Description of document:	**Department of Homeland Security (DHS) United States Secret Service (USSS) Strategic Impact Analyses, 2007**
Requested date:	24-July-2009
Released date:	30-July-2009
Posted date:	19-October-2009
Source of document:	Department of Homeland Security United States Secret Service Freedom of Information and Privacy Acts Branch Communication Center 245 Murray Lane, S.W. Building T-5 Washington, D.C. 20223

DEPARTMENT OF HOMELAND SECURITY
UNITED STATES SECRET SERVICE
WASHINGTON, D.C. 20223

Freedom of Information and Privacy Acts Branch
Communications Center
245 Murray Lane, SW
Building T-5
Washington, D.C. 20223

JUL 30 2009

File Number: 20070008

Dear Requester:

Reference is made to your recent request received by the United States Secret Service on July 24, 2009, for better quality copies pertaining to the United States Secret Service Strategic Impact Analyses.

Enclosed is a revised clean copy of your document.

Sincerely,

Craig W. Ulmer
Special Agent In Charge
Freedom of Information &
Privacy Acts Officer

Enclosure: Copy of Requested Documents

Strategic Planning – Strategic Impact Analyses

Strategic Impact Analyses -- produced for the Director, Deputy Director and all Assistant Directors - are two page summaries of issues that may impact the Service. The reports are posted on the Intranet.

SIA/SPM 01-01 -- Appointment of Paul H. O'Neill as Secretary of the Treasury. This analysis provides a brief biography on Paul H. O'Neill. O'Neill's appointment may impact the Service in the following areas: environmental planning/responsibility; health and safety programs; human resource management; accountability; a call for innovation and improvement; and technology application. (February 2001)

SIA/SPM 01-02 – CIA Using Innovative Procurement Method To Stay On The Leading Edge Of Technology. CIA is using venture-capital firm In-Q-Tel to influence the development of commercial-off-the-shelf technology they can use. The Service may be able to learn from this innovative procurement method, or use some of the technology being developed. (February 2001)

SIA/SPM 01-03 -- Proposed National Homeland Security Agency Will Deal With Critical Infrastructure Protection. This analysis presents highlights from the U.S. Commission on National Security Report "Road Map for National Security: Imperative for Change." Specifically, the analysis discusses the proposed creation of a National Homeland Security Agency (NHSA) to address the emerging threats posed by the spread of new technology and weapons of mass destruction. The analysis concludes that, although it does not seem likely that President Bush will create the NHSA, he will review the national security infrastructure and federal infrastructure protection efforts; these reviews may impact the Service. (February 2001)

SIA/SPM 01-04 -- House Rules Committee Adopts Rule Change Pertaining To Performance Goals And Objectives. The Rules Committee of the House of Representatives adopted a new rule change requiring that committee reports include a statement of general performance goals and objectives, including outcome-related goals and objectives, for which the measure (e.g., legislation) authorizes funding. Some Congressional Staffers believe that the new rule will cause Congress members to review agency strategic plans to draft the statement of general performance goals; others believe that Congress members will "work around" the new rule and use appropriations legislation (versus authorizing legislation) to obtain funding for initiatives. In general, the new rule should foster better communication between executive agencies and the legislative branch; Service members may be called upon to help members of Congress draft general performance goals. (March 2001)

SIA/SPM 01-05 -- FBI's Carnivore System Sparks Privacy Concerns And Public And Legislative Action. FBI's Carnivore system, a technical snooping system that can monitor cell phone conversations and sift through every email of a suspect's Internet Service Provider, has come under legislative and public scrutiny. Congress members are asking the Justice Department to suspend use and further development of the system until citizen's privacy concerns can be adequately addressed. The FBI continues to use Carnivore and the public has responded by developing and distributing free cryptology programs and services that provide users anonymity when surfing the web and sending emails. Some programs even wipe out hard drive files and can potentially erase any evidence that may be used in forensic examinations. The continuing Carnivore controversy may impact the Service a few ways: the Bush administration may pass privacy legislation which may hinder an investigator's ability to obtain information for a case; or, citizens may begin using free cryptology programs to conceal their identities when perpetrating white collar crime or threaten our protectees. (March 2001)

SIA/SPM 01-07 -- Seamless Integration of Stand-Alone Security Systems Allows for Remote Monitoring of Facilities. This analysis discusses the use of web-based systems that seamlessly and cost effectively

integrate stand-alone and proprietary CCTV, access control and building systems. These systems allow managers to remotely control via a web-browser all security and building systems for several different buildings. The analysis highlights one company that is developing a web-browser controlled robot that can roam through buildings to capture video and sound through an attached camera and microphone. We discuss the potential applications for this technology in the Service. (March 2001)

SPM/SIA 01-11 – Government at the Brink – Highlights. Senator Fred Thompson, U.S. Senator Committee on Governmental Affairs, released his two-volume report, "Government on the Brink" on June 5, 2001. This SIA summarizes Senator Thompson's report, which addresses the four most pervasive federal government problems areas -- workforce management, financial management, information technology management, and overlap and duplication. (June 2001)

SPM/SIA 01-12 – Office of Homeland Security. This analysis discusses the challenges Secretary Ridge must address as he coordinates the homeland security efforts of more than 40 departments and agencies. Although several studies show we are better prepared today for a chemical/biological/nuclear attack than we were five years ago, there is still much more that can be done to increase preparedness. (November 2001)

Background

Paul H. O'Neill, who describes himself as a radical maverick, left the Aluminum Company of America (Alcoa) in May 2000. During his tenure at Alcoa, he accomplished many things, the most significant of which was increasing both annual revenue and profits *fourfold*. He also insulated Alcoa from wild swings in aluminum prices, expanded Alcoa's global reach, and masterminded a series of acquisitions.

BIOGRAPHICAL INFORMATION

December 4, 1935	Born, St. Louis, Missouri
1955 – 1957	Site Engineer, Morrison-Knudsen, Inc.
1960	B.A. in Economics, Fresno State College
1960 – 1961	Claremont Graduate School
1962 – 1965	Post-Graduate Studies, George Washington University
1966	M.P.A. Indiana University
1961 – 1966	Systems Analyst, Veteran's Administration
1967 – 1969	Budget Examiner, Bureau of the Budget
1969 – 1970	Chief, Human Resources Program Division, OMB
1971 – 1972	Assistant Director, OMB
1973 – 1974	Associate Director, OMB
1975 – 1977	Deputy Director, OMB
1977 – 1981	Vice President, International Paper Company
1981 – 1985	Senior Vice President, International Paper Company
1985 – 1987	President, Director, International Paper Company
1987 – 2000	Chairman, CEO, Aluminum Company of America

Mr. O'Neill married Nancy Jo Wolfe on September 5, 1955. They have four children and twelve grandchildren.

While at Alcoa, O'Neill also was a strong supporter of integrating environmental, health, and safety processes into Alcoa's businesses – he fostered in the company an uncompromising principle of putting environment, health and safety first. In 1996, Alcoa received the World Environment Center (WEC) Gold Medal for International Corporate Environmental Achievement for their world-class commitment to continuous environmental improvement through training, research and application.[1] O'Neill also was instrumental in improving Alcoa's safety record. O'Neill targeted Dupont, the industry leader in safety, hoping to surpass their level of safety performance; Alcoa accomplished this goal in 2000.[2]

O'Neill has been described as a man of uncompromising integrity and profound intellect, a man with a deep-seated devotion to social and environmental responsibility.[3] It is likely that O'Neill's integrity and character influenced the values that Alcoa employees incorporate into their daily work processes. Some of these values – integrity; environment, health and safety; quality and excellence; customer; people; profitability; and accountability – may be stressed in the future within the Department of Treasury. O'Neill demonstrates his belief in social responsibility through his participation in several community and educational organizations

[1] World Environment Center selects Alcoa for environmental award. (1996, January). Business Wire.
[2] Post-Gazette News at Post-Gazette.com (www.post-gazette.com/businessnews/20000513alcoa3.asp)
[3] Alcoa Congratulates Paul O'Neill on Nomination as U.S. Secretary of the Treasury. (2000, December). Business Wire.

(approximately eight, including the Gerald R. Ford Foundation, the Council for Excellence, and the National Academy of Social Insurance). O'Neill's commitment to social responsibility also transferred to Alcoa, as they help communities by contributing funding to efforts in the areas of education, health and human services, the environment and ecology, civic and community improvements, and cultural endeavors. One can anticipate that O'Neill's strong leadership style and his commitment to several core values will influence business practices within the Department of the Treasury.

Potential Impact

O'Neill's career experiences and values may impact the Service in any of the following areas:

1. The Environment. O'Neill's appointment may trigger an increased emphasis on the Service's implementation of/adherence to the National Environmental Policy Act.

2. Health and Safety. O'Neill's appointment also may bring about an increased emphasis on safety and health programs, polices, and requirements as they apply to all employees, our protectees, and the public.

3. People. O'Neill's commitment to the people in his organization may direct more focus on the equal opportunity program, employee satisfaction, and rewards and recognition programs.

4. Accountability. Alcoa's "accountability" value holds individuals and teams accountable for actions and results. If O'Neill were to emphasize accountability within Treasury, bureaus may be required to focus more on audit follow-up programs, budget formulation and execution, inspection programs, and evaluation programs.

5. Quality and Excellence. Quality and excellence is characterized by continuous improvement and innovation in programs, products, and services. O'Neill's appointment may result in bureaus conducting more program evaluations to ensure they are achieving quality and excellence in their programs, products, and services.

6. Technology. While at Alcoa, O'Neill championed the use of technology to make business transactions more cost-efficient and timely. The Common Infrastructure Initiative (CII) and eBusiness were two key Alcoa initiatives that demonstrate O'Neill's commitment to using technology to improve business operations. O'Neill's appointment may result in all bureaus examining their use of technology to improve their business operations.

CIA Using Innovative Procurement Method To Stay On The Leading Edge Of Technology

In late 1999, the Central Intelligence Agency (CIA) launched In-Q-Tel, a non-profit venture-capital corporation, as a means to keep up with the technological revolution. In-Q-Tel – which acts as collaborative venture between the CIA, academia, and industry – coordinates the work of several partner organizations to develop innovative and unconventional information technology solutions to strategic problems. The CIA provided $28.5 million to In-Q-Tel, who takes a minority position in funding start-ups and helps bankroll other projects that have the potential to produce commercial products the CIA can buy and use. And, although In-Q-Tel sponsored security technology will be commercially available, in-Q-Tel officials are working with the CIA and the National Security Agency (NSA) to meet the challenge of the public "reverse-engineering" the security technology. The officials believe that if they take the right approach to public cryptography, the security technology can be public and very secure.

As of October 2000, In-Q-Tel had committed to seven investments from the more than 400 pitches they received last February. In-Q-Tel's initial projects focus on the following areas:

IN-Q-TEL SUCCESS STORY

Presidential Intelligence Briefing System (PIDS)

PIDS was one of the first In-Q-Tel projects to be implemented at the CIA. CIA analysts use PIDS to produce the daily brief for 16 senior government officials. In the past, CIA analysts read and shuffled hundreds of paper intelligence cables each day to produce this daily brief. Now, PIDS does the shuffling – it brings the cables into a Lotus Notes database, performs a variety of searching and analysis functions, and then puts the brief on a notebook computer. PIDS is built around Notes Release 5, NetOwl and a prototype document annotation tool.

Beside the obvious productivity savings, PIDS also yielded the benefits of more timely and accurate briefings and the fingertip accessibility of background information for analysts when they are asked to further elaborate on their briefings.

PIDS will be developed into a commercial product. The system will be used by organizations with analysts who must find, organize and present data from multiple sources.

Agency use of the Internet. In-Q-Tel is focusing specifically on Internet search and privacy issues. They are currently working with SRA International Inc. in Fairfax, Virginia. SRA has a commercial search engine called NetOwl that uses natural language processing (versus keywords) to find information. NetOwl is a text-mining tool that can deduce that a word is a person's name, an organization or a place. In-Q-Tel has greatly increased the power of NetOwl by funding enhancements that let it identify events and relationships and create structured data from unstructured text using XML.

Information Security. In-Q-Tel and its partners are concentrating on hardening intrusion detection, monitoring and profiling of information use and misuse, and network and data protection. In-Q-Tel is currently working with Science Application International on the further

development of netEraser, an effort aimed at repelling denial-of-service attacks and shoring up security efforts within Virtual Private Networks.

Analytic Data processing Capabilities. In-Q-Tel is focusing on the areas of geospatial and multimedia data fusion/integration, all source analysis, and computer data forensics.

Distributed Information Technology Infrastructure. In-Q-Tel is examining problems associated with the CIA's distributed information technology infrastructure, which is organizationally segmented and geographically dispersed. In the near future, the CIA, NSA, and In-Q-Tel funded companies will work on portable-device security, to include tamper detection, biometric authentication, cryptography, self-protecting data, secure enterprise storage and more.

In-Q-Tel also funds pilot projects to see how existing systems might be adapted to fit CIA needs and work requirements. An example of such an effort is CIA's pilot project with Systems Research and Development (SRD) in Las Vegas. SRD developed collusion-detection software that can spot casino cheaters and card counters by correlating information from multiple sources about relationships and earlier transactions. The software also could warn a casino that a job applicant once shared an address with a known criminal. The software might also find extensive use in industry to aid in fraud detection.

Potential Application to the Service

In-Q-Tel's innovative information technology initiatives can be applied throughout the Service in many areas, including but not limited to:

1. *Protection*. The Intelligence Division could use NetOwl or PIDS for protective intelligence gathering, assimilation and presentation.

2. *Investigation*. Investigative offices could use NetOwl to improve search capabilities and perform link analyses for all case types. Investigative offices also may be able to benefit from In-Q-Tel's work in the computer forensics area.

3. *Support*. Innovative security programs -- for wired and wireless networks, critical facilities, and our stakeholders in the financial sector – may be of interest to the Service. Additionally, the Service may learn from the CIA's creative approach to shaping the development of commercial products that can be used in the Agency.

Proposed National Homeland Security Agency Will Deal With Critical Infrastructure Protection

Commission Recommendations

A congressionally mandated commission recommended creating a National Homeland Security Agency to address the emerging threats posed by the spread of new technology and weapons of mass destruction. The commission also recommended major alterations in the Defense and State departments; a broader role for the National Guard; and, increased funding for the federal research and development budget by 2010. Further, the commission called on Congress to create a special select committee for homeland security to provide more effective support and oversight.

COMMISSION ISSUES REPORT

On January 31st, the U.S. Commission on National Security, headed by former senators Gary Hart and Warren B. Rudman[1], issued its report, "Road Map For National Security: Imperative For Change." The report warned of the threat of international terrorism, noting that a strike on U.S. soil is likely in the next 25 years.

The recommended National Homeland Security Agency, whose director would have Cabinet status, would protect American lives and infrastructure, such as the highway system and information technology. The new National Homeland Security Agency would be formed through the unification of the Coast Guard, the Customs Service, the Federal Emergency Management Agency and the Border Patrol. The new agency would coordinate defense against attacks and responses if an attack succeeded. The main task of the National Guard would be changed to deal with the prospect of an attack on U.S. soil.

Central to the new agency would be a directorate of CIP (critical infrastructure protection) that would manage cyber defenses for the various sectors of the economy, including banking and finance, telecommunications, transportation, and utilities. The CIP directorate would have two primary responsibilities: overseeing the physical assets and information networks that make up the U.S. critical infrastructure; and coordinating government and private sector efforts to address the nation's vulnerability to electronic or physical attacks. The CIP directorate would work with the private sector to enhance information-sharing on cyber and physical security, track vulnerabilities, propose improved risk management policies, and delineate the roles of various government agencies in preventing, defending, and recovering from attacks.

---

[1] In addition to Rudman and Hart, the commission included former House speaker Newt Gingrich (R-Ga.); lawyer and former commerce undersecretary Lionel H. Olmer; former representative Lee H. Hamilton (D-Ind.), director of the Woodrow Wilson International Center; business executive and former Air Force secretary Donald B. Rice; Norman R. Augustine, chairman of Lockheed Martin Corp.'s executive committee; Anne Armstrong, a Nixon and Ford administration official and former ambassador to Britain; John R. Galvin, former supreme allied commander for Europe; Council on Foreign Relations President Leslie H. Gelb; former NBC diplomatic correspondent John Dancy; James R. Schlesinger, a former energy and defense secretary and CIA director; former U.N. ambassador Andrew Young; and retired Adm. Harry D. Train.

The report's recommendation to create the CIP comes at a time when the entire federal critical infrastructure protection effort is coming under review by the Bush administration. There are dozens of government and industry bodies – such as National Infrastructure Assurance Council (NIAC), the President's Information Technology Advisory Committee, and the Export Council on Encryption – that are now involved in recommending and enforcing policies related to cybersecurity. Some cybersecurity experts argue that consolidating or eliminating some of these bodies will yield a leaner, more centralized government effort; other experts argue that there are too many powerful interests to make the centralized approach effective. National cybersecurity experts believe that Bush may appoint an IT "czar" by next summer to better manage the government's IT investments and possibly change the role of the FBI's National Infrastructure Protection Center (NIPC).[1]

Implementation of Commission Recommendations

Several factors may impede the implementation of the commission's recommendations. If history is an indicator of future success, this report may end up on a shelf with many previous departmental reorganization reports. Analysts also expressed doubts about the feasibility of creating a new security agency, given the large number of agencies and organizations seeking the same funds and authority. And Congress cannot reach consensus about security policy.

Impact on the Service

Although it may be unlikely that we will see a National Homeland Security Agency created in the near future, it is very likely that the Bush administration will review the national security infrastructure and federal critical infrastructure protection efforts. This may impact the Service in the execution of our responsibilities related to National Special Security Events; our relationships with the banking and financial industry infrastructures; execution of our emergency preparedness programs; and our dealings with other federal agencies, boards and councils in the areas of critical infrastructure protection and national security.

[1] The NIPC has come under fire for its perceived unwillingness to share information on investigations with intelligence and national security agencies and its failure to broadcast timely warnings during some virus outbreaks.

House Rules Committee Adopts Rule Change Pertaining to Performance Goals and Objectives

The Rules Committee, House of Representatives, adopted a rule change (see box) that will impact how authorizing committees prepare their committee reports.

RULE CHANGE

"The requirement that committee reports include a summary of oversight findings and recommendations by the Committee on Government Reform, if timely submitted, is repealed and replaced with a **new requirement that committee reports include a statement of general performance goals and objectives, including outcome-related goals and objectives, for which the measure authorizes funding.**" [1] *[Rule XIII, clause 3(f)(1)]*

In considering the rule change, the Subcommittee on Rules and Organization of the House heard testimony from fellow Congressmen, officials from the General Accounting Office and the Office of Management and Budget, and a respected academician. During this testimony, the House Committee on Rules discussed the ways in which committees design and advance performance goals, gained insight on how committees analyze these performance goals during authorization or reauthorization of programs, and received suggestions on how committees could better accomplish the oversight goals of the Results Act.[2] The Congressional Research Service (CRS) presented reports indicating that congressional committees are increasingly setting performance goals: the number of public laws with performance measure provisions nearly doubled from the 104th to the 105th Congresses and the number of committee reports containing performance measure provisions nearly tripled, from 27 to 78. CRS also cited a few instances when committees specified detailed performance indicators and directed that continued funding was contingent upon performance.[3]

A recent National Academy of Public Administration (NAPA) Legislative/Executive Forum brought together staff members from the House Committee on Rules, a respected academician, a representative from the CRS, and a former congressional staff member to discuss the impact of the rule change on federal agencies.

A former congressional staff member pointed out that the original text of the Government Performance and Results Act called for congressional establishment of performance standards and goals for all bills or resolutions that provided for the authorization of appropriations or appropriation of funds. He stressed that the rule change will not only require Congress to develop performance goals, but also to review agency strategic plans and work further with agencies affected by the authorization legislation to develop performance goals.

---

[1] Section-by-Section Summary of H.R.L.S.5 Adopting House Rules for the 107th Congress: U.S. House of Representatives Committee on Rules website at www.house.gov/rules/107rules_secsum.htm.
[2] Subcommittee hearing on "The Government Performance and Results Act and the Legislative Process of House Committees:" Statement of Congressman John Linder, Chairman, Subcommittee
[3] Ibid.

Current congressional staff members envision that the new rule will facilitate communication between the agencies and the authorizing committees. They believe the goals and performance measures will come from the agencies affected by the proposed authorizing legislation and urged agencies to work closely with the committees when drafting authorizing legislation. One staff member believes that all authorization legislation will soon contain "boilerplate" language that addresses this new need for a statement of performance goals.

Two other speakers were skeptical about whether the rule change would actually lead to the establishment of performance goals for authorizing legislation. One speaker contended that the rule change would not necessarily lead to the establishment of performance goals, citing Congress' noncompliance with existing legislation[4] as support that Congress does not always comply with the rules it imposes. These speakers emphasized the difference between authorization and appropriation legislation and stressed that appropriations legislation can provide funding to initiatives without the requirement to identify goals and performance measures. They expressed concern that, since the new rule only applies to authorization legislation, some members of Congress may use appropriation legislation to obtain funding for initiatives and thereby circumvent the requirement to establish performance goals.

Impact on the Service

Implementing this new rule may prompt the House's authorizing committees to refer to agency strategic plans to develop performance objectives. There also may be a need for Service representatives to work with congressional committees to draft authorization legislation that impacts our mission areas. The new rule should foster communication between the authorizing committees and Treasury and/or Service representatives, which presents an opportunity to make known to members of Congress the importance of our investigative and protective missions and to, perhaps, learn of prospects to expand our mission.

[4] Congressional Budget and Impoundment Control Act of 1974 (P.L. 93-344, 31 USC 1102, 2 USC 681-688)

FBI's Carnivore System Sparks Privacy Concerns and Public and Legislative Action

Carnivore, one of the Federal bureau of Investigation's (FBI) technological tools in its war against crime, can monitor cell phone conversations and sift through every e-mail of a suspect's Internet Service Provider and capture all incoming and outgoing communications. The FBI is beginning work on a expanded version of Carnivore, which is only one part of a larger suite of cybersnooping tools known as the "Dragon Ware Suite." Carnivore, renamed DCS100 due to its controversial name, is of great concern to a number of people – privacy advocacy groups, average citizens who want to protect the privacy of their cyber communications, and members of the Congress.

Although Carnivore has been used only about 25 times to monitor the email traffic of suspects in cases involving national security, privacy advocates worry that the use of this technology will evolve and end up being used as frequently as are wiretaps (there are several thousands court-ordered wiretaps a year for a much broader range of investigations).

The Privacy Foundation is calling for change in the Federal Wiretap Act to guarantee that the privacy and suppression of evidence safeguards that apply to the interception of telephone calls, also to apply to email and other electronic communications. They also advocate that law enforcement agencies be required to create "audit trails" for each investigation that uses Carnivore and that Congress institute penalties for tampering with those audit trails. Finally, they are pushing for Carnivore software modifications to ensure the program collects only the information Required by the court order.

STUDIES SHOW CITIZEN CONCERN

A recent study published by the National Consumers League showed that 56 percent of Americans are "very Concerned" about losing privacy, a higher number than Are worried about healthcare, crime, or taxes

An Information Technology Association of America Poll showed that over 80 percent of Americans had at Least some concern thqt the government-held personal Data about them would be misued.

On the internet, citizens are banding to gether to create and distribute free cryptology programs and services to provide users anonymity when surfing the web and sending email. Safeweb technology hides cutomers' identities and movements as they scan the web. Some of the capabilities of Safeweb include encryption and protection of content, masking of the user's computer address, blocking of profiling cookies, and profiling of the profilers. HushMail is a free, secure Web-based email system that eliminates the risk of leaving unencrypted files on Web servers and allows users to send and receive encrypted email messages and attachments. M-o-o-t (www.m-o-o-t.org) is an open source cryptography project that is secure against the United Kingdom's Regulation of Investigatory Powers Act, Carnivore, the Australian and proposed Council of Europe and New Zealand laws regarding seizure of stored data, intercepted data, traffic data and access to plaintext/keys of encrypted data. The self-contained software contains a suite of email, word processing, spreadsheet, and graphics programs and is shipped on

a bootable CD. User data and mail is encrypted and stored in offshore data havens, bypassing local storage

Members of Congress, too, are very concerned about the use of Carnivore and it's potential threat to an individual's privacy. House majority leader Dick Army (R – Texas) has denounced Carnivore as illegal. Mr. Army and 28 other members of Congress sent a letter to the Justice Department asking the Department to suspend use of the Carnivore system until questions about privacy concerns could be addressed. Despite Congressional concern over the use of this system, the Justice Department continued use of Carnivore and development of an expanded version of the program. The Justice Department did, however, commission an independent review (completed December 8, 2000) of the Carnivore system. Mr. Armey categorized this review as "superficial," conducted by a team with clear ties to the Clinton/Gore Administration. He continues to argue that the Justice Department should stop developing new versions of Carnivore and other cybersnooping software and stop using current programs until the constitutional questions surrounding the use of these programs have been adequately addressed.

How this may impact the Service

1. Protective and Investigative Operations. The following key attributes of the M-o-o-t project could impact our investigative and protective missions:

   - Email is not traceable – product information indicates that it is impossible for others to distinguish between email and other traffic or measure the amount of email; and

   - Hard drive data will be inaccessible – if the CD is removed, the system will shut down and access to local storage (hard drives etc.) will be disabled, so if a computer is seized there will be nothing to find.

2. The Bush Administration. Republican Congressman Dick Armey is not only the House majority leader, he is also from President Bush's state of Texas. That being considered, Mr. Army may gain more support from the Bush administration to keep systems such as Carnivore in check and implement controls to protect an individual's privacy.

Resources

Cannon, C. M. (2001, February). A laundry list of hot digital issues awaits George W. Bush. Fortune, p. 47.
CIA Spooks Privacy Freedom Fighters With Triangle Boy. (2001, February 21). Network News, p. 3.
Drell, A. (2001, March 7). Technology vs. privacy. Chicago Sun-Times, p. 6.
Freedom Works website. www.freedom.gov
Gordon, P. (2000, November 22). Wiretap law expert: new rules needed to restrain Carnivore. Privacy Foundation Web Site (www.privacyfoundation.org/release/storyScarniv.html).
Ross, F. (2001, April). Bad News for Snoops - This U.K. upstart takes the bite out of Carnivore: Company Business and Marketing. Ziff Davis Smart Business for the New Economy, p. 52.
Levin, D. (2001, February 18). Big Brother could read your e-mail -- Surveillance: The FBI's ability to wiretap the Internet puts individual privacy at risk.. The Baltimore Sun, p. 1C.
Raul, A. C. (2001, March 6). SPAM Is Annoying. But ID Theft Is Criminal. The Boston Globe, p. A15.

Resources

Cannon, C. M. (2001, February). A laundry list of hot digital issues awaits George W. Bush. Fortune, p. 47.
CIA Spooks Privacy Freedom Fighters With Triangle Boy. (2001, February 21). Network News, p. 3.
Drell, A. (2001, March 7). Technology vs. privacy. Chicago Sun-Times, p. 6.
Freedom Works website. www.freedom.gov
Gordon, P. (2000, November 22). Wiretap law expert: new rules needed to restrain Carnivore. Privacy Foundation Web Site (www.privacyfoundation.org/release/story5carniv.html).
Ross, F. (2001, April). Bad News for Snoops - This U.K. upstart takes the bite out of Carnivore: Company Business and Marketing. Ziff Davis Smart Business for the New Economy, p. 52.
Levin, D. (2001, February 18). Big Brother could read your e-mail -- Surveillance: The FBI's ability to wiretap the internet puts individual privacy at risk.. The Baltimore Sun, p. 1C
Raul, A. C. (2001, March 6). SPAM Is Annoying. But ID Theft Is Criminal. The Boston Globe, p. A15.

Seamless Integration of Stand-Alone Security Systems Allows for Remote Monitoring of Facilities

Businesses and government organizations may benefit from new web-based products designed to improve facilities and security management. Such products integrate web-browser technology, networking technology, and building and security systems to allow managers to remotely monitor facilities and respond immediately to problems that arise.

Vendors & Products

Onega InfoSystems. Onega InfoSystems is a California-based software company that manufactures Building Smart and FacilitySm@rt, products that use networking and web technologies to integrate building security, closed circuit television (CCTV), and building automation systems. Building Smart offers a variety of features, including remote control and monitoring, video data communication, real-time security and warning, automatic energy conservation, and dynamic parking lot management. Building Smart is primarily used in upscale residential and commercial buildings.

Using a web-browser, FacilitySm@rt seamlessly and cost effectively integrates stand-alone and proprietary CCTV, access control and building systems. FacilitySm@rt allows building and security managers to watch live streaming video, review digital video clips, and monitor and control the access control system. Managers have web access to all facilities from a browser on any personal computer. The system is easy to learn (point and click technology), uses open architecture for scalability and flexibility, and uses object oriented technology to reduce configuration time. Events can be triggered through the integrated access control system, or from traditional sensors. Management and/or security personnel are automatically notified of events via cell phones or other devices.

FacilitySm@rt was recently installed at Beulah High School in Valley, Alabama to combat school violence, survey for any terrorist activity, and provide real-time video to emergency personnel and other officials. The system was the first of its type to be installed on a school campus and was tested during a mock disaster exercise on March 20th. In December 2000, FacilitySm@rt was installed in Taipei, Taiwan in the Tan Moo Ballpark. Whenever an alarm is set off, FacilitySm@rt automatically turns on the ballpark's lighting system and captures video clips that can be used as criminal evidence. Ballpark personnel are notified automatically of the problem via their cell phones or other communication devices so they can immediately react. Ballpark and government officials are pleased with the system because it helps them better monitor the blind corners of the facility.

Xanboo. Xanboo uses a variety of personal computer-based controllers, cameras, and sensors to communicate over the Internet so homeowners and small business owners can keep an eye on the house/business from anywhere in the world. A review of the Xanboo system found it to still have bugs; it is only as reliable as the Windows operating system and can be tripped up by a

power failure or the computer going into sleep mode. The initial cost of the system is reasonable at $150 for the equipment and $14.95 per month to access Xanboo's web browser. The system consists of a central control unit about the size of a portable CD player, a color video camera with a built-in motion detector, a 60-foot video connector, and Xanboo controller software for Windows-based computers. Users can use up to four cameras and purchase other sensors, e.g., water, acoustic and door and window sensors. When a camera or sensor registers an alert, Xanboo sends notification to whatever text-enabled device the user specifies; the user can log onto Xanboo.com and check out the situation.

iRobot – Robot Surveillance. iRobot recently demonstrated an Internet-controlled, three-foot-tall robot called the iRobot-C. iRobot-C will likely go on sale sometime next year, with an estimated price tag of $ 2,000. The iRobot-C will be able to climb stairs, prowl around a building and its grounds, and send back over the Internet everything it sees with its nose-mounted video cam and everything it hears with its microphone array. The user can control the robot remotely through simple mouse clicks on a browser screen. The iRobot-C also can relay the user's voice as it roams through the building.

Impact on the Service

Protection and Building Support. FacilitySmart would allow for the simultaneous remote monitoring of several facilities – e.g., Embassies, 950H Street, 1111 18th Street – and automatically notify Service personnel of problems at those facilities. Problems may include a security breach or system malfunction (e.g., lighting, elevator, HVAC, etc.). The iRobot could roam through the facilities we protect to provide an additional security presence. The Service would need, however, to conduct thorough review and testing of these systems to ensure that any risks and vulnerabilities inherent to the systems are manageable and acceptable. We also would need to determine the cost and potential cost savings (including manpower savings) associated with the implementation of such systems.

RIF

References:

Fernadez, D. (2001, March 16). [METRO] Metro News+. The Atlanta Journal and Constitution, p. 2E.

Lewis, P. H. (2001, April 2). Remotely interesting: with Xanboo's surveillance system and a steady Net link, you can keep an eye on the house even while you're away on vacation – as long as your PC behaves. Fortune, p. 194.

Ortega InfoSystems Web Site at www.ortegainfo.com/main.htm.

Government at the Brink – Highlights

Senator Fred Thompson, U.S. Senate Committee on Governmental Affairs, released his two-volume report, "Government on the Brink" on June 5, 2001. The first volume of the report addresses the four most pervasive federal government problem areas – workforce management, financial management, information technology management, and overlap and duplication. The second volume includes descriptions of these and other problems at selected federal agencies. This paper summarizes key points from the two-volume report.

Although the Department of Treasury is referred to in both volumes of this report, no mention is made of the Secret Service. The Secret Service may, however, be impacted by departmental actions if issues cited in volume two of Senator Thompson's report are addressed, specifically information security, information technology investment management, money laundering and bank secrecy, and the safety and soundness of the banking industry. Additionally, Senator Thompson's discussion of serious management problems within the federal government may prompt Congressional and/or Presidential action, which could ultimately impact the Secret Service. The information presented by Senator Thompson also may be useful as the Service continues addressing critical issues, including outsourcing (OMB Circular A-76) and workforce restructuring (OMB Bulletin 01-07).

Problems

Workforce Management. The federal workforce is in a crisis state. For many agencies, the downsizing of the 1990s resulted in skills imbalances, knowledge deficits and the loss of experienced personnel. Downsizing was poorly managed – because cuts were taken at the lower levels, the government became more top heavy, with few younger employees to factor into succession planning. And because there was no commensurate reduction in workload or process reengineering, the government became less efficient. Adding to the severity of the situation, approximately 1/3 of federal employees will be able to retire over the next five years. The report predicts that disruption of government services will eminently result if the workforce crisis is not addressed. Yet, the federal civil service system is ill equipped to address this crisis; the processes for hiring, firing, promoting, training, and evaluating federal employees are broken and outdated. The report recommends that agencies identify their optimal workforce size and the skill mix required, hire to meet skill needs, and work to keep employees motivated and productive.

Financial Management. The government, as a whole, cannot pass a financial audit. The report references a General Accounting Office (GAO) finding that leading private organizations are using enterprise wide systems that integrate financial and operating data to support management decision making and external reporting requirements. These types of systems do not exist in the federal government. Most federal agencies do not have the right financial systems; only a few federal agency systems can be used for day-to-day operations and the inherent inadequacies of financial systems often lead to errors and mistakes. Inadequate training and supervision are cited as other causes of financial errors. The report states that the Department of the Defense is the

biggest offender in this area, providing one example of the Navy writing off $3 billion in inventory as "lost in transit." The report recommends that agencies make financial management an entity-wide priority; report the amount wasted each year; share information with other agencies to avoid erroneous payments to taxpayers; and recover money when necessary ("recovery auditing").

Information Technology Management. Computer Security was cited as the most important concern in the area of information technology management; in December 2000, information technology and security was identified as a "problem" category by 100 percent of the Inspector General offices at 27 different agencies. Inadequate computer security programs leave many agency systems vulnerable to attack and/or intrusion, putting at risk government data and the privacy of citizen data. To improve computer security, Senator Thompson's report recommends that agencies examine security risks; implement risk reduction approaches; educate users; and monitor the effectiveness of the risk reduction approaches. The report also states that most agencies do not align technology programs with their mission, do not use information technology to improve efficiency and effectiveness, and cannot properly manage information technology projects, citing many examples of how the government inefficiently manages large-scale projects. The report offers the following ways to improve information technology management: using early oversight and planning; avoiding reinvention of technology; sizing projects to manageable levels; encouraging innovation; creating incentives for contractors to perform better; communicating lessons learned; and reviewing existing large computer systems acquisitions.

Overlap and Duplication. Although Senator Thompson points out several examples of duplicative federal programs, he also recognizes that some duplication is good and it is often impossible to eliminate outdated programs in the federal government. In view of that, the report does not offer specific recommendations in this area. However, the report does state that reliable program data is needed to discuss and debate about federal programs and determine whether those programs should continue.

DUPLICATION IN LAW ENFORCEMENT

- Over 40 agencies are engaged in activity to combat terrorism, for combined annual spending of approximately $10 billion.
- At least 45 different federal agencies conduct federal criminal investigations; collectively they employ 50,000 investigators.
- Many federal agencies have their own internal "police department."

Fixing the Problems

The first way to fix management problems is to enforce legislation that is already in place, e.g., the Chief Financial Officers Act, the Federal Financial Management Improvement Act, the Government Performance and Results Act, the Clinger-Cohen Act, and the Government Information and Security Act. Senator Thompson also recommends that the Bush

Administration and Congress listen to and implement recommendations presented by the GAO, various Inspector General offices, and Senate and Congressional committees. He believes that the President and his administration must take a leadership role, make it a priority to solve government management problems, and task OMB to keep after agencies until the problems are resolved. OMB should establish performance goals, strategies, measures and timetables to resolve the issues, using as a starting point the solutions that have already been identified. The report also recommends that agencies and OMB identify the funding necessary to resolve the problems and Congress provide that funding. Finally, the report calls for linking funding to results; the President and Congress must insist on reliable performance information to determine what is working and what is not. If programs overlap, the most efficient and effective programs will be funded and others will not.

Office of Homeland Security – Highlights

With the appointment of Former Pennsylvania Governor Tom Ridge as the Assistant to the President for Homeland Security, much debate began over how much authority the Office of Homeland Security will have. Established by Executive Order 13228 on October 8th, the Office of Homeland Security is tasked with developing, coordinating, and implementing a national strategy to secure the United States from terrorist attacks. To implement this national strategy, the Office of Homeland Security must coordinate with approximately 43 federal departments/agencies and state and local emergency response units. As established, the Assistant to the President for Homeland Security will lack day-to-day authority over cabinet members and specific departments and agencies. There is also potential overlap in duties of other cabinet members and the Deputy National Security Advisor for combating terrorism.

According to press reports, the White House envisions that Tom Ridge's position will be similar to the position of National Security Advisor and has structured the Office of Homeland Security after the National Security Council. National Security Advisors are not subjected to Congressional influences and do not have administrative duties to divide their attention: they are not obligated to any one agency and therefore can work effectively with all. Although many in Congress believe that Tom Ridge's position will become as powerful as the position of National Security Advisor, they also believe legislation to strengthen the role would be beneficial.

HOMELAND SECURITY – ACTIONS PRIOR TO 9/11/01

- On May 8, 2001 President Bush instructed Vice President Cheney to head a special task group to study the federal government's ability to respond to an attack using a weapon of mass destruction. The task force concluded the U.S. needed a comprehensive, integrated federal response with responsibility for coordination at the highest levels. The report is due out in October.
- In January 2001, the U.S. Commission on National Security issued the report, "Road Map For National Security: Imperative For Change." The commission recommended creating a National Homeland Security Agency to address the emerging threats posed by the spread of new technology and weapons of mass destruction. The report also contained several other recommendations – including major alterations in the Defense and State departments and a broader role for the National Guard – and warned of the threat of international terrorism, noting that a strike on U.S. soil is likely in the next 25 years.
- A Pentagon study conducted in 2000 looked at the possibility of biological attacks, information warfare and nuclear warfare. The study concluded that the United States could not prevent such attacks.
- In 1995, President Clinton issued a directive to clarify agency roles in the event of a chemical/biological/nuclear attack. In 1996, the Defense Against Weapons of Mass Destruction Act was passed. Critics believe this act is woefully inadequate, largely because progress in implementing the act has been very slow.

Congress prefers using legislation to clearly define structures and establish obvious lines of oversight so it can retain control. Critics of such legislation argue that legislation could impede the flexibility and organizational effectiveness of the Office of Homeland Security. Presently, two bills propose making Homeland Security a cabinet level agency to give it a stronger statutory base of power – H.R. 1158 and S. 1534. Supporters of the legislation say it would give greater critical mass to under funded, scattered efforts. Critics say the bills do not create a single authority to defend the homeland because the FBI and FEMA remain in separate organizations. The new agency would have the authority to stop terrorists at the border and clean up after a terrorist attack, but without law enforcement, could not track terrorists after they enter the country and before they strike.

The Office of Homeland Security will face many challenges, whether it remains an office within the Executive Office of the President or becomes a cabinet-level agency. Perhaps the most significant challenge will be coordinating the activities of federal departments and agencies.

GAB – 2/2/07

RIF

Coordination efforts will be complicated because of the vertical integration of executive branch departments and agencies, unlinked/incompatible federal computer systems, overlapping jurisdictional areas, and different Cabinet-level bosses. Coordination difficulties can be foreseen, for instance, at our borders, where computer systems used by the U.S. Coast Guard, U.S. Customs Service and the Immigration and Naturalization Service cannot share information. Coordination difficulties also may be seen after a terrorist attack, as three entities with different goals respond: the FEMA responds to disasters; the FBI investigates terrorist attacks; and the military responds to threats of all enemies, foreign and domestic.

The war against terrorism involves every government agency at every level of government. It is essential that federal, state, and local entities coordinate, cooperate, and share information to support the national strategy for homeland security. Some entities already are doing this through such mechanisms as Joint Terrorism Task Forces and the FBI's Strategic Information Operations Center. Other organizations, such as the Army Information Dominance Center, use technology to share information. The Army's Information Dominance Center (now part of Army's Special Operations Command) uses an experimental intelligence system that taps into participating databases to collate data from every source on a particular subject. Representative Curt Weldon (R – PA) helped establish the center, which provided him eight pages of information about a shady Serbian official during the Kosovo conflict; the CIA provided him with one paragraph. The CIA and FBI have signed on to support and use the data mining system. Representative Weldon is trying to expand the system to a National Operations and Analysis Hub. The intelligent, data mining system uses commercial software to connect information bits into a cohesive analysis.

To win this war, agencies also must break out of their bureaucratic boxes and combine into constantly evolving collaborative structures, without confusing who does what for whom. The National Guard is the best example of an organization that acts in this manner. National Guard units routinely switch from one master and mission to another without losing track of who is in charge. In New York City, in the days following the September 11th attacks, the National Guard 1) provided logistical and security support at the clean up site, acting under the direction of the Governor, funded through state funds; 2) flew patrol missions over U.S. cities, acting under Presidential direction, funded through federal funds; and 3) provided additional airport security, acting under local direction, funded through federal funds. To successfully implement the national homeland security strategy, many federal, state and local entities may have to act like the National Guard.

The Office of Homeland Security will require a new type of leader across government. Agency leaders must be able to relinquish control – temporarily – of assets and people to interagency task forces. Interagency task force experience for any civilian aspiring to the Senior Executive Service level may become a necessity. Participation in such task forces may come in the form of smartly planned "virtual organizations" that invest heavily in secure technologies. Agency leaders may have to "subcontract" their staff to the Office of Homeland Security to ensure successful implementation of the national strategy for homeland security. Agency leaders must be willing to contribute as the Office of Homeland Security brings together every useful government tool, regardless of who owns it.

Potential Impact on the Service

USSS Offices and/or Personnel Potentially Impacted by Office of Homeland Security (Per Executive Order 13228)	
USSS Office/Personnel	**Affected by the Office of Homeland Security Responsibility**
Intelligence Division	• Collect, analyze, and disseminate intelligence, law enforcement and terrorist threat information.
Technical Security Division (TSD)	• Develop monitoring protocols and equipment for use in detecting the release of biological, chemical, and radiological hazards.
Emergency Preparedness Program and Presidential Protective Division (Continuity of Government) and Major Events Division (NSSEs)	• Review and assess the adequacy of the portions of all Federal emergency response plans that deal with terrorist threats within the United States.
All Offices and Personnel with Protective Responsibilities	• Coordinate domestic exercises and simulations that assess practice systems that would be called upon to respond to a terrorist threat or attack in the United States and coordinate training for Federal, state and local employees would may respond to such an attack..
Office of Investigations	• Coordinate efforts to protect critical public and privately owned information systems (e.g., finance and banking) within the United States from terrorist attacks.
Office of Protective Operations for facilities and complexes we are, by law, authorized to protect; Technical Security Division for security surveys of other government agencies and local municipalities	• Develop criteria for reviewing whether appropriate security measures are in place at major public and privately owned facilities within the United States.
Major Events Division	• Coordinate domestic efforts to ensure that special events determined by appropriate senior officials to have national significance are protected from terrorist attack.
Office of Investigations	• Coordinate efforts to ensure rapid restoration of public and private critical information systems (e.g., finance and banking) after disruption by a terrorist threat or attack.
Emergency Preparedness Program and Presidential Protective Division	• Review plans and preparations for ensuring the continuity of the Federal Government in the event of a terrorist attack that threatens the safety and security of the U.S. Government or its leadership.
Office of Government Liaison and Public Affairs and responsible offices	• Periodically review and assess the legal authorities available to executive departments and agencies to permit them to perform the functions described in the executive order.
Office of Administration and responsible offices	• Identify programs that contribute to the Administration's strategy for homeland security; provide guidance and advice to the Director of OMB on the level and use of funding in departments and agencies for homeland security-related activities; and, certify the funding levels to the Director of OMB that the Assistant to the President for Homeland Security believes are necessary and appropriate for the homeland security-related activities of the executive branch.
All Offices	• Request that employees of federal departments or agencies be assigned or detailed to the Office of Homeland Security.

Summary of Congressional Legislation Proposed Regarding Homeland Security

Congressional Action – In Brief	
H.R.3026 – Office of Homeland Security Act of 2001 • introduced on 10/4/2001 by Representative Jim Gibbons • Latest Major Action on 10/15/2001, referred to House subcommittee • 11 Cosponsors	The Homeland Security Act of 2001 is very similar to Executive Order 13228. It establishes an Office of Homeland Security within the Executive Office of the President. It requires the Director of the Office to create a national strategy for homeland security, to include all aspects of prevention and response to terrorist activities. The Director also develops a national homeland security budget and certifies federal agency counterterrorism budgets; reviews federal activities to ensure the national strategy for homeland security is effectively implemented; eliminates duplication and gaps in federal homeland security activities; develops a comprehensive national threat assessment; oversees emergency information sharing; and establishes a center within the Office to disseminate information learned from homeland security exercises. The Act also establishes the Homeland Security Advisory Council to advise the President and Director on the creation and implementation of the national strategy, and the Director on the operation of the Office.
H.R.1158 – National Homeland Security Agency Act • introduced on 3/21/01 by Representative William (Mac) Thornberry • Latest Major Action on 4/2/2001, joint hearings in House committee's/subcommittee actions • 11 Cosponsors, (10 joined after 9/11/01) • According to press reports, this is the leading legislation to make the Director of the National Homeland Security Agency more powerful	The National Homeland Security Agency Act transfers several federal government entities to a newly established National Homeland Security Agency. The Act requires the Agency's Director, who serves an advisor to the National Security Council, to: (1) plan, coordinate, and integrate Federal government activities relating to homeland security, including border security and emergency preparedness, and act as a focal point regarding natural and manmade crises and emergency planning; (2) work with State and local governments and executive agencies in protecting U.S. homeland security and support State officials through the use of regional offices around the country; (3) provide overall planning guidance to such agencies regarding homeland security; (4) establish operational and control procedures for potential contingencies, including those that require military assets; and (5) annually develop a Federal response plan for homeland security and emergency preparedness. The act transfers to the Agency the authorities, functions, personnel, and assets of the Federal Emergency Management Agency, U.S. Customs Service, Border Patrol of the Immigration and Naturalization Service, U.S. Coast Guard, Critical Infrastructure Assurance Office, Institute of Information Infrastructure Protection of the Department of Commerce, National Infrastructure Protection Center, and National Domestic Preparedness Office of the Federal Bureau of investigation. The act establishes within the Agency separate Directorates of Prevention, Critical Infrastructure Protection, and Emergency Preparedness and Response and an Office of Science and Technology. The act requires the Director to establish mechanisms to share information and intelligence with U.S. and international intelligence entities.

Congressional Action – In Brief

S.1534 – Department of National Homeland Security Act of 2001 • Introduced 10/11/01 by Senator Joseph I. Lieberman • Latest Major Action on 10/11/2001, referred to Senate committee • 1 Cosponsor	The Department of National Homeland Security Act of 2001 act establishes the Department of National Homeland Security by realigning several existing government entities. The act requires the Secretary of the Department, who is a member of the President's cabinet and of the National Security Council, to: (1) plan, coordinate, and integrate U.S. Government activities relating to homeland security, including border security and emergency preparedness, and to act as a focal point regarding natural and manmade crises and emergency planning; (2) work with State and local governments and executive agencies in protecting U.S. homeland security, and to support State officials through the use of regional offices around the Nation; (3) provide overall planning guidance to executive agencies regarding U.S. homeland security; (4) conduct exercise and training programs for employees of the Department and establish effective command and control procedures for the full range of potential contingencies regarding U.S. homeland security, including contingencies that require the substantial support of military assets; (5) annually develop a Federal response plan for homeland security and emergency preparedness. The act transfers to the Department the authorities functions, personnel and assets of the Federal Emergency Management Agency, U.S. Customs Service, Border Patrol of the Immigration and Naturalization Service, U.S. Coast Guard, Critical Infrastructure Assurance Office, Institute of Information Infrastructure Protection of the Department of Commerce, National Infrastructure Protection Center, and National Domestic Preparedness Office of the Federal Bureau of Investigation. The act establishes within the Department separate Directorates of Prevention, Critical Infrastructure Protection, and Emergency Preparedness and Response and an Office of Science and Technology. The act requires the Secretary to establish mechanisms to share information and intelligence with U.S. and international intelligence entities.
H.R.1292 – Homeland Security Strategy Act of 2001 • Introduced on 3/29/2001 by Representative Ike Skelton • Latest Major Action on 4/24/2001, joint hearings in House committee/subcommittee • 3 Cosponsors (1 joined after 9/11/01)	The Homeland Security Strategy Act of 2001 directs the President to identify specific homeland security threats through comprehensive threat and risk assessments and develop a comprehensive strategy for homeland security (protection from terrorist or strategic attacks) under which Federal, State, and local government organizations coordinate and cooperate to meet security objectives. The act also requires that the President implement the resulting strategy as soon as practicable; ensure that the strategy is carried out through the heads of appropriate executive departments and agencies; and designate a single Government official responsible for homeland security