Homeland Security Authorization Act
Fiscal Year 2006
H.R. 1817

Prepared by the Committee on Homeland Security Office of Communications
(202) 226-9600 http://homeland.house.gov

Table of Contents

Foreword

Congress created the Department of Homeland Security and set forth its missions in the Homeland Security Act of 2002, signed by the President November 25, 2002. As established in the Act, the DHS missions are to:

- Prevent terrorist attacks
- Reduce vulnerability to terrorism
- Minimize damage and assist in recovery from terrorist attack
- Be the focal point for handling natural and manmade crises and emergency planning
- Ensure that functions not directly related to homeland security are neither diminished nor neglected, except by Act of Congress
- Ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland
- Coordinate efforts to destroy narco-terror conspiracies

In late 2004 and early 2005, with advice from the National Commission on Terrorist Attacks on the United States (the 9/11 Commission) and from the House Select Committee on Homeland Security, Congress reorganized itself for the first time since the start of the Cold War to help DHS achieve its missions. The Senate created the Committee on Homeland Security and Governmental Affairs and the House of Representatives created the Committee on Homeland Security.

Just before midnight, after 13 hours of consideration on Wednesday, April 27, 2005, the House Committee on Homeland Security unanimously approved H.R. 1817, the Department of Homeland Security Authorization Act for Fiscal Year 2006—the nation's first ever comprehensive annual Homeland Security authorization legislation. The bipartisan bill was the result of hearings and oversight conducted by the House Select Committee on Homeland Security in the 108th Congress and by the permanent standing Committee on Homeland Security in the current 109th Congress. It is carefully crafted to help ensure that DHS possesses the resources and authority to achieve its missions. The House of Representatives will consider the bill on Wednesday, May 18, 2005.

Authorized Appropriations

Sections 101-108

The Department of Homeland Security Authorization Act authorizes appropriations not to exceed the following:

Purpose	*Amount*
For the Department of Homeland Security	$34,152,143,000
U.S. Customs and Border Protection	6,926,424,722
Border Security and Control Between Ports of Entry	1,839,075,277
Departmental Management and Operations	649,672,000
Homeland Security Regions Initiative	44,895,000
Operation Integration Staff	4,459,000
Office of Security Initiatives	56,278,000
Grants and Assistance for Critical Infrastructure Protection	465,000,000
Chemical Countermeasure Development	76,573,000
Nuclear Detection Office	195,014,000
Cybersecurity-related Research and Development	19,000,000
MANPAD Research and Development Technologies	10,000,000
SAFETY Act Anti-terror Technology Development	10,600,000
Screening Coordination and Operations	826,913,000
WMD Detection Technology	100,000,000
Container Security Initiative	133,800,000
Office for Interoperability and Compatibility	40,500,000
Grants to State and local governments for terrorism preparedness	2,000,000,000
Immigration and Customs Enforcement Legal Program	159,514,000

Preventing Attack

Deploying Counterterrorism Technology

Section 302

Challenge

The Department of Homeland Security has yet to establish the centralized Clearinghouse for advanced homeland security technology Congress envisioned in the Homeland Security Act of 2002. Entrepreneurs, laboratories, and governments are engaged in research, development, testing, and evaluation of advanced technologies and information resources applicable to defense and homeland security, but too few of these innovative

technologies are being utilized by the Department of Homeland Security, first responders, or others responsible for preventing attack, reducing vulnerabilities, and response and recovery. Terrorists will not wait for new technologies, but are working quickly to adapt existing technologies to their purposes.

Solution

To stay ahead of terrorist technology, the Act requires the DHS Directorate of Science and Technology to work quickly to transfer technology to prevent, prepare, respond, mitigate, and recover from threatened or actual terrorism to end-users. The Homeland Security Subcommittee on Emergency Preparedness, Science, and Technology approved this legislation on April 19, 2005. It sets a 90-day deadline after enactment to fully stand-up the Technology Clearinghouse.

Entrepreneurs, small and large firms, laboratories, and government research centers are vigorously pursuing research and development of advanced technologies and information resources for purposes ranging from administration to national defense to homeland security. The Act directs the Clearinghouse to identify, modify, and transfer homeland security technology for use by Federal, State, and local government agencies, first responders, and the private sector to prevent, prepare for, and respond to acts of terrorism. The bill authorizes surveys and reviews of available technologies developed by DHS, other Federal agencies, the private sector, and foreign governments for potential homeland security uses. It requires dissemination of the information gathered, including information about applicable standards and grants available for purchasing such technologies.

The Act clarifies the mission of the Technology Clearinghouse to engage the technological solutions and expertise of the private sector by establishing a technology transfer program to facilitate the identification, modification, and commercialization of existing technology and equipment for use by Federal, State and local governmental agencies, emergency response providers, and the private sector.

The Act directs the Under Secretary for Science and Technology to consult with other DHS offices to survey and review technologies that DHS, other Federal agencies, and the private sector have developed, tested, evaluated, and demonstrated that may prove useful to intelligence officers, border security officials, first responders, and all homeland security professionals. The S&T Directorate will itself conduct or support tests, evaluations, and demonstrations, as appropriate. It will consider the modification of certain technologies for antiterrorism use. And it will draw upon first responders, nationally recognized standards organizations, other government agencies, and technology centers to maximize the effectiveness and facilitate the commercialization of useful homeland security technology to speed the deployment of anti-terror technology.

Border Enforcement I: Security at the Line

Section 102

Challenge

America's vast land borders are the longest undefended and undisputed borders in the world. Few effective physical barriers prevent a determined terrorist from entering the United States from Canada or Mexico. New technology promises dramatic improvements in

border security in the coming years, but today's staffing levels do not permit the Border Patrol to adequately safeguard America.

Moreover, America's borders are the gateway for millions of visitors and for billions of dollars in trade. Leaving legal checkpoints short on staff diminishes free travel and free trade. Even modest enhancements to screening at legal border crossings require increased personnel in the absence of major technology upgrades. Securing borders against terrorists and terrorist materials is essential to preventing terrorist attack.

Finally, a shortage of Immigration and Customs Enforcement attorneys to represent the agency in removal proceedings before the Immigration Court and the Board of Immigration Appeals has reached a crisis point, creating opportunities for terrorist aliens to strike. The 9/11 Staff Report on Terrorist Travel specifically noted that, "[a]liens were granted multiple hearings, often resulting in lengthy delays. This system was easy to exploit. Because the immigration attorneys representing the INS in cases against aliens worked solely from paper files, they were often unable to properly track cases or access the necessary files to present their cases efficiently and knowledgeably. For much of the 1990s, case backlogs were considerable. Terrorists knew they could beat the system—and, as we have seen, they often did."

Solution

Within the $34.2 billion DHS budget, the Committee allocates up to 5.4%—$1.84 billion—for border security. This amount provides for full funding of the 2,000 new Border Patrol Agents Congress authorized in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). The administration sought only $36.9 million to hire 210 new Border Patrol Agents in FY2006. The Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief Act, 2005 (P.L. 109-13) funded 500 additional agents with monies that can be used in 2005 and 2006. The Homeland Security Authorization Act for Fiscal Year 2006 authorizes an additional $233 million to fill the balance of the 2,000 Border Patrol Agent positions. Assuming no deterrent effect on illegal crossings, 2,000 additional agents would permit the Border Patrol to increase the number of individuals apprehended for attempting illegal border crossings by an estimated 20%. More border agents will deter illegal crossing attempts and increase the likelihood of capturing groups and individuals crossing with the intent to commit terrorist acts. The Committee also fully supports the development and deployment of new border security technology.

To reduce delays caused by the shortage of ICE attorneys, the Act authorizes an additional $40 million for the hiring of 300 additional attorneys and their training and support, as well as sufficient funds for 300 additional adjudicators and their training and support. DHS may adjust fees as necessary to fund the adjudicators.

Border Enforcement II: Focus on the Mission

Section 501

Challenge

In 2004, more than 430 million people crossed the U.S. border legally, of whom 61% were not U.S. citizens. According to the Urban Institute, an estimated 800,000 people enter

the United States illegally each year. Of an estimated 11 million individuals in the United States illegally, one-third are believed to hold expired visas.

Two separate agencies within DHS are responsible for enforcing border security, creating unnecessary overlap and duplication and limiting accountability. On the border itself, Customs and Border Patrol attempts to identify and detain those seeking to enter the nation without legal authority or with the intent to commit terrorism. Within the United States, Immigration and Customs Enforcement attempts to find and arrest the same individuals. Both agencies work abroad.

Redundant intelligence gathering, legislative outreach, public affairs, internal coordination, and support staff waste taxpayer money, diminish resources available to combat terrorism, limit cooperation and information sharing, and cause operational and administrative difficulties that hamper the prevention of terrorist attack. Rationally allocating resources between the two agencies to achieve their closely-related missions is difficult at best under the current organizational structure.

Solution

The bureaucratic walls created by the CBP/ICE divide must be eliminated without compromising the outstanding work of both agencies. Even with organizational obstacles, border patrol agents and inspectors work tirelessly and effectively to keep America safe. ICE investigators have a strong record of accomplishment, from capturing child predators to shutting down intellectual property pirates. A unified chain-of-command would provide for more timely and effective communication between border personnel and interior enforcement personnel. Working together, these agencies would be able to use economies of scale to accomplish even more.

The Act directs the Secretary of Homeland Security to describe the rationale for the current system to Congress, review and evaluate the effectiveness of the current organizational structures in achieving the DHS mission to prevent terrorism, and to develop a plan to correct the operations and administrative challenges created by the division of CPB and ICE. The Secretary is to consider whether duplicative offices and functions can be reorganized so that scarce border security resources can be used more efficiently and is to submit "appropriate reorganization plans," so that DHS can more effectively accomplish its mission to block the entry and facilitate the capture of terrorists.

Streamlined Security Systems

Section 201

Challenge

Registered traveler and worker identification programs in DHS require background checks and security screening. Programs to expedite travel—such as Free and Secure Trade, Registered Traveler, and NEXUS/SENTRI—as well as programs to provide secure identification to workers—such as the Transportation Worker Identification Card and the Hazmat Endorsement Credential for drivers' licenses—have separate application processes, fees, and enrollment facilities. While these programs may use common resources to make credentialing decisions, the programs appear stovepiped to individual Americans using them.

For some, participation in these multiple programs means hundreds of dollars in fees and even more expense in lost time. Participation can require interstate travel and hours of duplicative work to supply similar information for multiple checks. While each program has unique missions, there is duplication in the application information required. For example, all applications require personal and biometric data and the screening of individuals against terrorist and criminal databases. This creates duplications and inefficiencies that waste taxpayer and customer resources.

Solution

The Act requires the Secretary to establish a single application program for conducting security screening and background checks on individuals participating in certain voluntary or mandatory credentialing or registered traveler program. A single process for submitting application information and biometric data and for background checks will eliminate unnecessary redundancies.

A consolidated background check process is simply common sense. Individuals who hold security clearances that satisfy the requirements of DHS programs should not be forced to repeat the entire clearance process, and expediting the process for some will mean DHS application analysts can assist others more quickly and efficiently. To ensure that privacy is protected, the Act requires the Secretary to establish privacy standards and procedures before implementing the program.

Easing the burden on transportation workers and travelers not only makes the application process more convenient and customer friendly, but enhances the well-being of all Americans by reducing the cost of commerce.

Risk-based Cargo Screening

Section 305

Challenge

The Container Security Initiative, a DHS program placing Customs and Border Protection inspectors at selected foreign ports to target and inspect containers destined to the United States, currently covers 36 ports. Plans call for its expansion to approximately 50 ports. CSI funding is $126 million for 2005 and $138.8 million for 2006.

CSI lacks a risk-based strategy. Initial port selection was based on shipping volume. Now that large European and Asian ports are covered, further expansion should be prioritized based on risk, not on proxies for risk such as shipping volume. Moreover, the world lacks standards for risk-based screening and inspection to protect against terror-related shipments and expedite safe shipping. As CSI expands, some nations may find it difficult to purchase and maintain reliable non-intrusive inspection equipment.

Solution

To ensure that DHS personnel and resources are used in the most appropriate locations to combat the threat of terrorists using containers too accomplish their aims, the Act requires the Secretary to conduct risk assessments at all foreign ports where DHS may consider implementing CSI. The Act authorizes DHS to purchase, install, and provide training for screening equipment at foreign ports that meet certain inspection standards. The

Act also requires that containers be evaluated using the same criteria whether they originate from a CSI or non-CSI port.

Red Teaming

Section 214

Challenge

While few officials considered the possibility of terrorists using commercial aircraft as weapons of mass destruction before 9/11, no formal process raised sufficient concern to cause the implementation of effective countermeasures. Now that the capability to use aircraft as WMD has been limited, terrorists seek new and innovative ways to strike bigger blows against civilization. Administrative reforms have enhanced the ability to predict and defend against such efforts, but legislation has yet to fully support the effort to predict terrorist innovation. Intelligence and operational agencies use red teams to "think like the enemy," and to help anticipate and defeat new types of attacks. The Intelligence Reform and Terrorism Prevention Act (the implementing legislation for the 9/11 Commission Report) mandated the use of red teams to test conventional views and assessments, but did not focus on using red teams for analyzing nuclear and biological threats.

Solution

The Act requires DHS to apply red team analysis to terrorist use of nuclear weapons and biological agents. As terrorists seek to exploit new vulnerabilities, it is imperative that appropriate tools be applied to meet those threats. The Act will broaden the intelligence process, thereby strengthening preemptive capabilities.

Priority on Personnel: IAIP Recruiting

Section 221

Challenge

DHS, as a new player in the intelligence community, competes with other members of the intelligence community and the private sector for experienced and trained analysts from a relatively small pool of qualified candidates. The Information Analysis and Infrastructure Protection Directorate requires highly trained personnel to conduct complex risk assessments to ensure that limited resources are put to their highest and best uses.

Solution

The Act gives the Secretary authority to pay recruitment bonuses for expert career civil service analysts of up to 50% of annual pay. The authority expires at the end of fiscal year 2008.

Nuclear and Biological Intelligence

Section 213

Challenge

The key to preventing the most serious terrorism imaginable—a nuclear or biological attack—is intelligence. DHS lacks robust intelligence capability to detect nuclear threats in the planning and preparation stage and to develop new means to pre-empt such efforts.

Solution

The Act requires the establishment of analytic expertise within the DHS Office of Information Analysis to create and disseminate intelligence products specifically covering terrorist efforts to use nuclear and biological weapons.

Open Source Strategy

Sections 224-225

Challenge

DHS has no comprehensive open source intelligence strategy, despite broad recognition in the intelligence community that more effective use of open sources will improve prevention capabilities.

Solution

The Act establishes a "one stop shop" within DHS for reliable, comprehensive, and accessible open source information by assigning the Undersecretary for IAIP to implement an open source information and analysis strategy within DHS. This strategy will enable the Assistant Secretary to produce and disseminate reports and analytic products based on unclassified open-source information.

Information for Local Leaders

Section 212, 216, 220

Challenge

The Homeland Security Act of 2002 made the Secretary accountable for the distribution and distribution of threat warning information to state and local governments and to the public. Despite the law, other Federal agencies have issued homeland security alerts without coordinating with DHS. This results in mixed messages being received by state and local officials, the media, and the public—and raises questions about federal credibility.

Solution

The Act coordinates federal threat advisories by requiring that analytic products and conclusions be communicated in a manner that limits confusion and operational conflicts. It strengthens the Office of Information Analysis by giving it access to terrorist threat related information and ensuring that it is routinely given access to all terrorism-related information acquired by any DHS component. It gives IA direct access to DHS databases to the extent technologically feasible.

The Act also formalizes DHS relationships with State, local, tribal and private sector officials. It formally authorizes the Homeland Security Information Network, a national, real time communication system for DHS, other government agencies, the media, and the public.

Being Prepared

Clarifying Threats and Colors

Sections 216 and 223

Challenge

Congress assigned the Information Analysis and Infrastructure Protection Directorate within DHS to administer the Homeland Security Advisory System to provide information about terrorist threats to governments and the public. However, the color-coded system is vague and threat warnings remain broad. The public discounts the importance of the system, and even law enforcement professionals and emergency response personnel have deprecated it for vagueness and for lacking associated guidance.

Solution

The Act reforms the Advisory System to communicate more specific information, command greater confidence, and strengthen preparedness. It instructs DHS, to the extent possible, to use the system to provide specific warnings to targeted facilities, regions, states, localities, and private sector industries. Region-based and sector-specific warnings are given priority, and guidance to state and local officials on measures to take in response to warnings is required.

The Act requires that appropriate terrorist threat information to help implement protective measures and countermeasures be provided to state and local government officials, the media, and the public, recognizing both the importance of giving local agencies the tools they need to prevent, prepare for and respond to acts of terror, and supporting efficient local management of limited protective resources. The use of colors to indicate the threat condition becomes optional, under the Act, which provides that other methods of communicating threat information may be employed.

Communication among First Responders

Sections 107 and 308

Challenge

Many jurisdictions continue to experience communication difficulties among first responders contributing to confusion, delays, and risk. Effective communications interoperability requires extensive training, specialized equipment, and inter-jurisdictional agreements. The FY06 DHS budget lacks sufficient funding for the Office for Interoperability and Compatibility (OIC) to fulfill its responsibilities.

Solution

The Intelligence Reform and Terrorism Prevention Act of 2004 authorized OIC to provide technical assistance and grant guidance to help first responders achieve interoperable

communications. OIC is responsible for establishing a comprehensive national approach to achieve interoperable communications. By issuing letters of intent to commit future funds, OIC encourages planning. The Act increases the authorization for OIC to $40.5 million, to ensure that the billions available for interoperability are spent wisely.

Exercise Goals

Section 301

Challenge

Frequent and effective exercises are essential to terrorism preparedness at all levels of government. America is fortunate that the actual need to respond to terrorist attacks, and the opportunity to learn from responses, has proven infrequent. All levels of government have conducted terrorism preparedness exercises since 9/11. However, such exercises are often conducted in isolation, without quality control, adequate dissemination of best practices, or adequate tools to help agencies and different levels of government communicate.

Solution

The Act makes the DHS Office for Domestic Preparedness the central coordinator for exercises. Placing this responsibility in ODP makes terrorism preparedness exercises more effective by ensuring that minimum standards will be achieved as multi-disciplinary responses are implemented. For example, the Act directs ODP to establish a National Terrorism Exercise Program to establish basic requirements for all federal, state, and local exercises. This will help make terrorism preparedness exercises multi-disciplinary, including, as appropriate, cybersecurity components. It will also make the exercises more realistic by basing them on current risk assessments, including the risk of catastrophic attack. Realism increases the likelihood that corrective actions and new resources will address actual threats. ODP's coordination will also facilitate the adoption of uniform performance measures and provide more information for the implementation of corrective actions identified as necessary by the exercises. ODP is also expected to help assess exercises based on best practices, which can be disseminated to all appropriate government and training institutions to expand the benefits of training exercises.

The Act directs the Secretary to regularly organize and conduct National Level Exercises involving top officials from all levels of government, providing additional legislative guidance for biannual TOPOFF exercises. National Level Exercises allow response evaluation and discovery of problems that arise when multiple agencies and nations work together to prevent, prepare, and respond. The United States conducted TOPOFF exercises in 2000, 2002, and 2005. The Act instructs the Secretary to better incorporate detection, disruption, and prevention in future TOPOFF exercises.

Counter-Cyberterrorism

Sections 312-313

Challenge

The information infrastructure that controls much of the nation's vast physical resources and communications network—making modern civilization possible—remains

highly vulnerable to terrorist attack. The Director of the National Cyber Security Division at DHS, serving under the Assistant Secretary for Infrastructure Protection, is currently responsible for the cybersecurity mission at DHS. The cybersecurity mission is too important too handle at this relatively low level.

Cybersecurity—the prevention, protection, and restoration of the information infrastructure—is an essential element of American life. Protecting against deliberate, debilitating cyber attacks is as much a part of the homeland security mission as protecting against physical attacks. A cyber attack holds the potential of catastrophic consequences far exceeding those of many physical attacks. Cybersecurity requires both protection of the nation's cyber and information systems and active defenses against cyber weapons.

Solution

The Act elevates the cybersecurity mission in DHS, putting an Assistant Secretary for Cybersecurity in charge of the National Cybersecurity Division (NCSD) and the National Communications System, recognizing the convergence of data and telephony. In doing so, the Act incorporates elements of H.R. 285, the Cybersecurity Enhancement Act of 2005, as approved by the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity on April 20, 2005.

Making the director of the NCSD an Assistant Secretary will focus the mission of the office within the Department, give it required stature, and increase accountability.

Homeland Operations Collaboration

Section 217

Challenge

While some state and local officials work closely with the Department of Homeland Security Operations Center, many do not fully understand the capabilities and requirements of the new center. Moreover, federal officials lack full knowledge of the capabilities and requirements of state and local homeland security officials.

Solution

Under the 9/11 Memorial Homeland Security Fellows Program, state and local homeland security professionals will serve 90-day rotations at the Homeland Security Operations Center. They will bring to the HSOC knowledge to help federal officials more effectively serve state and local officials to prevent terrorist attack and respond to incidents while returning to their regular duty stations with invaluable hands-on knowledge of the resources and limitations of the HSOC.