeland Security Council," released on October 30, 2001, created a "Homeland Security Council Principals Committee," – as the "senior interagency

---

[65](...continued)
of "preparedness," it was tasked to coordinate national efforts to ensure public health preparedness, including stockpiling of vaccine and pharmaceuticals and hospital capacity. Under the function of "protection," the office was to coordinate efforts to protect critical infrastructure, including energy, telecommunications, nuclear materials, transportation, agriculture, food and water systems, and access to, and use of, chemical, biological, radiological, nuclear, explosive or other materials. It was also assigned, as part of its "response and recovery" functions, coordination of containment and removal of biological, chemical, radiological, explosive or other hazardous materials. (Executive Order Establishing Office of Homeland Security and the Homeland Security Council, Oct. 8, 2001.)

[66]"President Establishes Office of Homeland Security, Summary of the President's Executive Order, The Office of Homeland Security and the Homeland Security Council," White House Press Release, Oct. 8, 2001.

[67]Executive Order Establishing Office of Homeland Security and the Homeland Security Council, Oct. 8, 2001.

[68]"President Establishes Office of Homeland Security." White House Press Release, Oct. 8, 2001.

forum under the Homeland Security Council."[69] Also established at this time was a Homeland Security Council Deputies Committee (HSC/DC) to serve as the senior sub-Cabinet interagency forum for consideration of policy issues affecting homeland security. The OSTP director was not named a member of the group.

Under the directive, eleven "Policy Coordination Committees" were attached to the Homeland Security Council Office to coordinate the development and implementation of homeland security policies by multiple federal departments and agencies and to coordinate those policies with State and local government. The committees also are to provide "policy analysis for consideration by the more senior committees of the HSC system...." Members "shall include representatives from the executive departments, offices and agencies represented in the HSC/DC" of which the OSTP is not a member. One committee deals with "research and development," and is to be chaired by a senior director from the Office of Homeland Security.[70] It is not clear what relationship the OSTP Director will have to this committee since he is not among the members of the OHS/DC. As noted above in the section on "Office of Science and Technology Policy," the OSTP Director has undertaken some activities related to interagency coordination of counter terrorism and homeland security R&D. Responsibilities and lines of authority are still evolving.

Congressional Proposals to Authorize a Homeland Security Agency With Responsibilities for R&D

Legislative proposals have been made to authorize statutorily the Office of Homeland Security. Two reasons are paramount. Because the office was created by executive order and not by statute, its relationship with Congress is evolving but Congress appears to have no direct oversight of its activities, except for its authority to fund White House offices.[71] Also, there are complaints that since the OHS has no

---

[69]The OSTP Director was not named a member of the Principals Committee. The members are the Secretaries of the Treasury, of Defense, of Health and Human Services, and of Transportation; the Attorney General, the Director of OMB, the Assistant to the President for Homeland Security, the Assistant to the President and Chief of Staff; the Director of Central Intelligence; the Director of the Federal Bureau of Investigation, the Director of FEMA; the Assistant to the President and Chief of Staff to the Vice President. The Assistant to the President for National Security Affairs shall be invited to attend all meetings. The following people are to be invited to the committee meetings when issues pertaining to their responsibilities and expertise are discussed: the Secretaries of State, of the Interior, of Agriculture, of Commerce, of Labor, of Energy, and of Veterans Affairs, the Administrator of the EPA, and the Deputy National Security Advisor for Combating Terrorism. The Counsel to the President may also be invited. Other heads of departments and agencies and senior officials shall be invited, when appropriate.

[70]Homeland Security Presidential Directive-1, Subject: Organization and Operation of the Homeland Security Council, October 29, 2001.

[71]The relationship between the Congress and the OHS is still evolving. The OHS was not established by statute, its chief is not subject to Senate confirmation and has not yet testified before Congress, and funding and support are to be provided from funds currently available to the White House As a result, Congress has less direct oversight than if the office were

(continued...)

specific budgetary authority, it will not be able to effectively establish and coordinate policies.[72]

Some of the legislative proposals would give an authorized office specific responsibilities to deal with federal R&D or science and technology coordination.[73] For instance, H.R. 1158, introduced on March 21, 2001, is under consideration by the House Committee on Government Reform. It would establish a "Homeland Security Agency," which, among other actions, would assume operational authority for the Federal Emergency Management Agency, the Coast Guard, the Border Patrol, and the U.S. Customs Service and some infrastructure protection functions in Commerce and the FBI. It would establish within the new agency an Office of Science and Technology, which would advise the agency Director about R&D efforts and priorities for the directorates established in the agency. These are the Directorate of Prevention; Directorate of Critical Infrastructure Protection, including utilities, transportation, energy resources, and cyber security; and the Directorate for Emergency Preparedness and Response. It would not have explicit authority to coordinate R&D activities at other federal agencies. Hearings were held on the bill, but no further action was taken on it. S.1534, introduced on October 11 would create a cabinet-level Department of National Homeland Security. Its provisions are similar to those of H.R. 1158. Hearings were held on October 12.

H.R. 3026, introduced October 4, 2001 would establish an Office of Homeland Security within the EXOP, with a presidentially appointed, Senate-confirmed Director. Its responsibilities would include establishing a national strategy for homeland security; with OMB developing, reviewing, and approving a budget for homeland security; and reviewing the programs, plans and activities of the agencies to insure effective implementation of a homeland security strategy. The homeland security strategy would include among other things, "a comprehensive research, development, and procurement plan for supporting homeland security."

---

[71](...continued)
statutorily created, direct annual appropriations were provided and the incumbent office head was required to testify before Congress on substantive issues For a discussion on these points, see: Ron Moe, "Office of Homeland Security," CRS Terrorism Briefing Book, Nov. 1, 2001. Somewhat similar constraints on congressional oversight of the National Security Council (which is statutorily authorized) and the Assistant to the President for National Security are discussed in Richard A. Best, Jr., *The National Security Council: An Organizational Assessment*, CRS Report RL30840, February 9, 2001, 42 p. The OSTP is statutorily authorized, funds are appropriated for it annually, the Director is required to be confirmed, and the Director has not been named Assistant to the President and likely will testify on current substantive issues before the OSTP.

[72]See, for instance, "Mr. Ridge Goes to Washington, " *New York Times*, Oct. 8, 2001, op-ed page; Jason Peckenpaugh, "Office of Homeland Security Needs More Power, Lawmakers Say," *GovExec.com*, Daily Briefing, Oct. 10, 2001; and Lauren Hafner, "Office of Homeland Security's Lack of Budgetary Reach Questioned," *Washington Fax*, Oct. 10, 2001.

[73]Other bills that would authorize a form of homeland security agency do not include provisions relating to R&D or S&T. For instance, S. 1449 that would establish a National Office for Combating Terrorism does not include any language relating to R&D.

H.R. 525 would respond to the concern expressed by most counter terrorism commissions that federal-state-local coordination in antiterrorism/response efforts is lacking. It would require the President to ensure that federal response plans and programs are adequate to respond to the consequences of terrorism directed against a target in the United States and it would establish the President's Council on Domestic Preparedness, an interagency council chaired by the President, "tasked with crafting Administration [terrorism] policy and priorities." In its only reference to science and technology, the bill would require "An evaluation of available technologies and practices to determine the best means of protecting transportation, energy, and other infrastructure facilities against terrorist attacks" to be included in the required annual plan. The bill was approved by the Subcommittee on Economic Development, Public Buildings and Emergency Management Subcommittee of the House Committee on Transportation and Infrastructure and was reported to the full committee on September 20.

Other Counter Terrorism R&D Proposals

Other activity is proposed or underway relating to conducting creative counter terrorism R&D, including proposals for a new RAND corporation, an enhanced DARPA and a new "Manhattan" project.

Proposal to Create a RAND-like Independent Think Tank to Support the Office of Homeland Security

A recommendation was made by Joseph S. Nye, dean of the Kennedy School of Government at Harvard, that the then-proposed Office of Homeland Security "be supported by a new research corporation created to deal with terrorism, as the RAND corporation was created in the cold war [by the Air Force] to deal with the nuclear threat. ...[It] should not be bound by the rigidities and inadequate salaries of the federal bureaucracy [and its] ... independence should allow ...[it] to plan an antiterrorist system that can find gaps and overlaps in government agencies' antiterrorism efforts and examine weaknesses in private systems like computer networks."[74]

An Enhanced DARPA or "Manhattan" Project for Counter Terrorism

The Defense Advanced Research Projects Agency (DARPA) is the central R&D agency for the Department of Defense (DOD). It manages and directs selected basic and applied R&D projects, and pursues research and technology where risk and payoff are both very high and where success may provide dramatic advances for

---

[74]Joseph S. Nye, How to Protect the Homeland," *New York Times, Editorial,* September 25, 2001.

traditional military roles and missions.[75] DARPA gives its program managers considerable autonomy to select creative university and industrial scientists for problem solving R&D at the cutting-edge without adhering to the rigorous competitive award procedures customarily used in awarding federal grants and contracts.[76]

Dr. Maxine Singer, President of the Carnegie Institution, recommended that in order to deal with counter terrorism R&D, "An enhanced DARPA, reaching out more widely than it has in the past, may now be desirable. However, a special organization, independent as was the [World War II Office of Scientific Research and Development] OSRD,[77] might be the most productive way to help the nation excel and prevail in the 21st century's arts of war."[78]

Related to this proposal, former Senator Sam Nunn, now head of the Nuclear Threat Initiative which also addresses chemical and biological warfare, reportedly recommended creation of a "A 'Manhattan project' [like the special government/academic/industrial collaborative scientific effort during World War II that led to the development of the atom bomb] to accelerate research and provide more and better vaccines and antibiotics"[79] to enhance the fight against counter terrorism.

Creative R&D for Counter Terrorism

There has been discussion in the media about fostering creative non-traditional counter terrorism R&D. For example, a recent news article described a contract awarded by the U.S. Army to the University of Southern California's Institute for Creative Technology, with film makers and writers with connections to terrorist-movie production to "brainstorm about possible terrorist targets and schemes in America and to offer solutions to those threats..." [80] More mainstream is the Center for Emerging Threats and Opportunities, (CETO), a unit of the Marine Corps headquartered at Quantico, which does research and interacts with the public to explore creative methods and to identify emerging non-traditional threats and

---

[75]From: http://www.arpa.mil/.

[76]From: http://www.arpa.mil/body/overtheyears.html

[77]During World War II, the Office of Scientific Research and Development (OSRD) in the White House not only mobilized nongovernmental academic and industrial scientists for defense (leading to the success of the Manhattan project and development of nuclear weapons, penicillin and radar, which contributed to the Allied victory), but laid the foundation for the creation of the White House Science advisory apparatus. (See, for instance, G. Pascal Zachary, *Endless Frontier: Vannevar Bush, Engineer of the American Century,* Cambridge, MIT Press, 1999, 518 pp.)

[78]Maxine Singer, "Answers From Outside the Box," *Washington Post,* Sept. 14, 2001, p. A21.

[79]Albert R. Hunt, "An Accelerated Agenda for the Terrorism Threat," *Wall Street Journal,* October 25, 2001, p. A21.

[80]"U.S. Army Seeks Hollywood Theories," *MSNBC News,* Oct. 8, 2001.

capabilities to meet these challenges.[81] Some scientists, coping with dilemmas about the potential evils that can flow from misuse of science and technology by terrorists, formed a think tank called the Foresight Institute in Los Altos, California. Its goal is to assess the uses and consequences of new technology, in particular "to prepare for the transforming powers of new technologies, and in particular, of nanotechnoloy."[82]

Priorities for, and Coordination of, Bioterrorism and Information Security Counter Terrorism R&D

Definition of the Policy Issue

Even before the terrorist attack of September 11, as noted above, expert reports recommended that mechanisms be established to set priorities and coordinate programs for counter terrorism R&D. For instance, the CSIS recommended that "...the vice president and the national coordinator [for homeland security which it proposed creating] need to assess the United States' present and future needs against its ongoing research efforts and make detailed recommendations to the president and the Congress."[83] Recommendations have been made in authoritative reports, congressional testimony, and by noted experts, for instance the National Commission on Terrorism, the Defense Science Board, and the House Science Committee chairman, for specific priorities for federal counter terrorism R&D in a variety of "functional" program areas.[84] Presented next is information and options related to

---

[81]See: [http://www.ceto.quantico/usmc.mil/about.asp].

[82]Gina Kolata, "When Science Inadvertently Aids An Enemy," *New York Times,* Sept. 26, 2001

[83]Frank Cilluffo, Joseph J. Collins, Arnaud de Borchgrave, Gouréé, and Michael Horowitz, *Defending America in the 21st Century: New Challenges, New Organizations, and New Policies Executive Summary of Four CSIS Working Group Reports on Homeland Defense*, CSIS, 2000, pp. 15-16.

[84]In a speech before SUNY university presidents on October 1, 2001, House Science Committee Chairman Boehlert advised that "the general thrust of R&D need not change" as a result of the September 11 terrorist attacks. But he identified a few areas where research "has probably been inadequate," including computer security, intelligence – "research that will enable us to gather better intelligence to foil terrorist plots and other crimes before they are implemented –" identification techniques, social sciences and humanities research on the causes of terrorism and the reaction to it, and some environmental areas. (Available at [http://www.house.gov/science/press/speeches/ speech100101.htm].) Many congressional committees have held hearings on counter terrorism and research-related issues relating for instance to bioterrorism, vaccine R&D, cyber security, R&D for critical infrastructure protection, aviation safety, and so forth. (For the latest information on these topics, see the various policy issues discussed in the electronic CRS, "*Terrorism Briefing Book: Legislative Issues*," available to Congress at [http://www.congress.gov/brbk/html/ebter1.html], continuously updated.)

The Defense Science Board in February 2001 issued a 4 volume report, *Protecting the*

(continued...)

two program areas – bioterrorism R&D and information security R&D. Key recommendations for priorities and coordination mechanisms are reviewed and actions and legislative proposals relating to these topics are summarized to illustrate the various alternative mechanisms being used for counter terrorism R&D in specific functional areas.

Funding for Bioterrorism R&D and Information Security R&D. As noted above, it is difficult to assess priorities because the federal government does not uniformly collect data which describe programs and expenditures for counter terrorism R&D in specific functional areas such as "bioterrorism" or cyber security. For instance, GAO reported that the six federal agencies, excluding DOD, allocated about $160 million to bioterrorism R&D in FY2001.[85] This may be an underestimate, given that DHHS alone reported funding of over $108 million for bioterrorism research for FY2001. In addition, although GAO said it could not report figures for DOD, appropriations report data show that DARPA alone spent about $167 million in FY2001 for chemical and biological warfare R&D and, in addition, the rest of DOD allocated about $392 million to chemical and biological defense RDT&E spending.[86] DOD alone was seeking about $849 million for FY2002 for its chemical and

---

[84](...continued)
Homeland, 2000 Summer Study, that identified actions needed, including R&D priorities for unconventional nuclear threat, threat to information security, and biological warfare threats.

The Bremer/Sonnenberg Commission listed "the type of projects that could constitute a long-term R&D program." These included:

- New sensors to detect nuclear weapons in transit (e.g., gamma-ray imaging systems, including stimulation to elicit detectable emissions).
- High power ultraviolet beams to destroy BW agents and to clean up contaminated areas.
- New types of "tripwires" suitable for many different entry-points (e.g., explosive-sniffers, body scanner), and their proto-typing for mass-production.
- Advanced development of anti-virals for smallpox.

It also discussed the option of establishing a research/prototyping operation at a national laboratory especially in the fields of biotechnology and pharmaceutical production techniques with special incentives that would attract talented scientists to work for the government for a two-year period. (Bremer/Sonnenberg report, Chap. 4.)

Among the priorities for targeted research cited by the Gilmore Commission were: responder personnel protective equipment; medical surveillance, identification, and forensics; improved sensor and rapid readout capability; vaccines and antidotes; and communications interoperability. It also tasked the National Institute of Standards and Technology (NIST) and the National Institute for Occupational Safety and Health (NIOSH), as federal co-lead agencies for the technical aspects of standards development for counter terrorism technology. (Gilmore report, pp. xi. and 36-39.)

[85]GAO, *Bioterrorism: Federal Research and Preparedness Activities*. September 2001, GAO-01-915, pp. 8, 9.

[86]This information appeared in an as yet unnumbered House Appropriations Committee report on the DOD appropriations bill, FY2002. RDT&E is the term DOD uses to report R&D funding.

biological RDT&E programs. For security purposes DOD does not differentiate between funding for biological and chemical R&D.[87]

With respect to information security R&D, according to the President's Commission on Critical Infrastructure Protection, about $250 million was being invested in FY1997 (the latest year for which data are available) on critical infrastructure protection R&D, with 60% or $150 million, for information security. The commission recommended an increase ranging from $250 million to $500 million in FY1999, "with incremental increases ... over a five-year period to $1 billion in FY04."[88] It is generally acknowledged that DOD provides the lion's share of information security R&D funding because of its mission needs. Precise funding amounts are unknown. However, one of DOD's constituent agencies, the National Security Agency (NSA), reported an information security RDT&E budget of $308 million for FY2000 and requested $415 million for FY2001.[89]

Bioterrorism R&D

Agencies that support bioterrorism R&D coordinate priority-setting and programs informally via consultative mechanisms. Options have been discussed to make coordination mechanisms more formal and to increase funding for R&D. Other options include a proposal to create a federally owned, contractor-operated facility for drug/vaccine R&D and production.

Options for Priority-setting and Organization. Experts suggest that the nation's public health infrastructure and medical care system are ill-equipped to deal with a bioterrorist attack. They contend that too few medical personnel are trained to recognize biological attacks. Some say that different agencies use different lists of dangerous biological agents, that there is a shortage of sophisticated laboratories to identify the agents, and that laboratories lack an accessible information system for communicating and sharing data rapidly with one another and with other components of the pubic health system. Inadequate plans exist for setting up quarantines and emergency facilities to handle the sick and infectious victims. Some describe inadequate cooperation between the intelligence and scientific communities as a serious defect.[90] Among the recommendations for improving the nation's bioterrorism preparedness and response capability is the establishment of new research

---

[87]DOD's programs in these fields were detailed by Dr. Anna Johnson-Winegar, Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense, in "Biological Terrorism: Department of Defense Research and Development," Testimony before the House Science Committee, Dec. 5, 2001.

[88]*Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection*, October 1997, p.89.

[89]DOD, *DOD's Amended FY2001 Budget, R-1* document.

[90]Comments attributed to outgoing Institute of Medicine President Kenneth Shine and to Margaret Hamburg, Vice President for Biological Programs at the Nuclear Threat Initiative (Lauren Hafner, "Preparation for Bioterrorist Episodes Will Require a "Broader and Deeper" Research Agenda, Says Hamburg," *Washington Fax,* Dec. 19, 2001.

and development priorities[91] and organizational changes to enhance R&D and to develop bioterrorism R&D policy.

A September 2001 GAO report, *Bioterrorism: Federal Research and Preparedness Activities,* reiterated recommendations of previous GAO reports that federal bioterrorism R&D was not well coordinated and therefore led to possible program duplication. It also faulted the OMB for not identifying better priorities for bioterrorism programs. It described some on-going informal federal agency collaborative activities and difficulties in coordinating bioterrorism R&D since different agencies have responsibility for coordinating different aspects of the program. It mentioned that the Vice President was charged with working with the National Security Council to integrate bioterrorism response activities and that the TSWG has supported bioterrorism research projects which were relevant to several agencies.[92]

The National Commission on Terrorism's recommendations relating to bioterrorism research focused largely on physical security of pathogens used in research laboratories.[93] CSIS concluded that "...many experts believe that the federal government should foster an acceleration of research in immunology and genetics with the objective of putting improvements in immune responses ahead of the ability to create new and more deadly biological agents." It recommended that costs and benefits of this option be studied.[94] It also said that the government should take other steps to improve bioterrorism R&D, including

> Tap the scientific and biomedical research communities. Develop networking relationships with the scientific and biomedical research communities, whose knowledge of emerging capabilities and of other information gleaned from the open scientific literature, international scientific collaborations, and conferences could prove invaluable to the intelligence community—particularly with respect to the bioterrorism threat...[95]

---

[91]For an authoritative report, see, Centers for Disease Control and Prevention, *Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response, Recommendations of the CDC Strategic Planning Workgroup,* April 21, 2000 / 49(RR04); 14 pp, [http://www.cdc.gov/mmwr/preview/mmwrhtml/rr4904a1.htm]. See also: Sheryl Gay Stolberg, "Health Secretary Testifies About Germ Warfare Defenses," *New York Times,* Oct. 4, 2001 and "When Menacing Microbes Become Deadly Weapons," *Wall Street Journal,* (Review of *Germs: Biological Weapons and America's's Secret War*), Oct. 4, 2001.

[92]GAO, *Bioterrorism: Federal Research and Preparedness Activities*, September 2001, pp. 8, 14-15, and 19.

[93]Bremer/Sonnenberg report.

[94]Frank Cilluffo, Joseph J. Collins, Arnaud de Borchgrave, Daniel Gouréé, Michael Horowitz, *Defending America in the 21st Century: New Challenges, New Organizations, and New Policies Executive Summary of Four CSIS Working Group Reports on Homeland Defense,* CSIS, pp. 14-15.

[95]*Defending America in the 21st Century*, p. 17.

> Develop an integrated plan for biomedical research capabilities of the Departments of Defense and Health and Human Services. Ensure that applied research receives adequate focus as compared to long-term bench research projects. [96]
>
> Give greater attention to psycho social issues and public response. Research must be conducted to better anticipate public response, short-term and long term, in the event of a bioterrorism attack. Appropriate communications strategies, interventions and response plans must be developed in light of that research. In addition, training of psycho social service providers must be undertaken, and such providers must be fully integrated into crisis and consequence management planning.[97]

One of the most comprehensive agendas for bioterrorism was included in the Institute of Medicine report, *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response to Chemical and Biological Terrorism Incidents*, prepared in 1999.[98] The report was prepared for the U.S. Department of Health and Human Services' Office of Emergency Preparedness. It includes recommendations for R&D needs in the areas of pre-incident communication and intelligence: linking the intelligence and medical communities; personal protective equipment; detection and measurement of chemical agents; recognizing covert exposure in a population; detection and measurement of biological agents; patient decontamination and mass triage; availability, safety, and efficacy of drugs and other therapies; prevention, assessment, and treatment of psychological effects; and computer-related tools for training and operations.

The Defense Science Board (DSB) in a February 2001 report, made three major R&D-related recommendations to deal with biological warfare. The first was that the DOD should take action to develop a database of biological weapons, a "Bio-Print" database that would create "signatures" of the top 50 bioagents that cause human disease to help in developing medicines and vaccines against them and trace their "leakage," The second recommendation was to create a "Zebra Diagnostic Chip" to automatically diagnose biological warfare related diseases in patients and to identify the pathogen against those in the "Bio-Print" database to permit rapid diagnoses and treatment protocols. The third priority was to develop a computer network to rapidly warn health care centers about man-made outbreaks of bioagents. The DSB recommended "that the Pentagon invest heavily in research and development for bioagents drugs and vaccines, and work with the Food and Drug Administration to accelerate" the process used to review and certify drugs.[99]

Proposals to Create a Government-Owned Facility for Bioterrorism R&D and Drug Production. Recommendations have been made to create a government facility for R&D and manufacture of vaccines and drugs for bioterrorism.

---

[96]*Defending America in the 21st Century*, p. 22.

[97]Frank J. Cilluffo, Sharon L. Cardash, and Gordon N. Lederman, *Combating Chemical, Biological, Radiological and Nuclear Terrorism: A Comprehensive Strategy,* CSIS, p. 74.

[98]Available from the National Academy Press, 304 pp.

[99]*Protecting the Homeland*, Report of the Defense Science Board 2000 Summer Study, Executive Summary, Vol. 1, February 2001, pp. 13-14.

For instance, the Defense Science Board recommended that the "Pentagon fund a $50 to $100 million manufacturing facility for vaccines or 'after exposure drugs' in order to speed production."[100] The Gilmore Commission, in a new report released October 31, 2001, recommended creation of a government-owned, contractor-operated national laboratory to research, develop and produce vaccines to combat biological terrorism. It reasoned that the private sector is unlikely to develop and manufacture some of the more difficult vaccines such as for smallpox and anthrax for lack of funding and concerns about vaccine liability that a proposed federal laboratory would be able to overcome. The commission also urged the government to develop a "comprehensive plan for the full spectrum of medical and health research for terrorism-related medical issues.[101] In hearings before the Senate Government Affairs Committee, Phillip Russell, former director of the U.S. Medical Research Institute for Infectious Disease at Fort Detrick, "said a government-owned, contractor-operated facility to manufacture vaccines for possible biological weapons that have no commercial interest to private industry should be 'seriously considered.'"[102] Similarly, it was reported that "the governing council of the Institute of Medicine, chaired by IOM president Kenneth Shine, concluded on 5 November that a "National Vaccine Authority" is "long overdue."[103] The Defense Department established and chairs a Federal Interagency Advisory Group to coordinate interests of agencies, including OHS, OSTP, NSC, OMB, FEMA, DHHS, Department of Agriculture, U.S. Agency for International Development.[104]

In contrast, in an October 2000 report on the military's anthrax vaccine program, the Institute for Defense Analysis concluded against a government owned, contractor-operated facility on the grounds that it could cost more than a commercial facility and could make the government responsibility for a biohazard facility that would become obsolete in a few years.[105] Alternatively, the Biotechnology Industry Organization (an organization that represents over 1,000 biotechnology firms, academic institutions and state biotechnology centers) proposed that the government provide long-term financial commitment and protection from antitrust actions and private lawsuits for R&D on agents to counter a bioterrorist attack. Federal support is necessary, the group said, since a commercial market might not exist for these products, preventing industry from obtaining financial support or venture capital for this work. Others say that caution is necessary and the government should not compromise regulatory

---

[100]*Protecting the Homeland*, Executive Summary, Vol. 1, February 2001, pp. 13-14.

[101]Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Third Annual Report to the President and the Congress, Advance Executive Summary, III. For Ray Downey,* Oct. 31, 2001, p. 8.

[102]Nura Shehzad, "National Vaccine Lab Should Be Established, Says Gilmore Commission," *Washington Fax,* Nov. 9, 2001.

[103]Eliot Marshall, "Counterterrorism: U.S. Enlist Researchers as Fight Widens Against Bioterrorism," *Science,* Nov. 9, 2001, pp. 1254-1255.

[104]Anna Johnson-Winegar, Testimony, Dec. 5, 2001, op. cit.

[105]Institute for Defense Analyses, *Resuming Production of the Anthrax Vaccine as Quickly as Possible; Analysis of Alternative Business Arrangements, Vol 1, Main Report,* October 2000, IDA. Paper P-3553.

standards since some drug companies may be seeking to profit by obtaining more federal support for drug R&D, exemption from antitrust regulations, and immunity from lawsuits for vaccines developed to combat bioterrorism.[106]

Policy Actions. Both major federal agencies that support most federal bioterrorism R&D, the Department of Health and Human Services and the Department of Defense, appear to have developed formal intra-agency coordination mechanisms to set priorities and guide programs. However, interagency coordination is informal, raising questions about the extent of collaboration in priority-setting and program implementation.

For instance, in 1993, Congress passed Public Law 103-160, of which Section 1703 created a Joint Service Chemical and Biological Defense Program (JSCBDP), which develops and oversees the defense research and development program in this area. It is chaired by a Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense. The JSCBDP establishes priorities, monitors work and sees that results are integrated into defense programs. It coordinates via informal consultations with other agencies that support or conduct bioterrorism R&D, such as NIH and DOE, to ensure eliminating duplication. It also established and chairs a federal interagency advisory group to deal with the issue of establishing a production facility for "biological defense vaccines" with participation from OSTP, the Office of Homeland Security, National Security Council, OMB, Federal Emergency Management Agency (FEMA), DHHS agencies.[107] The JSCBDP is required to report to Congress annually.[108] DOD also supports a Joint Medical Chemical and Biological Defense Research Program.

The Department of Health and Human Services has taken steps to coordinate bioterrorism activity within the agency. In June 2001, Dr. Scott Lillibridge, a leading national bioterrorism expert, was named the Secretary's Special Assistant for National Security and Bioterrorism.[109] On November 1, to help coordinate the response to bioterrorism, DHHS Secretary Tommy Thompson created an Office of Public Health Preparedness, headed by Dr. Donald A. Henderson, director of the Johns Hopkins Center for Civilian Biodefense Studies and one of the nation's leading bioterrorism experts. His special adviser on vaccine is retired Maj. Gen. Philip Russell, former

---

[106]Leslie Wayne and Melody Petersen, "Drug Industry, A Muscular Lobby Tries to Shape Nation's Bioterror Plan," *New York Times*, Nov. 4, 2001.

[107]Statement of Dr. Anna Johnson-Winegar, Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense on Biological Terrorism, before the Senate Committee on Government Affairs, Oct. 17, 2001.

[108]*Department of Defense Chemical and Biological Defense Program, Annual Report to Congress And Performance Plan*, July 2001, pp. 14-15, [http://www.acq.osd.mil/cp/nbc01.pdf]. See also, *Joint Program Chemical and Biological Defense Program Overview, FY 2001*, at[http://www.acq.osd.mil/cp/reports.html].

[109]"Secretary Thompson Testifies on HHS Readiness and Role of Vaccine Research and Development Tuesday," DHHS Press Office, Oct. 23, 2001.

head of the Walter Reed Army Institute of Research.[110] The new office's R&D coordination functions have not been described yet. The DHHS Secretary has described the department's informal mechanisms for collaborating in bioterrorism R&D with CDC, FDA, NIH, especially the National Institute of Allergy and Infectious Diseases,[111] and DOD, especially the Army Medical Research Institute of Infectious Diseases, the Office of Naval Research, and DARPA.[112]

As noted above, the Homeland Security Council has Policy Coordination Committees to ensure interagency coordination of specific aspects of homeland security. One committee deals with Research and Development and another focuses on Medical and Public Health Preparedness. The secretaries of major departments, including DHHS and DOD, are members of the council and groups which comprise the Homeland Security Agency. The functions of these groups have not been publicly discussed.

Congressional Options. Many congressional hearings, several addressing research issues, have been held on bioterrorism this fall.[113]

---

[110]Ceci Connolly, "U.S. Reorganizes Bioterror Strategy, Moves Aimed At Improving Relations Between HHS, CDC," *MSNBC News*, Nov. 8, 2001.

[111]NIAID developed new bioterrorism programs with seven R&D initiatives. (John T. Softcheck, "NIAID Creates Bioterrorism Initiatives to Facilitate Outpouring of Science-Community Support," *Washington Fax*, Dec. 13, 2001. These include Rapid Response Grant Program on Bioterrorism-Related Research, Small Business Program on Bioterrorism-related Research, Partnership for Novel Therapeutic, Diagnostic and Vector Control Strategies in Infections Diseases , Exploratory/Developmental Grants, NIAID Investigator-initiated Small Research Grants, and contracts for U.S.-Based Collaboration in Emerging Viral and Prion Diseases, and SAIC Anthrax Vaccine Contract [http://www.niaid.nih.gov/dmid/bioterrorism/].

[112]Statement of Tommy G. Thompson, "Civilian Preparedness for Biological Warfare and Terrorism: HHS Readiness and Role in Vaccine Research and Development," Testimony Before the Committee on Government Reform, Subcommittee on National Security, Veterans Affairs and International Relations, Oct. 23, 2001.

[113] In the Senate, by the Committee on Foreign Relations, "The Threat of Bioterrorism and the Spread of Infectious Diseases," Sept. 5; Committee on Appropriations, Subcommittee on Labor, Health and Human Services, and Education, "To Examine Bioterrorism Issues, Focusing on Strengthening Health Surveillance Capacity, Support for Preparedness Measures and Continued Research, and Helping Hospitals and Medical Professionals in the Face of Possible Attacks," Oct. 3; Committee on Health, Education, Labor, and Pensions, "Effective Responses to the Threat of Bioterrorism," Oct. 9; Committee on Governmental Affairs, Subcommittee on International Security, Proliferation and Federal Services, "To hold hearings to examine federal efforts to coordinate and prepare the United States for bioterrorism," Oct. 17; Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, "To examine the Dark Winter scenario and Bioterrorism ," Oct. 25; Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information, "To Examine New Threats to America, Focusing on Germs, Toxins, and Terrorism, Nov. 6; Committee on Governmental Affairs, Subcommittee on Technology, Terrorism, and Government Information, "To Examine New Technologies for Terrorism Prevention, Focusing on Biometric Identifiers," Nov. 14; Committee on the Judiciary, Subcommittee on Technology, Terrorism , and Government Information, "To Examine the Availability of Security Related

(continued...)

Legislative action relating to bioterrorism R&D focused on increasing funding and improving the organization of research. These options will be discussed next. (In P.L. 107-56, the "USA PATRIOT Act," the Congress enacted legislation that criminalized the possession of a biological agent, toxin or delivery system while protecting situations where the use is "reasonably justified by a prophylactic, protective, bona fide research or other peaceful purpose" and instituted controls on access to some

---

[113](...continued)
Equipment and the Status of the Development of Future Technologies to Prevent Terrorism , Focusing on Applied Biometrics (The Statistical Study of Biological Phenomena), Including an Integrated " Nov. 14; Subcommittee on Technology, Terrorism , and Government Information, "To Examine the Protection of Nuclear, Radiological Materials, and Infrastructure from Terrorism," Nov. 29; Committee on Appropriations: Subcommittee on Labor, Health and Human Services, and Education, "To Examine Funding for Bioterrorism Preparedness, Focusing on Increased Surveillance and Epidemiological Capacity, Coordination Of Community Disaster Response Plans, and Improvement of Decontamination and Treatment Facilities, U.S. Passenger and Transit Rail Infrastructure, Focusing on Counter-terrorism Equipment, Security Related Training Programs, and Technologies Capable Of Detecting Chemical and Biological Agents on Transit Systems," Dec. 13. In the House, by the Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, "A Silent War: Are Federal, State, and Local Governments Prepared for Biological and Chemical Attacks?" Oct. 5; Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, "Combating Terrorism: Assessing the Threat of Biological Terrorism,"' October 12; Committee on Government Reform, Subcommittee on National Security, Veterans' Affairs, and International Relations, "Biological Warfare Defense Vaccine Research and Development Program," Oct. 23; Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, "A Review of Federal Bioterrorism Preparedness Programs: Building an Early Warning Public Health Surveillance System," Nov. 1; Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, "HHS Inspector General's Review of Physical Security at NIH and CDC Facilities," Nov. 7; Committee on Energy and Commerce, "A Review of the Role of the Centers for Disease Control and Prevention (CDC) in Public Health Protection," Nov. 15; Committee on Government Reform, Subcommittee on National Security, Veterans' Affairs, and International Relations, hearing on ``Chemical and Biological Defense: DOD Medical Readiness,'' Nov. 7; Committee on Science, "Decontamination of Anthrax and Other Biological Agents," Nov. 8; Committee on Government Reform, "Comprehensive Medical Care for Bioterrorism Exposure–Are We Making Evidence-Based Decisions? What are the Research Needs?," Nov. 14; Committee on Energy and Commerce, "Bioterrorism and Proposals to Combat Terrorism," Nov. 14; Committee on Agriculture, "USDA Biosecurity Programs and Authorities." Nov.15; Committee on International Relations,"Bioterrorism: Potential Sources of Anthrax," Dec. 5; Committee on Science, "Science of Bioterrorism: Is the Federal Government Prepared?'' Dec. 5; Committee on International Relations, "Hearing on Russia, Iraq, and Other Potential Sources of Anthrax, Smallpox and Other Bioterrorist Weapons,"Dec. 3; Committee on the Budget,"Re-Structuring Government for Homeland Security: Nuclear/Biological/Chemical Threats, Dec. 5; Committee on Government Reform, Subcommittee on Technology and Procurement Policy, "Battling Bioterrorism: Why Timely Information-Sharing Between Local, State and Federal Governments is the Key to Protecting Public Health,"Dec. 13; and by the Permanent Select Committee on Intelligence, Subcommittee on Terrorism and Homeland Security, "Defending the Homeland: Reports of the Defense Science Board on Biological, Chemical, Nuclear and Other Asymmetric Threats and Defenses," Oct. 3..

persons. Additional legislation has been introduced on this topic. This issue is not addressed in this report).

NIH and CDC and Other Health Agencies. Major legislative proposals that address bioterrorism R&D in the health agencies focus on such issues as enhancing R&D priority-setting and coordination, expanding funding for specific kinds of R&D, improving cooperation with pharmaceutical firms, and R&D coordination on bioterrorism at the Department of Veterans Affairs.

The creation of an interdepartmental "Working Group on Preparedness for Acts of Bioterrorism," composed of the Secretary of DHHS in coordination with the Secretary of Defense, was authorized by P .L. 106-505 (which incorporated the text of S. 2731, the "Public Health Threats and Emergencies Act," that had been introduced by Senators Edward Kennedy and Bill Frist during the 106th Congress). Among its functions, the working group would "coordinate research on pathogens likely to be used in a bioterrorist attack on the civilian population as well as therapies to treat such pathogens;" coordinate R&D on equipment to detect pathogens likely to be used in a bioterrorist attack and to protect against infection; and develop priorities for, and conduct, research relating to, among other things, epidemiology and pathogenesis of potential bioweapons, the development of new vaccines against pathogens, and the development of medical diagnostics to detect potential bioweapons. The law authorized a demonstration program to detect and respond to bioterrorist attacks, with awards to public entities and required that the awards approval process consider the applicant's proximity to, and collaboration with, a major research university. $215 million was authorized for the first year for the DHHS Secretary to deal with the consequences of bioterrorist attacks. Funds were never appropriated to implement these provisions. Reportedly, Senators Kennedy and Frist were seeking full funding of the act[114] at $1.4 billion[115] via a request to the Senate Appropriations Committee.

Senators Kennedy and Frist introduced the "Bioterrorism Preparedness Act of 2001," S. 1715, on November 16. It was subsequently reintroduced as S. 1765;[116] the House companion bill,. introduced by Representative Ganske, is H.R. 3310. Total funding requested for S. 1765 was about $3.2 billion, more than double the amount of the Administration's proposal of $1.5 billion[117] and more than the $2.96 billion authorized in the House bill. With respect to R&D, Title II of S.1765, would improve

---

[114]Bradie Metheny, "Full Funding of Public Health Energy Act Passed Last Year Sought By Kennedy and Frist," *Washington Fax,* Sept. 19, 3001.

[115]David Glendenning, "Sponsors Expect Smooth Passage of More Bioterrorism Money on Broad Senate Bill," *Washington Fax,* Oct. 24, 2001.

[116]Placed on Senate Legislative Calendar under General Orders. Calendar No. 255, Dec. 5, 2001.

[117] This amount is about 1/3 of the original Kennedy/Frist goal ("Kennedy Seeking More Bioterror Funds," *News From the New York Times*, Oct. 19, 2001); David Glendenning, "Sponsors Expect Smooth Passage of More Bioterrorism Money on Broad Senate Bill," *Washington Fax,* Oct. 24, 2001; Major Garrett, "White House to Back Bioterrorism Bill," *CNN.Com,* Nov. 15, 2001.

the federal laboratory capacity for surveillance and would establish an Assistant Secretary for Emergency Preparedness at DHHS to coordinate all functions within DHHS relating to emergency preparedness, including preparing for and responding to biological threats and attacks. Title III would create an expanded interdepartmental Working Group on Bioterrorism, including the Secretaries of DHHS, DOD, Veterans Affairs, Labor, and Agriculture, the Director of FEMA, the Attorney General and other officials. Among the group's responsibilities would be coordination of the development of bioterrorism countermeasures, research on pathogens likely to be used in a biological attack, and development of shared standards for equipment to detect and protect against biological pathogens. Title III would also give the Director of the Occupational Safety and Health Administration specific authority to expand research on health and safety of workers at risk from biological threats. Title IV would accelerate "countermeasure R&D" at DHHS in specific areas including biological agents and toxins, new treatments and vaccines, new diagnostic tools and R&D relating to children and vulnerable populations. It also would provide a limited antitrust exemption to allow vaccine and drug manufacturers to discuss and agree upon how to develop and produce new countermeasures.[118] Title V authorizes specific amounts for biosecurity upgrades for agricultural security R&D facilities and programs at the Departments of Agriculture and DHHS. Specific amounts were authorized to be appropriated for some other authorized activities.

H.R. 3448, on the same subject and introduced by Rep. Tauzin, passed the House on December 12. It is similar in many respects to S. 1765 that was passed in the Senate on December 20, 2001, as a substitute amendment to H.R. 3448. The original House bill would among other things require an evaluation the potential for collaboration between the DHHS and Department of Veteran's Affairs in bioterrorism research and prevention, would establish the Office of Assistant Secretary for Emergency Preparedness in the DHHS to among other things coordinate R&D for priority vaccines, other biological products, drugs, and devices useful for detecting or responding to a bioterrorist attack or other public health emergency. Like S. 1765, it would create an interdepartmental Working Group on Preparedness for Acts of Bioterrorism, with responsibilities like those outlined in S. 1765. Also, like S. 1765, it would authorize DHHS to develop a program of accelerated countermeasure research and development and technology development and R&D on worker safety; it would authorize the Secretary of Energy to conduct R&D on pathogens related to bioterrorism and provide for accelerated research on adulteration of food under Federal Food Drug and Cosmetic Act.

H.R. 3448 does not include the antitrust exemption provisions for drug company R&D of S. 1765, nor does it include the provisions of S. 1765 relating to agriculture bioterrorism and some of food safety inspection authority. The House bill includes funding for water security technology not in the Senate bill. A conference is pending on the bills. These bills are the authorizing legislation that will guide the allocation of $2.5 billion for bioterrorism R&D that was include in the $20 billion energy spending package attached to the FY2002 defense spending bill (H.R. 3338) that was sent to the President for signature on December 20.

---

[118] *Congressional Record,* Nov. 15, 2001, pp. S11951-S11593.

S. 1747, introduced by Senators Harkin and Specter on November 28, 2001 also would allocate specific amounts of funding for bioterrorism R&D in P.L. 107-38. It would have authorized greater amounts of funding than the amounts allocated in the compromise version of H.R. 3338 that was enacted and sent to the President for signature on December 20, 2001.

In another authorization proposal, Rep. Chris Smith, chairman of the House Veterans' Affairs Committee, introduced H.R. 3253, the National Medical Emergency Preparedness Act of 2001, November 8, 2001, to establish a four new National Medical Preparedness Centers for R&D on radiological, chemical, and biological threats" R&D would be conducted by the Department of Veterans Affairs in cooperation with such other agencies as DOD and the Office of Homeland Security.[119] $20 million would be authorized for each fiscal year to 2006.

S. 1764, introduced by Senator Lieberman on December 4, would provide incentives to increase research by commercial, for-profit entities to develop vaccines, microbicides, diagnostic technologies, and other drugs to prevent and treat illnesses associated with a biological or chemical weapons. It would, among other things, expand the list of select agents regulated as bioterrorism threats requiring research registration, allow tax incentives for private groups to expand research on countermeasures for such agents, establish a "Bioterrorism Countermeasure Purchase Fund," in the Treasury Department to permit the CDC director to buy new counter terrorism products; extend patent terms and allow liability indemnification for certain privately developed countermeasures for certain biological or chemical agents or toxins; and authorize the NIH director to fund the construction of additional biosafety laboratories by grant or contact. It would authorize NIH Countermeasures Partnership Challenge Grants "to promote joint ventures between the NIH, its grantees, and for-profit biotechnology, pharmaceutical, and medical device industries for the development of countermeasures and research tools." It authorized $200 million for each of the next five years for the program.

Department of Agriculture. Additional funding for bioterrorism R&D for the Department of Agriculture would be authorized in S. 1546, introduced on October 15. It would provide the Secretary of Agriculture with about $101.2 million for biosecurity initiatives required under Presidential Directive (PDD-67) to secure resources at existing facilities of the Agricultural Research Service and the Animal Plant Health Inspection Service. Also, it would provide $177 million for research in support of bioterrorism response initiatives for each of the fiscal years for the ten-year period 2002 through 2011; and, for each of the fiscal years 2002 through 2011, it would provide $57 million annually to continue joint research initiatives between the Agricultural Research Service, universities and industry on counter-bioterrorism efforts. It would also make $25 million available for the same 10-year period for competitive grants to universities and qualified research institutions for research on

---

[119]See also, "Chairman Smith Proposes New National Medical Preparedness Centers Within VA," Press Release, House Committee on Veterans Affairs, Oct. 15, 2001 and Shirley Haley, "VA Centers for Medical R&D on Weapons of Mass Destruction Would be Established Under Smith Bill," *Washington Fax,* Oct. 24, 2001.

counter-bioterrorism. Some specifically earmarked R&D funds were also proposed to be authorized. The House version is H.R. 3174 introduced on October 25.

S. 1563, "to establish a coordinated program of science-based countermeasures to address the threats of agricultural bioterrorism," introduced October 17, 2001, would strengthen the U.S. R&D capacity to respond to an agricultural bioterrorism threat. It would expand the functions and funding of the Agricultural Research Service to protect the food supply with funding authorized at $140 million annually for fiscal years 2003 through 2007; create a consortium of higher education institutions to partner with federal agencies to address agricultural bioterrorism issues, funded at $50 million for each of the five fiscal years; authorize agricultural bioterrorism competitive research grants, funded at $30 million for each of the five years; expand the bioterrorism functions of, and increase the appropriations for, the Animal and Plant Health Inspection Service, and the Food Safety Inspection Service.

Multi-agency Bioterrorism R&D. S. 1486, the "Biological and Chemical Weapons Preparedness Act of 2001," introduced in the Senate on October 3, 2001, would, among other things, authorize funding for improving vaccine, antibiotics and therapeutic R&D, upgrade bioterrorism capacity in CDC, provide better training and strengthen the National Pharmaceutical Stockpile and other critical capacity building. These activities would be authorized $844 million for FY2002 and sums as necessary to 2006. In addition the bill would authorize additional R&D on biological and chemical terrorism in four agencies, the Departments of Energy, Justice, and Agriculture, and the Environmental Protection Agency; with appropriations of $10 million for each of the four agencies for FY2002 and such sums as necessary for each of the fiscal years in the five year period 2003 to 2006. The House version of this bill is H.R. 3242, introduced on November 7, 2001.

House Democrats formed a Democratic Homeland Security Task Force, which proposed H.R. 3255, "The Bioterrorism Protection Act (BioPAct) of 2001," introduced on November 8. Among other things, it would authorize for FY2002

> $509 million for research to develop and produce new and improved vaccines, therapeutics, and antibiotics to respond to chemical and biological agents that may be used in terrorist activities,
>
> $220 million for the Department of Agriculture to among other things increase vaccine research and production of high-threat animal pathogens, and
>
> $100 million for the Department of Defense R&D to accelerate technology development in chemical and biological research (prevention and treatment), advanced sensors, and other promising technologies, and
>
> $120 million for programs of cooperative R&D for Russian, Uzbek and Kazakh current and former biological weapons scientists and engineers to develop counter-measures to biological agents used as weapons or means of terror.

S.1560, the "Biological Agent-Environmental Detection Act of 2001," introduced October 17, 2001, would strengthen U.S. capabilities in environmental detection and the monitoring of biological agents. Among other things, it directs the Secretary of Health and Human Services to form an interagency task force (to include

representatives from industry) to encourage "non-duplicative" public-private research relating to environmental monitoring and detection tools with respect to biological (infectious) agents. It would authorize to the DHHS Secretary $13 million for FY2001 for cooperative agreements; $13 million for new technologies and to identify clandestine laboratories; and $14 million for the development of new detection technologies.

Information Security R&D

An executive order was issued that, among other things, requires coordination and priority-setting for information security R&D.

Options for Priority-setting. Numerous studies and witnesses in recent congressional hearings[120] have examined cyber security issues and made recommendations for specific R&D programs.[121] For instance, in 1997, the President's Commission on Critical Infrastructure Protection recommended expanded R&D in cyber defense, including "real-time detection, identification and response tools," and for more R&D relating to information assurance, intrusion monitoring and detection, vulnerability assessment and systems analysis, risk management decision support, mitigation, and incident response and recovery.[122] It also called for the establishment of new partnerships between government, industry, and academia to ensure a focused R&D program and for the National Research Council of the National Academy of Sciences to define more precisely the outline of an information security program.[123]

The Transition Office of the President's Commission on Critical Infrastructure Protection and Critical Infrastructure Assurance Office issued a report entitled, *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures,* July 1998. Like the previous 1997 report, it included recommendations in several areas: banking and finance, energy, information and communications, transportation, and vital human services. It focused on R&D requiring government investment and recommended research roadmaps for R&D that encompassed near-term, mid-term, and long-term time periods and divided research

---

[120]For instance, House Committee on Science, "Cyber Security—How Can We Protect American Computer Networks from Attack," Oct. 10, 2001, and "Cyber Terrorism – A View From the Gilmore Commission," Oct. 17, 2001; Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, "Cyber Security: Private-Sector Efforts Addressing Cyber Threats," Nov. 15, 2001; House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, "Computer Security in the Federal Government: How do the Agencies Rate?," Dec. 2001.

[121]See for instance, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 April 25, 2001.

[122]These recommendations are detailed in a separate report, *Research and Development: Recommendations for Protecting and Assuring Critical National Infrastructures, Report of the President's Commission Critical Infrastructure Protection,* 1997, 26 p.

[123]*Critical Foundations. Protecting America's Infrastructures.* pp. 89-90.

priorities into three categories – "most important," "very important," and "important." Estimates of funding resources needed to achieve each research goal were included. While information technology issues were relevant to all the sectors examined, the separate section on information and communications included in the "most important" category, the R&D topics of

- Vulnerability Detection and Analysis
- Characterization and Notification of Threats
- Intrusion and Incident Detection and Warning
- Response, Recovery and reconstitution,
- Security architectures,
- Assurance technologies, and
- Management of information protection.[124]

The Defense Science Board defined a slate of priorities for the Global Information Grid (GIG), a DOD information network system of "interconnected sensors and information systems," that uses DOD-unique software and system and commercial infrastructure. R&D, it said, was needed to develop new methods of "mobile code" to defend against attacks, and on forensics, tagging and trace back. It also called for "high leverage" R&D to maintain the Defense Information Infrastructure, including work on "scalable global access control, malicious code detection and mitigation, mobile code security, fault tolerance, integrity restoration, recovery and reconstitution." It recommended that DOD's R&D funding for these topics be increased by $40 million for FY2001 and $350 million over the next five years.[125]

The CSIS reported that the U.S. capability for combating cyber security threats could be improved if the government provided "direct financial incentives to universities to develop information security curricula, and to integrate information security not only into their current information science programs, but into their humanities and public policy courses as well."[126]

Options for Organization. It is difficult to coordinate R&D for cyber systems because many federal agencies support R&D which may be relevant to this area and systems applications largely are a private sector responsibility. Suggestions for an organizational format to determine R&D priorities vary from placing the responsibility in a new Office of Homeland Security to creating a new agency.

The CSIS focused on "threats emanating from the convergence of multiple technologies and sciences (e.g., information technology, nanotechnology, biotech,

---

[124]See pages 2-17 to 2-19.

[125]Defense Science Board. *Protecting the Homeland. Report of the Defense Science Board Task Force on Defensive Information Operations, 2000 Summer Study, Vol. II,* March 2001, pp. 12, 30. Detailed recommendations are in Chapter 3. "Technology," pp. 57-62.

[126]Frank Cilluffo, Joseph J. Collins, Arnaud de Borchgrave, Daniel Gouréé, Michael Horowitz, *Defending America in the 21st Century: New Challenges, New Organizations, and New Policies Executive Summary of Four CSIS Working Group Reports on Homeland Defense*, CSIS, pp. 23-24.

robotics, and microelectromechanical.)" It said government has failed to provide among other things, "...the necessary investments in research and defensive and offensive tools to fulfill national security objectives." CSIS concluded

> A clear delegation of authority or chain of command both in the prevention and remediation of cyber attacks remains lacking. There also is no clear-cut authority for dealing with the issue of national information infrastructure protection. Even though certain agencies such as Space Command and the National Infrastructure Protection Center (NIPC) have been assigned general duties, the parameters of their responsibilities are nebulous at best, and leave clear gaps in the defense of national assets.[127]

In testimony before the House Science Committee on October 16, Governor Jim Gilmore testified that the commission would recommend "Creation of an entity to develop and implement a comprehensive plan for research, development, test and evaluation of processes to enhance cyber security."[128] This recommendation, which was elaborated in a report released on October 31, said:

> We envision a government-funded consortium of not-for-profit entities with expertise in the field. The Institute for Security Technology Studies (ISTS) at Dartmouth College is providing resources to form the basis for establishing such an entity, including formal discussions with experts about the structure of such an organization; a comprehensive national needs assessment developed from a survey of stakeholders in government (Federal, State, and local), academia, and the private sector; and the development of a definitive near- and long-term agenda for RDT&E for cyber security. This is a significant first step toward establishing the type of entity we envision, and may be the logical nucleus around which the President could form such an entity.[129]

Policy Actions. Currently the federal R&D information technology program is coordinated at the interagency level by the Interagency Working Group (IWG) on Information Technology Research and Development (IT R&D) of the National Science and Technology Council (NSTC) and its Committee on Technology (CT). This interagency activity was authorized by the High Performance Computing Act of 1991 P. L. 102-194. The group also supports the President's Information Technology Advisory Committee (PITAC) composed of 22 industrial and academic members.[130] This group's responsibilities extend beyond information-security related

---

[127]Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, Michèèle M. Ledgerwood, *Cyber Threats and Information Security Meeting the 21st Century Challenge*, CSIS, pp. 23-24.

[128]"Governor Gilmore Gives Recommendations on Cyber Terrorism," October 17, 2001, from [www.house.gov/science].

[129]Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Third Annual Report to the President and the Congress, Advance Executive Summary, III. For Ray Downey,* Oct. 31, 2001, p. 16.

[130]It serves as the internal deliberative organization of the NSTC for IT R&D policy, program, and budget guidance and direction for the Executive Branch. It coordinates planning budgeting and assessment activities of the multi agency IT R&D enterprise. It is composed

(continued...)

issues. This R&D coordination activity is separate from the apparatus established by the government to deal with the information technology components of critical infrastructure protection.

During the last Administration, President Clinton issued Presidential Decision Directive 63 for Critical Infrastructure Protection largely directed to dealing with cyber attacks. In 1998, the Administration named Richard Clarke as National Coordinator for Security, Infrastructure Protection, and Counter-terrorism; and created a Critical Infrastructure Coordinating group (CICG), which had 13 subcommittees. Reporting responsibility was through the Assistant to the President for National Security and the Assistant to the President for Economic Affairs. One CICG subcommittee focused on R&D priorities, and was headed by OSTP. This subcommittee evolved into the Interagency Working Group on Critical Infrastructure Protection for Research and Development, abbreviated CIP R&D IWG. The working group was established under the National Science and Technology Council to coordinate multi-department, multi-agency R&D to develop technology to protect critical infrastructures and to accelerate the development of advanced technologies. The primary outcome of deliberations relating to information security protection R&D was to endorse creation of an Institute of Information Infrastructure Protection that had been proposed by the PCAST, with funding of $50 million for this purpose included in the President's FY 2001 budget. Funds were not appropriated for this institute.[131]

After the terrorist attack on September 11, the Bush Administration took steps to develop a capability to coordinate cyber security activities with the nation's counter terrorism effort and to better link information security R&D to these efforts. The mechanism established parallels with the organization created by the Clinton Administration. However, it differs in important ways and, potentially, has more authority, because it is closely linked to the anti-terrorism effort and to the OSTP, and

---

[130](...continued)
of agency representatives and staff from the OMB, OSTP, National Economic Council and staff of the National Coordination Office for IR R&D. - a 12 agency collaborative effort that reports to the OSTP and NSTC. (Information from the NSTC website.)

[131]John D. Moteff, "Critical Infrastructures: Background and Early Implementation of PDD-63," CRS report RL30153, June 19, 2001. The Institute program would have been an R&D "fund operated through the National Institute of Standards and Technology (NIST) to support research that might not otherwise be conducted by the private sector or defense agencies. Currently nearly all of the current information security research and development funds go to defense agencies. While operated through NIST, the Institute would report to a Federal Coordinating Council consisting of the President's Science Advisor, the Deputy Director/Office of Management and Budget, the Director/National Security Agency, the Director/NIST, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. The Institute would consult with the National Infrastructure Advisory Council and the Sector Coordinator" While this program was not funded, NIST established a Critical Infrastructure Protection Grants Programs, that awarded its first grants in October 2001 – 9 awards totaling $5 million – for R&D on computer and telecommunication systems security. NIST Awards Grants to Enhance Security of Infrastructure Networks," *Aerospace Daily*, Oct. 8, 2001, p.7.)

has specific authority to work with agencies to develop priority R&D programs and budgets.

In Executive Order 13231, October 16, 2001,[132] the President created "The President's Critical Infrastructure Board," charged with preventing disruptions of critical infrastructure and information networks in water, telecommunication, financial and transportation, health care and emergency services and manufacturing. Although it is directed to work closely with industry and State and local governments, it is composed wholly of executive agency officials, including the OSTP Director and 24 other agency heads and officials. It is chaired by the Special Advisor to the President for Cyberspace Security,[133] who will report both to the Assistant for National Security and the Assistant for Homeland Security. The Board was given responsibility "to recommend policies and coordinate programs...." With respect to R&D, the board is mandated to

> Coordinate with the Director of the Office of Science and Technology Policy (OSTP) on a program of Federal Government research and development for protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, and ensure coordination of government activities in this field with corporations, universities, Federally funded research centers, and national laboratories. In this function, the Board shall work in coordination with the National Science Foundation, the Defense Advanced Research Projects Agency, and with other departments and agencies, as appropriate.

The executive order established 10 standing committees, including one on Research and Development, chaired by a designee of the Director of OSTP. In addition to proposing plans for "subjects within its purview," and making recommendations to OMB on agency budgets "that fall within the Board's purview, after review of relevant program requirements and resources," the Board was given specific authority to "annually request the National Science Foundation, Department of Energy, Department of Transportation, Environmental Protection Agency, Department of Commerce, Departments of Defense, and the Intelligence Community .... to include in their budget requests to OMB funding for demonstration projects and research to support the Board's activities."

On October 9, President Bush named Richard Clarke, the Clinton Administration Critical Infrastructure coordinator, and considered to be an information security expert, to serve as his special advisor on cybersecurity and director of the President's Critical Infrastructure Board.[134] He was not specifically mentioned on the organizational chart as a member of the senior-level OHS Principals Committee, but

---

[132]Executive Order 13231, "Critical Infrastructure Protection in the Information Age," October 16, 2001,, 66 FR 53063 to 66 FR53071.

[133]"Bush Creates Cyber Terrorism Panel," *GovExec.com*, Daily Briefing, Oct. 17, 2001.

[134]"Fact Sheet on New Counter-Terrorism and Cyberspace Positions," White House Office of the Press Secretary, Oct. 9, 2001; "White House Bush Establishes New Positions For Fighting Terrorism, Cyberspace Security," *Daily Report for Executives*, Oct. 10, 2001, p. A-44.

he was listed among those who will attend meetings of the sub-Cabinet Deputies Committee if cyber security is discussed."[135]

Congressional Options. Computer security-related legislation that deals with R&D includes S. 1456, "Critical Infrastructure Information Security Act of 2001," introduced on September 2, which is intended to promote information sharing among government and industry to allay industry's fears that Freedom of Information Act (FOIA) requests could be used to disclose proprietary information in collaborative information security R&D projects; it would also allow companies to cooperate and share more information among themselves without fear of breaking antitrust laws. Hearings were held by the Senate Committee on Energy and Natural Resources. The companion House bill is H.R. 2435.

S. 1407 designates a primary research resource center for protecting cyber- and physical critical infrastructure systems. It would establish the National Infrastructure Simulation and Analysis Center as the core research and analytical facility to support the President's Critical Infrastructure Protection Board created via Executive Order. It would authorize $8 million through the Defense Threat Reduction Agency for the center to support policy decisions through modeling, simulation and analysis of the critical infrastructure systems. P.L. 107-56, the compromise anti-terrorism bill, signed on October 26, 2001, authorized appropriations of $20 million to the Defense Department for activities of the National Infrastructure Simulation and Analysis Center.[136]

H.R. 3316, the "Computer Security Enhancement and Research Act," introduced November 16, would fund a program of research and training to improve the security of networked information systems through the NIST in collaboration with academic and industrial researchers. This research program is authorized for a 10-year period, growing from $25 million in the first year to $85 million by the 5th year.

H.R. 3394, the "Cyber Security Research and Development Act," reported from the House Science Committee on December 6, 2001, would fund new research and other activities against cyber-terrorism. It would authorize $875 million over the next five years – with $568 million for NSF and the remainder for NIST for cybersecurity R&D. New NSF programs would include cybersecurity research centers, undergraduate program grants, and competitive fellowship grants. The bill also would create new NIST joint university/industry programs and new NIST fellowships to attract more researchers to the field of computer and network.

---

[135]Bar Vaida, Cybersecurity Adviser Gets Second-tier Role in Homeland Defense," *GovExec.com,* Oct. 31, 2001.

[136]For a summary of related legislation see Derrick Cain, "Cyberattack Fears Prompt Flurry of actions: Legislation, Hearings, Study, Executive Order," *Daily Report for Executives*, Oct. 19, 2001, p. A-34.

National Academy of Sciences

Several professional associations and groups have developed special programs to synthesize information related to their field and to inform their membership about federal government counter terrorism R&D activities and needs.[137] The National Academy of Sciences and its related organizations have been among the most active. Several months before the September 11, 2001 attack, the Hart-Rudman Commission recommended that "All four parts of the National Academies of Sciences should play key roles in bringing the most knowledgeable scientists and engineers in contact with members of the Legislative branch" to provide direct advice and continuous dialogue on countering terrorism.[138] Subsequently, on September 20, 2001 the three National Academies' Presidents (for the National Academy of Sciences (NAS), the Institute of Medicine (IOM), and the National Academy of 'Engineering (NAE) sent a letter to President Bush offering "advice and counsel...." The Academies would convene small groups of senior national experts – both security specialists and scientists – to meet privately to explore the new dimensions of terrorism and to "propose ways to marshal the enormous intellectual capacity of the scientific and technological communities ...to respond to our new threats."

Lewis Branscomb, a Harvard University professor and former Director of the National Bureau of Standards, chief scientist at IBM, and National Science Board chairman, and Richard Klauser, former Director of the National Cancer Institute and president of the newly created Case Institute of Health, Science and Technology, in Washington, D.C. were named as co-chairs of the Academies' work[139] in the Committee on the Science and Technology Agenda for Countering Terrorism. The 22-member committee consists of eminent research professionals.[140] Subsequently, Dr. Klauser was also named senior fellow and special adviser to the presidents for counter terrorism at the National Academies, to serve as the liaison between the director of the White House Office of Science and Technology Policy and the new counter terrorism efforts of the Academies – helping to coordinate these activities with those of the government.[141]

The Academies' effort has several parts. The long-range activity will be conducted by committees within the National Research Council that perform contracted studies for federal agencies. Under Phase I of the project, the group will form panels on biological; chemical; nuclear and radiological threats; information technology, computers, and telecommunications; transportation; energy facilities,

---

[137]For instance, the American Association for the Advancement of Science held a symposium on "The War on Terrorism: What Does It Mean for Science?," on December 18, 2001. [http://www.aaas.org/news/terrorismsymposium.html].

[138]Hart-Rudman report, p. 114.

[139]David Malakoff and Robert Koenig, "Counterterrorism: U.S. Science Agencies Begin to Lend a Hand," *Science*, Oct. 26, 2001, pp. 761-762.

[140]NAS, "Committee on Science and Technology for Countering Terrorism," Dec. 3, 2001.

[141]"Klauser Accepts Position as National Academies' Adviser on Counter terrorism," *National Academies News*, Dec. 19, 2001.

buildings and fixed infrastructure; and behavioral, social and institutional issues. The committee will characterize the threat for each area, develop research agendas, examine cross-cutting multi disciplinary research topics for these "domains," and conduct short term studies or provide consultations and advice.[142] A research agenda for each of the seven target areas is to be produced by May 2002. The second phase will be a report that will focus on the organization of federal R&D agencies for counter terrorism. This report is expected by September 2002.[143] In addition the National Research Council will develop studies on counter terrorism R&D in specific areas, some of these for federal agencies. Among the studies planned or underway are those relating to cyber security, issues affecting universities, agricultural bioterrorism, transportation security, water supply protection, chemistry and national security.[144] The academies also plan cooperative work with counterpart foreign National Academies of Science. The NAS is also exploring additional ways to interact with industry to identify specific vulnerabilities and critical infrastructure needs. The Academies plan to assist agencies by convening groups of experts to advise agencies through meetings or written reports. Funding sources will include: foundations, the NAS's own endowment, (reportedly it has used $2 million of its endowment to start activities),[145] and contract funds from specific agencies which seek information about particular technologies or topics.

Several months before the attack, the National Academy of Engineering said it would "mount a study of 'homeland defense' against terrorism." Reportedly, the study would now move ahead according to William Wulf, President of the National Academy of Engineering.[146] The Academies also made available on their website the text of 25 publications about the science and policy issues surrounding terrorism and security. This includes titles such as: *Airline Passenger Security Screening: New Technologies and Implementation Issues,* 1996, and *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response,* 1999.[147]

P.L. 105-153 declared that the National Academy of Sciences was not subject to Federal Advisory Committee regulations. But the law opened up the Academy meeting/report writing process to the public. It required the Academy to announce

---

[142]"Klauser Accepts Position as National Academies' Adviser on Counter terrorism," *National Academies News,* Dec. 19, 2001 and information about Project Number DEPS-L-01-02-A. Reportedly the Academies have been advising the CIA and the FBI on specific issues and are convening export panels to generate real-time advice and quick studies. (AAU, *CFR Weekly Wrap-Up,* Nov. 21, 2001.

[143]Wil Lepkowski, "The Academies and the World," *Science and Policy Perspectives,* Dec. 11, 2001; Wil Lepkowski, "Science Mobilizes," *Science and Policy Perspectives,* Nov. 5, 2001, [http://www.cspo.org/s&pp/110501.html]. See also, William J. Broad, "Government Reviving Ties to Scientists," *New York Times,* Nov. 20, 2001.

[144]Wil Lepkowski, "Addition: Academies Detail War Plan," *Science and Policy Perspectives,* Jan. 3, 2002.

[145]Lepkowski.

[146]Science Scope, *Science,* Sept. 21, 2001.

[147]The inventory of text searchable publications is at [http://nap.edu/terror/index.html].

meetings; to make publicly available summaries of closed session meetings; to hold open meetings that are focused on gathering information, unless the meeting deals with internal Academy matters, is comprised wholly of Academy officials agents or employees (i.e., when deliberating about report conclusions and personnel issues), the material discussed is classified, or the material is exempt from disclosure as specified in FOIA regulations. As a result, the Academy may find it difficult to close meetings that discuss sensitive scientific and technical information that does not fall within these parameters, even if the topic is counter terrorism.

Policy Options for Priority-setting and Coordination

Debates about R&D priority-setting and coordination reflect fundamental tensions of the balance between centralization and decentralization in decision making and program implementation. These tensions are reflected in the arrangements that are evolving for planning and coordinating counter terrorism R&D policy and programs. Two levels of counter terrorism R&D coordination have emerged since the terrorist attacks of September 1. One is at the interagency R&D policy-making level, and the other is at the programmatic level for specific functional areas of R&D.

Interagency Coordination at the Policymaking Level

Options for coordinating counter terrorism R&D priority-setting and programs at the interagency policymaking level focus primarily on the Office of Science and Technology Policy, the Office of Homeland Security, and the National Security Council. It is not readily apparent that any of the mechanisms developed so far meet all the objectives outlined in the above cited reports that criticized the absence of effective priority-setting and coordination mechanisms. However, mechanisms are evolving. The Administration did not identify counter terrorism R&D as a major function of the Office of Homeland Security, but established an interagency Homeland Security Council Policy Coordination Committee (HSC PCC) on Research and Development. At this point, little is known about functions of the committee, except that it will focus on interagency coordination. It is to be directed by an OHS staff member. However, the OSTP Director said that his office has temporarily assumed the R&D function for OHS and advises the OHS on scientific and technical issues. The NSTC, which is managed by the OSTP, is creating five working groups to deal with counter terrorism issues. In addition, OSTP was tasked formally to work with the OHS on specific projects – technology for immigration and policy for foreign student entry and course surveillance. In contrast, pursuant to the executive order that was issued relating to information systems protection, the OSTP Director was given lead responsibility to work with agencies to coordinate cyber security R&D.

Coordination of homeland counter terrorism R&D by the OHS offers the advantages of linking R&D priorities directly to the President's policy to deal with terrorism, and allows the President to use an organization he created – and one that

is not now subject to direct congressional oversight – to achieve his objectives.[148] Since the OHS has no budget authority, the extent of R&D coordination that will be undertaken by the HSC PCC is uncertain. Notwithstanding the advantages of a White House office created by executive order, there is no guarantee that such an office will foster the kinds of cooperative relationships among agencies that are specified in organization charts because cooperation often depends upon personalities, leadership, and the amount of collaboration and sharing department and agency heads view as appropriate. The White House may view OSTP's filling this role on an informal basis and "for the time being" as the most appropriate way to provide appropriate collaboration.

Legislation has been introduced to statutorily authorize a homeland security agency with specific responsibilities to coordinate R&D, as was recommended in several authoritative commission reports. While such an agency could provide Congress with the program and policy oversight some believe is desirable, there are complications. Congressional authorization and appropriations jurisdiction for R&D are shared among several different committees and subcommittees, making centralized administration of funding difficult.[149] Also some analysts have noted that because the agency and its director would be authorized by Congress, the President might not have as much confidence in the office as he does in the OHS, which is wholly within the Executive Office of the of the President, whose "head" is not confirmed by the Senate, and whose activities are not closely overseen by the Legislature. At present, the President's Assistant for National Security, who is "supervisory officer" of the National Security Council,[150] and the Assistant to the President for Homeland Security, who heads the OHS, have been given more responsibility, at least publicly, for aspects of counter terrorism R&D policy making than the OSTP Director, whose office is subject to greater congressional control even though it is within the EXOP.[151] (OSTP is statutorily authorized and the OSTP Director is confirmed and required to testify before Congress.)

There is continuing uncertainty about whether the National Security Council's role should be limited to traditional defense/foreign policy issues or should be

---

[148]It is possible that a weak link with Congress could be detrimental to the OHS receiving congressional support. See Moe, op. cit.

[149]On this point see: William C. Boesman, *A Department of Science and Technology: a Recurring Theme*, CRS Report 95-235 SPR, Feb. 3, 1995. 6 p.

[150]Best, op. cit., p. 10.

[151]Neither the Director of the OHS, who has been named Assistant to the President for Homeland Security nor the Assistant to the President for National Security are confirmed by the Senate; the OSTP Director is required to be confirmed by the Senate and the Senate receives testimony about OSTP's activities. . Furthermore "Congress annually appropriates funds for...[NSC's] activities, but does not, routinely, receive testimony on substantive matters from the National Security Adviser or from NSC staff. Proposals to require Senate confirmation of the Security Adviser have been discussed but not adopted."(Richard A. Best, Jr., *The National Security Council: An Organizational Assessment*, CRS Report RL30840, February 9, 2001, 42 p.)

broadened to include "homeland defense" issues.[152] As a result, there is a potential for overlap between the NCS and OHS in dealing with priority-setting and coordination for counter terrorism R&D. There may be a need to link the coordination activities handled by the NSC PWMD R&D Subgroup and the HSC PCC on R&D. OSTP chairs the NSC subgroup but it was not given specific membership or responsibilities on the HSC PCC on R&D.

So far the President has not given OSTP, at least publicly, a major role in defining counter terrorism R&D policy, but its role is evolving. Further definition of OSTP's responsibility could develop over time as the President and the OSTP Director work together more closely and as the OSTP Director gains the confidence of the President and the Assistant to the President for Homeland Security. OSTP has a history of effective coordination in some functional R&D program areas (especially for interagency programs that have been designated as Presidential initiatives or for which Congress enacted legislation mandating R&D coordination, notably global change and information technology development). OSTP also has well-established relationships with other federal agencies, the scientific community, academia, and the National Academy of Sciences, and it has its own nongovernmental advisory body, PCAST, and its own FFRDC to conduct policy analysis. The OSTP Director's proposed establishment within NSTC of an Interagency Antiterrorism Task Force with working groups in specific functional areas will probably give more definition to OSTP's coordination functions. However, the reported termination of the OSTP's national security division has raised questions about OSTP's potential to work effectively in this area.

Federal policies for counter terrorism R&D are likely to address several cross-cutting issues, which typically have been handled at the OSTP level. These include:

- Compiling an inventory of federal agency R&D on counter terrorism that clarifies discrepancies in existing inventories. It should describe what is being funded, using not only customary reporting categories of R&D by field of science or the "goal" categories in OMB's counter terrorism funding report, but also present data categorized according to interagency functional R&D areas, such as bioterrorism, cyber security and decontamination. These data can then be used for priority-setting at the interagency level by identifying areas of duplication and gaps for short- and long-term counter terrorism R&D.

- Ensuring that there is adequate financial support for traditional fields of R&D which enrich the knowledge base generally and which support U.S. science infrastructure and science and engineering education programs in order to sustain national security. (The electron beam x-ray devices being used now to scan mail derive from basic physics research.) This could become a controversial issue since OMB director Mitch Daniels has announced the possibility that

---

[152]In summary, "Some argue that the NSC should be broadened to reflect an expanding role of economic, environmental, and demographic issues in national security policymaking. The Clinton Administration created a National Economic Council tasked with cooperating closely with the NSC on international economic matters, but the contours of the relationship between the two Councils could change in the George W. Bush Administration. The increasing overlap between national security and law enforcement issues provide new challenges to the NSC as do efforts to coordinate the protection of critical infrastructures from cyberattacks by terrorists. On the other hand, some observers believe that traditional defense and foreign policy issues must continue to be the focus of the NSC's efforts." (Best, op. cit., Summary.)

budgets for activities that do not contribute to the effort to combat terrorism will be reduced.[153]

- Mitigating the possibly negative effects on the conduct of R&D from recent actions taken to ensure the security of sensitive U.S. scientific and technical information. These actions include terminating public access to some federal science agency websites and laboratories; closing laboratory campuses and facilities to certain persons; prohibiting access to certain potentially toxic biological materials by certain aliens, criminals, mentally ill persons, dishonorably discharged persons, and so forth; and prohibiting some foreign students from studying sensitive subjects.

- Ensuring that creative, risky kinds of R&D and new working relationships among government, industry, and academia,[154] are supported and that non-traditional kinds of funding mechanisms can be used to provide the government with "out of the box", rapid turn- around research, and even off-the-shelf technology (which is especially important to DOD).[155] This might include endorsing R&D funding or awards approval processes that do not necessarily utilize traditional peer review, which, some say, can disadvantage creative risky R&D. Such mechanisms include the NSF Small Grants for Exploratory Research Program[156] and the NIH Director's Discretionary Fund. Another illustrative mechanism is the October 23 DOD'S TSWG issuance of a broad agency announcement (BAA) request – a special method DOD uses to place a contract to procure information or technology rapidly and with less red tape

---

[153]Glenn Keller, "OMB Chief Signals New Spending Goals," *Washington Post,* Oct. 17, 2001, p.A3; Nancy Ognanovich, "U.S. Budget, OMB's Daniels Mulls Spending Freeze, Other Restraints to Rein in Lawmakers," *Daily Report for Executives,* Oct. 19, 2001, p. A-20.

[154]On November 6, 2001, the Association of American Universities (AAU) president wrote to Government Tom Ridge offering the assistance and expertise of the 61 member AAU research universities in meeting the nation's terrorism challenge. "Our campuses have wide-ranging expertise in area such as language and culture, engineering and technology, aerospace and bioterrorism and political science and economics. ...We want to ...make you aware that we can serve as a conduit through which you and your staff would be able 6to seek our experts in a wide variety of fields." [Http://www.aau.edu/publicatons/ wrapup11.9.01.html.]

[155]The importance of procuring or adapting commercial off-the-shelf technologies for security/defense-related needs was underscored in DOD's *Quadrennial Defense Review Report,* issued on September 30, 2001, which stated: "During the Cold War, U.S. government programs were a primary impetus for research into new technologies, particularly in areas such as computers and materials. Today and well into the foreseeable future, however, DOD will rely on the private sector to provide much of the leadership in developing new technologies. Thus, the Department has embarked on an effort (a) to turn to private enterprise for new ways to move ideas from the laboratory to the operating forces, (b) to tap the results of innovations developed in the private sector, and (c) to blend government and private research where appropriate. This 'quiet revolution' will take advantage of science and technology and continue to private U.S. forces with technological superiority." (Quoted in Richard M. Jones, "DOD Report Calls for 3% Investment in S&T," *FYI: The AIP Bulletin of Science Policy News,* No. 130, Oct. 18, 2001)

[156]NSF, "At WTC Site, New Federal Grants to Study Structural Engineering and Hazard Response," NSF Media Advisory, PA/M 01-36, Sept. 28, 2001; and "Post-Attack Grants to Study Human, Social Responses to September 11 Crisis," PA/M 01-38, Oct. 5, 2001.

than is typical.[157] This BAA announced to researchers and inventors that DOD was seeking information to develop 38 specific counter terrorism technologies for military, intelligence, and security operations that can be deployed within the rapid time frame of 12 to 18 months.[158]

- Working with the private sector to ensure development of appropriate security-related products and technologies that have not yet been marketed for lack of capital, demand, or regulatory barriers. Consideration is required to assess the pros and cons of industrial concerns about changing federal regulations to deal with the production of technology that could violate constitutional guarantees of privacy; the release of propriety information for cooperative work that does not meet the tests for exemption to Freedom of Information Act (FOIA) requests; concerns about violating antitrust regulations if companies work too closely together to develop security-related products; inadequate technology transfer and sharing of information; allegedly slow certification procedures for some technology, especially FAA security devices and some drugs;[159] and the requirements for incentives or tax credits for producing terror resistant technologies.[160]

Coordination at the Functional Program Level

Bioterrorism and cyber security R&D as discussed above, are two examples of coordination at the functional program level. Expert reports have criticized the informal efforts that agencies took in the past to coordinate counter terrorism R&D

---

[157]"Each proposal will be evaluated on the merit and relevance of the specific proposal as it relates to the TSWG program rather than against other proposals for research in the same general area." (Under Secretary of Defense for Acquisition, Technology and Logistics and Combating Terrorism Technology Support Office , Technical Support Working Group, *Broad Agency Announcement BAA 02-Q-4655,* October 23, 2001, p. 16.

[158] According to one news report, "Officials ...said it was an attempt to find a new way of doing business in a time of urgent need." Commercial versions already exist for some of the requested technologies and some industrial officials said "...many of the systems the Pentagon wants have been in development for years but until now have suffered from a lack of funding and attention. (Greg Schneider and Robert O'Hare,"Pentagon Makes Rush Order for Anti-Terror Technology," *Washington Post,* October 26, 2001, p. A10.) Among the technologies and systems DOD seeks are an automated system to use voice prints to locate and track terrorist suspects; a speaker recognition system to identify Middle Eastern and Central/South Asian languages in speech; technoloy that enables authorities to identify faces in a crowd; methods to track human movement by video image in uncontrolled lighting environments; a data base of patterns, trends and models of behavior of terrorist groups and individuals; a system to detect, locate, and map underground and concealed activities that may serve as secure havens for terrorists; early warning devices or remote sensors to alert tactical forces of the near presence of non-friendly personnel; through-wall imaging capability technologies; methodology to determine if terrorists have worked with weapons of mass destruction; a system to detect chemical, biological warfare agents and selected toxic industrial chemicals before release in a terrorist attack; products to rapidly and expediently neutralize suspect chemical or biological agents in battlefield situations; a battery-powered device to analyze liquid samples for the presence of biological warfare agents; and walkthrough portals for nonstationary personnel screening. (BAA 02-Q-4655, pp. 17-23.)

[159]William Triplett, "Technology Will Assist the Fight Against Terrorism," *Nature,* Sept. 20, 2001.

[160]CSIS, *Cyber Threats and Information Security Meeting the 21st Century Challenge,* p. 39.

in these areas. More formal approaches have been adopted in these two fields since September 11, but they differ significantly.

Federal R&D typically has been coordinated through the formation of interagency groups attached in one way or another to the NSTC. NSTC's coordination activities have involved activities as diverse as infectious diseases, nanotechnology, and children's education. Coordination at this level necessitates that participating agencies develop strategies to achieve broader Administration goals, that they identify priorities for R&D, and determine which specific agencies will implement the various program tasks. Agencies participating in the effort need to budget resources to meet the objectives of the interagency program, possibly conflicting with bureaucratic tendencies to maintain control to achieve agency goals. Formal interagency mechanisms may be required to ensure cooperation in the national interest. So far, it appears that the Administration has chosen not to use the NSTC to coordinate interagency bioterrorism and information security R&D.

The federal structure to coordinate bioterrorism R&D does not appear to be as fully and formally developed as the structure to coordinate information security R&D. It has been recommended that interagency bioterrorism R&D mechanisms be strengthened to inventory R&D funding and programs; set priorities; eliminate duplication; and develop policy for effective collaboration with industry, professional groups, academia and federal laboratories. The two agencies with the largest bioterrorism programs, DHHS and DOD, have internal structures to coordinate R&D within each department. Coordination between these two agencies and among them and the others that support work in this field, including the Department of Agriculture and Department of Energy, seems to occur informally on a consultative basis. A formal coordination mechanism like that used for information security R&D has been suggested. However, such a mechanism may be difficult to establish and implement given the size of DOD's and DHHS's bioterrorism R&D programs and the power and prerogatives of each agency. Attention could be given to dealing with bioterrorism at the NSTC level or by creation of a Special Advisor to the President for Bioterrorism like the Special Advisor to the President for Cyberspace Security. Proposals have been made to mandate interagency coordination in bioterrorism R&D, to increase funding in several agencies, and to create a laboratory for bioterrorism R&D and vaccine production. When considering these options, Congress could assess which priority-setting and coordination mechanisms are best suited to ensure efficient and effective R&D.

Coordination of information security R&D has been formalized within the office of the Special Advisor to the President for Cyberspace Security and the President's Critical Infrastructure Board, which was also given some authority to require agencies to allocate budget resources to priority R&D topics that serve the board's agenda. This model of cooperation clearly is different from the informal coordination mechanisms used for bioterrorism R&D. The need to collaborate closely with industry in information security R&D and other aspects of infrastructure protection may have motivated creation of a separate interagency coordination mechanism. It remains to be determined whether this mechanism will be able to identify R&D priorities and compel agencies to allocate budgetary resources for projects to meet the board's requirements.

Conclusion

Counter terrorism R&D programs, policies, and coordination mechanisms are still developing. Interagency issues that Congress may wish to consider include

- Tensions between centralization and decentralization of decisionmaking for R&D programs and policies,
- Pros and cons of coordinating R&D in an office established by Congress and subject to more congressional oversight or in an office that reports exclusively to the President,
- Linkage between coordinating policies for counter terrorism R&D handled by the National Security Council and by the Office of Homeland Security,
- Improvement in the quality of information about the nation's counter terrorism R&D programs and funding levels,
- Importance of linking counter terrorism R&D policy making to policies for R&D more broadly,
- Need to ensure efficient expenditure of R&D funds for counter terrorism priorities, and
- Whether a formally constituted coordination body is required and feasible for specific functional areas.

APPENDIX 1, Administration's Goals for Counter Terrorism for Weapons of Mass Destruction

1. The Administration's counter terrorism for WMD R&D goals are:[161]

1. WMD-Related Basic Research and Enabling Capacity
Goals: Expand the knowledge base in areas relevant to preparedness for terrorist WMD incidents. Fundamental research is essential for building the knowledge base to enable developments for meeting a broad range of increasingly complex needs to prevent, counter, or respond to nuclear, radiological, chemical and biological terrorism.

2. Personal and Collective Protection and Device Disposition
Goals for Protection: Make available personal and collective protective equipment, vehicles, and shelters for first responders that permits them to fully perform their mission with an adequate margin of safety, and in a timely manner, at a scene contaminated with chemical, biological, radiological, or nuclear (CBRN) agents. Make available personal protective equipment for victims that adequately assures their safety until the hazard dissipates or until evacuation. Make available ventilation systems for buildings that detect, neutralize or screen out dangerous CBRN agents.

3. Detection and Measurement of WMD Agents
Goals: Develop rapid, accurate diagnostic tools that can confirm exposure—or nonexposure—to WMD agents. Tools should also identify the agent, in order to facilitate treatment and to feed into warning and epidemiological investigation systems. Ensure that personnel responding to, managing, or investigating a contaminated scene can sufficiently detect, characterize, and delimit the extent of hazardous materials in the environment. Develop systems to continuously monitor specific facilities or areas for WMD threats. Develop a routine mechanism for credible and authoritative testing, evaluation, and certification of detection equipment. Develop means for nonintrusive or remote detection of WMD agents within containers or packages, or in transit. A goal specific to bioterrorism is to develop techniques for rapidly identifying components and virulence factors in engineered organisms and for rapidly determining the agent's drug or countermeasure sensitivity. Develop knowledge of existing naturally occurring pathogens, their distribution, and environmental factors affecting their population .

4. Personal and Environmental Decontamination
Goals: Improve knowledge and effective methods of personnel and property decontamination. Develop decontamination solutions or processes that are effective for a wide range of chemical and/or biological agents, environmentally safe, transportable, and simple to use. Develop noncorrosive, non-water-based decontamination materials or processes for sensitive equipment and hard-to-reach interior surfaces. Develop area environmental decontamination materials that can recover use of wide areas contaminated by agents thought to persist in the environment. Develop criteria for "how clean is clean" that can be established and defended by policymakers. Understand the effects of low-level exposure, develop effective decontamination techniques, and develop adequate instrumentation to verify the effectiveness of decontamination.

---

[161]OMB, *Annual Report to Congress on Combating Terrorism*, FY2001, Part 4.

5. Vaccines, Therapeutics, and Treatments, including Psychological Effects
Goals for Vaccines, Therapeutics, and Treatments: Ensure a sufficient set of therapeutic substances and devices (e.g., autoinjectors) to treat individuals subjected to an attack from rapidly acting chemical agents. Develop therapies for known pathogens – particularly viruses and drug-resistant microbes–that have significant potential for use as bioweapons. Develop broad-spectrum therapies, pretreatments, or countermeasures that can address the wide range of potential threat agents or the possibility that a bioengineered agent might act in novel ways. For particular high threat diseases such as anthrax and plague, develop vaccines that are suitable for post-exposure treatment of exposed or at-risk populations. Ensure capability to produce and rapidly distribute vaccines that would be needed to mitigate the spread of either known, novel or bioengineered infectious agents.

6. Information Systems, Modeling, Simulation, and Analyses
Goals: Develop tools and assessment methodologies for generating realistic threat scenarios, performing vulnerability assessments and evaluating potential response architectures, including assets and operations. Develop modeling tools to support managers' situational awareness and to allow them to make timely decisions. Develop tools and methodologies for identifying gaps in prevention, response or consequence management, and predicting the full impact of an incident.

APPENDIX 2, Table on Research and Development Funding by Category as a Subset of Federal Funding to Combat Terrorism, Including Defense Against Weapons of Mass Destruction, FY1998-2001, by Monterey Institute of International Studies

Research and Development Funding by Category as a Subset of Federal Funding to Combat Terrorism, Including Defense Against Weapons of Mass Destruction, FY1998-2001, by Monterey Institute of International Studies, 2000, (Millions of Dollars)[162]				
ALL GOVERNMENT BY CATEGORY	**FY1998**	**FY1999**	**FY2000**	**FY2001 (requested)**
Research and Development	$403.1	$527.0	$727.9	$812.8
WMD figure for the above category	$239.8	$368.8	$537.0	$589.9
- Basic Research, including Gene Sequencing	$70.5	$31.0	$48.0	$92.3
- Detection/Diagnostics	$17.8	$59.0	$78.3	$97.0
- Modeling, Simulation, Systems Analyses	$3.6	$10.6	$16.7	$16.7
- Personal/Collective Protection	$12.0	$10.0	$30.0	$28.2
- Personal/Environmental Decontamination	$1.8	$9.3	$20.3	$24.2
- Therapeutics/Treatments	$0.0	$16.0	$20.9	$26.6
- Vaccines	$2.9	$35.7	$82.6	$99.2
- Other	$131.2	$197.2	$240.3	$205.8

[162]Excerpted from information in Monterey Institute of International Studies, *Federal Funding to Combat Terrorism, Including Defense Against Weapons of Mass Destruction, FY1998-2001*, 2000. Source: http://cns.miis.edu/research/cbw/terfund.htm/. "Unless otherwise noted, all figures are taken from: Executive Office of the President, Office of Management and Budget. *Annual Report to Congress on Combating Terrorism*. Pursuant to FY 1998 National Defense Authorization Act (Public Law 105-85) May 18, 2000, p. 47-51, 58-65."

APPENDIX 3, Table on Research and Development Funding by Agency and Category as a Subset of Federal Funding to Combat Terrorism, Including Defense Against Weapons of Mass Destruction, FY1998-2001, by Agency and Category, by Monterey Institute of International Studies, 2000

Research and Development Funding by Agency and Category as a Subset of Federal Funding to Combat Terrorism, Including Defense Against Weapons of Mass Destruction, FY1998-2001, by Monterey Institute of International Studies, 2000, (Millions of Dollars)[163]				
BY AGENCY & CATEGORY	**FY1998**	**FY1999**	**FY2000**	**FY2001 (Requested)**
Department of Agriculture				
Research and Development	$5.2	$6.7	$6.7	$29.2
WMD figure for the above category	$5.2	$6.7	$6.7	$29.2
- Basic Research, including Gene Sequencing	$0.0	$0.0	$0.0	$10.0
- Other	$5.2	$6.7	$6.7	$19.2
Laboratory Infrastructure Improvements				$19.2[164]
Department of Commerce				
Research and Development	$12.1	$10.5	$10.5	$10.5

[163]Excerpted from information in Monterey Institute of International Studies, *Federal Funding to Combat Terrorism, Including Defense Against Weapons of Mass Destruction, FY1998-2001,* 2000. Source: http://cns.miis.edu/research/cbw/terfund.htm. "Unless otherwise noted, all figures are taken from: Executive Office of the President, Office of Management and Budget. *Annual Report to Congress on Combating Terrorism.* Pursuant to FY 1998 National Defense Authorization Act (Public Law 105-85) May 18, 2000, p. 47-51, 58-65.

[164]According to Monterey Institute: *Annual Report to Congress on Combating Terrorism,* May 18, 2000, p. 22.

WMD figure for the above category: Basic Research, including Gene Sequencing	$10.0	$9.0	$9.0	$9.0
Department of Energy				
Research and Development	$12.1	$10.5	$10.5	$10.5
WMD figure for the above category: Basic Research, including Gene Sequencing	$10.0	$9.0	$9.0	$9.0
Dept of Health & Human Services				
Research and Development	$15.9	$34.9	$112.0	$91.7
WMD figure for the above category	$15.9	$34.9	$112.0	$91.7
- Basic Research, including Gene Sequencing (NIH)	$13.0	$17.2	$21.8	$21.8
- Detection/Diagnostics	$0.0	$5.7	$5.7	$8.3
Rapid Toxic Screen (CDC)			$5.0[165]	
- Personal/Collective Protection	$0.0	$0.0	$0.0	$1.2
- Therapeutics/Treatments	$0.0	$4.0	$4.4	$4.4
- Vaccines	$2.9	$6.1	$48.5	$56.2
New vaccines for Smallpox and Anthrax			$30.0[166]	
· Development and production of tissue culture smallpox vaccine (CDC)			$22.5	

[165] According to the Monterey Institute: "Johns Hopkins University-Center for Civilian Biodefense Studies. "Department of Health and Human Services FY2000 Anti-Terrorism Funding" (Abstracted from DHHS Summary Document). *Biodefense Quarterly*, March 2000, Volume 1, Number 4. [http://www.hopkins-biodefense.org/pages/news/quarter.html]. Develop in-house capability to test 200 blood and urine samples per day for 150 toxicants."

[166] According to the Monterey Institute: "Department of Health and Human Services FY2000 Anti-Terrorism Funding." This source applies to all figures under this item.

· Expedited review, approval of new vaccines (FDA)			$7.5	
- Other	$0.0	$1.9	$31.7	$0.0
Evaluation of State of Readiness of Medical Care System (AHRQ)			$5.0[167]	
· Research on early detection (3 grants)			$3.0	
· Priority areas			$1.0	
· Assessing capacity			$0.5	
· Literature reviews			$0.5	
Independent Studies (Carnegie Mellon, St. Louis Univ., Univ. of Texas-Galveston, Noble Hospital-Ft. McClellan, Johns Hopkins)			$4.7[168]	
Department of Justice				
Research and Development	$27.0	$16.9	$36.9	$30.5
WMD figure for the above category	$15.0	$12.7	$32.7	$20.9
- Detection/Diagnostics	$3.0	$2.7	$2.7	$3.9
- Personal/Collective Protection	$12.0	$10.0	$30.0	$17.0
Technology and Standards Development				$17.0[169]
Federal Bureau of Investigation (...part of above DOJ funding figures)				

[167]According to the Monterey Institute: "Department of Health and Human Services FY2000 Anti-Terrorism Funding." This source applies to all figures under this item."

[168]According to the Monterey Institute: "Department of Health and Human Services FY2000 Anti-Terrorism Funding."

[169]According to the Monterey Institute: *Annual Report to Congress on Combating Terrorism.* May 18, 2000, p. 30.

Research and Development	$4.4[170]			
National Security Community				
Research and Development	$271.0	$322.0	$422.5	$502.7
WMD figure for the above category	$170.8	$230.8	$293.9	$347.0
- Basic Research, including Gene Sequencing	$44.5	$0.0	$6.3	$37.5
- Detection/Diagnostics	$0.3	$34.1	$48.5	$62.3
- Modeling, Simulation, Systems Analyses	$0.0	$8.6	$10.0	$10.0
- Personal/Collective Protection	$0.0	$0.0	$0.0	$10.0
- Personal & Environmental Decontamination	$0.0	$6.5	$17.1	$21.0
- Therapies/Treatments	$0.0	$12.0	$16.5	$22.2
- Vaccines	$0.0	$29.6	$34.1	$43.0
- Other	$126.0	$140.0	$161.5	$141.0
Department of State				
Research and Development	$2.0	$8.0	$2.0	$2.0
WMD figure for the above category	$0.0	$1.0	$0.0	$0.0
Department of Transportation				
Research and Development	$44.6	$51.8	$50.6	$49.7

[170]According to the Monterey Institute: "U.S. General Accounting Office. *Combating Terrorism: FBI's Use of Federal Funds for Counter terrorism-Related Activities (FY 1995-98)*. Report to the Chairman, Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, U.S. Senate, November 1998, p. 45. Some and/or all of the money allocated to the FBI may already be included in the DOD figures."

WMD figure for the above category: Detection/Diagnostics	$0.0	$0.0	$0.5	$0.0
Department of the Treasury				
Research and Development	$0.7	$0.8	$2.7	$2.

APPENDIX 4, Other Recommendations to Strengthen U.S. Science and Technology Infrastructure to Deal With National Security Threats, Made Primarily by the Hart-Rudman Commission

Other recommendations, largely by the Hart-Rudman Commission, were made to strengthen U.S. science and technology infrastructure to deal with national security threats. These focus on strengthening the base or science infrastructure, increasing federal R&D funding, instituting special science education programs, reorganizing and reorienting the mission of some national laboratories, and modifying rules dealing with independent research and development.

Proposals to Increase Federal R&D Funding

The Hart-Rudman Commission recommended that federal R&D resources be doubled to strengthen the science base as preparation for a national security defense and that OSTP play a paramount role in collecting data about R&D developing policies to strengthen the science base. It observed that there is no one place in the federal government which knows the government's physical, capital, and intellectual S&T assets (what it called "inventory stewardship" to enable an identification of research bottlenecks, opportunities, and priorities). "...[C]ollating and analyzing this information *in one place*, and using the conclusions of that analysis to inform the R&D budget process, is the *sine qua non* of a more effective public R&D effort."[171]

"Recapitalizing America's strengths in science and education" in order to strengthen U.S. national security capabilities was one of five key organizational changes recommended by the Hart-Rudman Commission.[172] The commission said "Second only to a weapon of mass destruction detonating in an American city, we can think of nothing more dangerous than a failure to manage properly science, technology, and education for the common good over the next quarter century." It cited serious under funding of public basic research with the potential for other countries to outperform the United States in R&D if funding were not increased. While there have been dramatic breakthroughs in the pace of change caused by S&T and implications for human intellectual and social adaption, the commission predicted future U.S. inadequacies because the United States would not profit from certain kinds of research the nation had chosen not to support, including the Superconducting Super Collider and basic electronics engineering.[173] It recommended "doubling the federal research and development budget by 2010 [to about $160 billion annually], and instituting a more "competitive environment for the allotment of those funds." This would involve fostering "a creative market' for a greater number of research institutions to bid on government research funds," so that less capable academic

---

[171]Hart-Rudman Commission, Phase III report, p. 34.

[172]Hart-Rudman Commission, Phase III report, p. 30.

[173]Hart-Rudman Commission, Phase III report, p. 32.

institutions can compete with "...high-prestige major schools with ample endowments...."[174]

Science and Engineering Education

The Hart-Rudman Commission cited American students' low performance in international tests of science and mathematics competence and ranked science and education as paramount concerns to national security because

> ...the inadequacies of our systems of research and education pose a greater threat to U.S. national security over the next quarter century than any potential conventional war that we might imagine. American national leadership must understand these deficiencies as threats to national security. If we do not invest heavily and wisely in rebuilding these two core strengths, America will be incapable of maintaining its global position long into the 2lst century."[175]

As a policy response the commission recommended "...a new National Security Science and Technology Education Act to fund a comprehensive program to produce the needed numbers of science and engineering professionals as well as qualified teachers in science and math." The commission used as a model for its plan the National Defense Education Act of the late 1950s and 1960s that provided both loan forgiveness incentives for those willing to serve in the military or teach in disadvantaged areas and also scholarships to those studying physical and natural science and mathematics. It recommended that "Congress should significantly expand the National Security Education Act of 1991 (NSEA) [from foreign language and foreign area studies] to include broad support for social sciences, humanities, and foreign languages in exchange for military and civilian service to the nation."[176] Incentives would include loan forgiveness and other financial incentives in exchange for a period of teaching science or mathematics in elementary or secondary schools, or military or government service. Those students who would choose government service in return for aid would also be allowed to defer educational loan repayment or reduce the loan principal amount while they serve in government. The report also recommended providing resources to modernize laboratories in science education, to expand existing programs aimed at helping economically-depressed school districts, to strengthen historically black colleges and universities, and to improve the training of science math teachers.[177]

National Laboratories

Duplication of effort in federal laboratories was cited in the Hart-Rudman Commission report as a serious problem that needed to be remedied in order to strengthen the U.S. science infrastructure and national security. While it did not specifically single out Department of Energy laboratories, the report cited laboratories that conduct R&D related to the DOE missions – such as nuclear, other energy

---

[174]Hart-Rudman Commission, Phase III report, p. ix, 32-34.

[175]Hart-Rudman Commission, Phase III report, p. ix.

[176]Hart-Rudman Commission, Phase III report, p. 89.

[177]Hart-Rudman Commission, Phase III report, p. x.

resources, and environment. It said that while the labs had a clear mission during the Cold War, they now "have been left to drift." One laboratory can fulfill the tasks needed to maintain nuclear weapons and manage their radioactive wastes. It concluded "...the labs remain critical in fulfilling America's S&T national security need and in addressing S&T issues pertinent to the public good. Each major laboratory needs a clearly defined mission area." It also warned that attention must be given to addressing morale problems that have occurred because of physical and intelligence breaches and attendant security investigations.[178] The commission recommended that "The President should propose, and the Congress should fund, the reorganization of the national laboratories, providing individual laboratories with new mission goals that minimize overlap."

Other Proposals to Strengthen U.S. Science Infrastructure

Enforce Independent Research and Development (IR&D) Rules. The Hart-Rudman Commission recommended more enforcement of IR&D rules to enhance private sector security-related R&D:

> The Defense Department cannot depend entirely on speeding up its integration with the commercial sector. The nation also needs to invest in selected research programs where military systems have no commercial counterparts. Unfortunately, large and complex DOD research and development projects generally suffer from a distortion of cost competition since companies often underbid the R&D phase in hopes of security funding in more profitable production phases. The Commission thus recommends that the laws prohibiting the use of Independent R&D (IR and D) funding for program support be more broadly interpreted and more strictly enforced."[179]

Create Interagency Space Working Group. The Hart Rudman Commission also reported that no interagency process for space exists and recommended establishment of an Interagency Working Group on Space (IGS) at the National Security Council to coordinate all aspects of the nation's space policy and place on the NSC staff those with the necessary expertise in this area. "This would allow space to be considered "systematically and consistently as a critical element of U.S. national security policy." [180]

Use More Open Source S&T Literature in Intelligence Analysis. The HR report also called for the intelligence community to place more emphasis on collected scientific and technological information and incorporate more open source intelligence into its analytical products.[181]

---

[178]Hart-Rudman Commission, Phase III report, p. 36-37.

[179]Hart-Rudman Commission, Phase III report, p. 72.

[180]Hart-Rudman Commission, Phase III report, pp. 79-80.

[181]Hart-Rudman Commission, Phase III report, p. 84.

APPENDIX 5, Abbreviations

CBRN	Chemical, Biological, Radiological, Nuclear
CBW	Chemical and Biological Warfare
CDC	Centers for Disease Control and Prevention
CSIS	Center for Strategic and International Studies
DARPA	Defense Advanced Research Projects Agency
DHHS	Department of Health and Human Services
DOD	Department of Defense
DOE	Department of Energy
DSB	Defense Science Board
E.O.	Executive Order
EXOP	Executive Office of the President
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
GAO	General Accounting Office
HHS	Health and Human Service [Department]
HSC	Homeland Security Council
IBM	International Business Machines Corp.
IOM	Institute of Medicine
NAE	National Academy of Engineering
NAS	National Academy of Sciences
NIH	National Institute of Health
NSC	National Security Council
NSTC	National Science and Technology Council
OHS	Office of Homeland Security
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PCAST	President’s Council of Advisors on Science and Technology
PCC	Policy Coordination Committee
PWMD	Preparedness Against Weapons of Mass Destruction Group
R&D	Research and Development
RDT&E	Research, Development, Test, and Evaluation
S&T	Science and Technology
TSWG	Technical Support Working Group
WMD	Weapons of Mass Destruction