Presidential Strategy for Homeland Defense: A Summary of Recent Proposals

The Federalist Society
for Law and Public Policy Studies

The Federalist Society would like to acknowledge the work of Stewart Greenleaf and Geoffrey McGovern on this paper.

MEMO

Date: 8/6/02
To: Leonard Leo, V.P.
From: Geoff McGovern, Intern
Re: Revisions to National Strategy for Homeland Defense

On July 16, 2002, President Bush released a new National Strategy for Homeland Defense. The initiative, constructed as an active measure to secure the country from possible terrorist activity, was described by the President as a "guidance directive" designed to reorganize, modernize, and streamline existing defenses at the federal and state levels. The following pages offer a review of the included measures in the strategy, focusing on the major areas of new policy, and provide a look at some existing criticisms of the measures by civil rights/civil libertarian groups and policy advocates.

Overview of National Strategy

The National Strategy identifies three major objectives and policy goals set forth for defensive policy: prevention of domestic terror attacks; reduction of national vulnerabilities to possible hostile action; and the minimization of damages in the event of future attacks. Six "critical mission areas" are developed as focus groups for emerging policy: intelligence and warning; border and transportation security; domestic-counter terrorism; protecting critical infrastructure and key national assets; defenses against

catastrophic threat; and emergency preparedness and response. These identified areas work as interrelated key sectors to secure the proper outlets for security policy in an increasingly complex regulatory and international environment.

The foundations of the strategy rest upon "uniquely American strengths that cut across all of the mission areas, across all levels of government and across all sectors of our society." These foundations, which serve are the platforms for the reform initiatives, include law, science and technology, information sharing and systems, and international cooperation. From these segments each of the policy shifts are developed and tailored.

President Bush's strategy calls for reorganization of the many separate agencies and regulatory bodies that already deal with issues critical to national security. Under the new measures, and with pending congressional approval, the currently autonomous operations would be consolidated into a cooperative network overseen by the Department of Homeland Security (DHS). The DHS would thus be comprised of twenty-two federal entities charged with the implementation of the new strategic measures. The reorganization will facilitate information sharing, maximizes the concentration of field experts, allows the security community to speak with one voice, and boosts efficiency through the elimination of duplicate operations across the different offices. Although these agencies have additional duties that do not relate directly to homeland defense initiatives, they will continue to complete their non-security operations independent of the DHS initiatives.

Responding to the needed reforms in the operation of security measures, the National Strategy actively seeks cooperation across several key elements, including federal agencies, state authorities and resources, and the private sector. Governors are

encouraged to respond to the call to action in their home states by creating Homeland Security Task Forces equipped with the necessary tools to respond in times of crisis, and create policy that dynamically seeks-out measures to improve citizen safety. These task forces would serve as the state's coordinating body with the DHS. For closer cooperation with the private sector, a Homeland Security Advisory Council would encourage private risk assessment, seek specialized knowledge from industry as to possible areas of vulnerability, and emphasize investment in key asset protection.

Objectives of National Strategy

I. Intelligence and Warning

The priority of improving intelligence gathering capabilities for use as early detection and warning devices must continue to serve as a primary focus for a successful defense initiative. The New Strategy stresses this factor, but does so in a manner that recognizes concerns regarding fundamentally protected liberties of the citizenry. Mindful of the tension between security and liberty, the strategy states, "efforts to gather intelligence on potential terrorist threats can affect the basic rights and liberties of American citizens." Therefore, the new policies are designed to grant necessary authority to strategic enforcement agents, while preserving the privacy and freedom of individuals.

To effectively deal with security concerns, the National Strategy departmentalizes the various stages of analysis, active operations, and strategic planning. Information analysis operations for identifying potential threats are broken into four segments. Tactical Threat Analysis involves the thorough analysis and dissemination of information on terrorists and terrorist activities. Following the collection of sensitive intelligence

from field operatives the Tactical Threat Analysis team reviews the material for evidence of sinister activity. This aspect becomes a joint operation by the Department of Central Intelligence (DCI), the FBI, and the DHS, all under the administrative authority of the latter. The Strategy also mentions the development of a monitoring system for dual-use machinery and devices, i.e., fermentation equipment that can be used for both legitimate pharmaceutical manufacturing and biological weaponeering. This first stage of analysis represents the primary examination of information coming before the intelligence community. Strategic Analysis of the Enemy entails a deep understanding of organizations and the intents of foreign governments, and likewise falls under the purview of the DCI, FBI, and DHS. More theoretical than threat analysis, the strategic analysis works from softer data in a predictive fashion, assessing motive and alliance possibilities.

Vulnerability Assessments fall under the complete control of DHS. This division is charged with the responsibility of assessing the level of risk associated with various key elements and possible targets in the country, and works extensively on achieving greater security pursuant to the goal of protecting critical infrastructure (discussed subsequently). Furthermore, DHS assumes responsibility for conducting Threat-Vulnerability integration that "maps" the groups that pose the greatest threats over the sectors where they are most vulnerable. Much of this work already takes place under current protective details; however, the new strategy focuses the attention, compiling the resources of the independent agencies into a cohesive whole.

After the analysis stage, the assessments are to be translated into specific actions, or Tactical Preventative Action, undertaken by the National Joint Terrorism Task Force

of the DHS. More of a front-line enforcement branch, the task force will disrupt terrorist acts and detain the suspects when analysis uncovers covert plotting. Additionally, Warning and Protective Action, taken by DHS, will serve a communicative function to prompt sectors in security implementation, terrorist deterrence, and in increasing citizen awareness. In the effort to continue to devise effective policy in the security environment, a Strategic Response office in the Office of Homeland Security will develop new strategies to deal with terrorist threats.

One of the main provisions of the Intelligence and Warning section of the strategy is to enhance and update the analytic capabilities of the FBI. Answering Attorney General Ashcroft's request for expanded abilities to effectively deal with terrorist threats, the proposal increases the FBI's analytical staff fourfold, drawing upon twenty-five high-level experienced analysts from the CIA. Additionally, the secretary of DHS is granted broad authority to access intelligence information, including working "with state and local law enforcement and the private sector to leverage the critical homeland security information in the possession of these entities."

II. Border and Transportation Security

The homeland security strategy designates a single entity within the DHS to manage who and what enters the United States. This shift is another large reorganization of existing agencies; the Immigration and Nationalization Service, Customs Service, Animal and Plant Health Inspection Service, and the Transportation Security Agency would all fall under the authority of the DHS.

The reorganized conglomerate would control the vital transportation and immigration functions such as the issuance of visas and border security. As part of a new initiative (the Enhanced Border Security and Visa Entry Reform Act) suggested by the National Strategy, special identification requirements would be necessary, requiring visitors to present biometric identification (i.e., retinal scans, fingerprinting) at borders and when applying for visas.

Also included under these provisions are the recapitalization of the Coast Guard (at the largest budget increases in its history in both 2003 and 2004), and the implementation of the Aviation and Transportation Security Act of 2001, which federalized airport security. The proposals also call for increased monitoring of shipping containers into the country by prescreening the cargo and developing technology for self-screening shipments.

III. Domestic Counter-Terrorism

The new proposals for counter-terrorism guidelines hone in on the FBI's role as terrorist investigator. This represents a shift in the role of the FBI, and hence the proposals are designed to retool the guidelines as necessary for a revised mission. Under the new initiative, hundreds of active FBI agents will be reassigned from the criminal division to the terrorism investigations unit. This includes mobile special agents trained to deliver leadership and guidance wherever an incident may arise, domestically or internationally, and separately forms the National Joint Terrorism Task Force.

The National Strategy aims to modify the FBI's current investigative guidelines to bring them more in-line with the new responsibilities added from the expanded terrorist

investigation duties. Consequently, the proposal offers greater latitude and flexibility for agents conducting counter-terrorism investigative activities within the United States' borders, and permits the use of commercially available data-mining technology for internet searches related to suspected terrorist activity. Current regulations (non-Strategy guidelines) restrict agents from conducting such non-intrusive searches unless specifically tied to a pending criminal investigation.

Other terrorist-targeted policies are included in the security strategy. Fingerprint data from all suspected terrorists would be collected into a central database for identification purposes, and terrorist financial networks would become specific targets of investigation and, ultimately, seizure. These latter two policies regarding financial resources would fall under the express duties of The Review Group, a multi-agency effort staged by the FBI and Operation Green Quest, and jointly headed by the Department of Justice and the Customs Service.

IV. Protecting Critical Infrastructure and Key Assets

As mentioned previously, defending the nation's essential elements of operation and administration becomes a top priority under the strategy's guidelines. As defined by the USA PATRIOT Act, critical infrastructure includes: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or the destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." This wide definition protects as included sectors agriculture, water resources, public health, emergency services, government, the defense industrial base, information and

telecommunications services, energy, transportation, banking and finance, the chemical industry, and postal and shipping services. Monuments and events of national scale are also covered under this definition.

Key to providing the necessary security to these assets is the unification of the country's protection efforts. Although currently independent, the National Strategy advocates the consolidation and cooperation of the following agencies: the Critical Infrastructure Assurance Office (Department of Commerce), the National Infrastructure Protection Center (FBI), the Federal Computer Incident Response Center (General Services Administration), the Computer Security Division of the National Institute of Standards and Technology (Department of Commerce) and the National Communications System (Department of Defense).

The initiative also places heavy emphasis on the role of the private sector in taking primary responsibility for public safety risks posed by their industry. Government is to encourage firms to voluntarily share important and necessary information about the infrastructure under their immediate control. As a means to protect against inside threats to privately held critical infrastructure, the policy proposes national standards for screening and background checks, mandatory for personnel employed in the operation and use of such infrastructure.

Cyberspace and internet terrorism issues are set apart as a unique priority concern. To assess the nature of this threat, compose viable solutions, and recommend enforcement measures, the strategy grants authority through the National Strategy to Secure Cyberspace, governed by a joint steering committee with the Mexican and

Canadian governments. A multinational focused measure, the proposal partners with the international community to protect transnational infrastructure.

V. Defending Against Catastrophic Threat

Faced with the threat of proliferating weapons of mass destruction, the Strategy offers measures designed to mitigate the risks to the nation's human and structural resources. New inspection procedures are proposed for the national transportation systems. As for chemical and biological weapons (CBW) and agents, the guidelines stress the need for newer and more accurate devices for detecting deadly agents. Designed to address the biological threat, a public health surveillance system would monitor both public and private databases for indications of attack, allowing the information to become available to a wider range of experts who have extensive experience in diagnosis and treatment of these maladies. In tandem, the Center for Disease Control's Epidemic Intelligence Service—a program conducting epidemiological surveillance—would be expanded.

As a reactive preparedness measure, the initiative calls for the development and storage of a broad spectrum of vaccines, anti-microbials, and antidotes for use in the instance of a CBW attack. As part of the development of these vaccines, research into the possible effects of genetic engineering must also be considered. Expanding research into chemical and biological agents increases the risk of theft or misplacement of dangerous agents. In response, the proposal offers a stronger Select Agent Program that regulates the shipment of bio-organisms and toxins.

VI. Emergency Preparedness and Response

Unlike current provisions for emergency responses to federal incidents, the National Strategy's plan pushes for the coordination of response measures under one federal Incident Management Plan (IMP). The plan emphasizes the need for seamless communication among emergency responders, a factor missing from the disparate programs lacking centralization. Efforts would include a national emergency communication plan to establish protocols and standards for technology acquisition. All federal grant programs supporting the purchase of terror related communication equipment would be tied to this plan.

To create the federal Incident Management Plan, the strategy makes state adoption of the IMP a requirement for certain federal grant monies. It also encourages, as an additional cooperative device, state and local governments to sign mutual-aid agreements with each other in case of an emergency.

The strategy also provides for the assistance of military resources in civil emergencies. This is accomplished through the creation of U.S. Northern Command, a unified combatant command responsible for homeland security as pertaining to civil authorities. In conjunction, Operation TIPS—a government system allowing citizens to report suspicious activity—would be given greater emphasis.

Foundations of Homeland Security Defense: Implementation Techniques

I. Law

The National Strategy for Homeland Defense's appeal to the basic foundations for implementation breaks out into two components: the first proposes federal initiatives for

working within the pre-existing regulatory and legal framework, and offers some revisions to federal statutory regulations that would facilitate the new provisions; the second tackles the same on the state level.

For the federal sphere, the initiative proposes the narrowing of public disclosure laws in an effort to encourage the voluntary sharing of information between private sector and government. Flowing from the critical infrastructure objective, easing vague restrictions on disclosure may foster increased cooperation from owners of privately held key assets.

Some of the more major changes to federal law would include military assistance in domestic security measures. The strategy would allow military involvement in law enforcement activities within the nation's borders. The plan additionally seeks the reconstitution of the presidential reorganization authority. Amending Title 5, Chapter 9 of the United States Code would allow the President to reorganize the executive branch without congressional approval. Given the broad powers of the DHS, reorganization authority would be necessary.

For state initiatives, several provisions could facilitate the increased security of the citizenry. For example, a national minimum standard for driver's licenses could be adopted by state legislatures to make it more difficult for terrorists to duplicate the document. The strategy also suggests that states enhance market capacity for terrorism insurance with a regulatory approach that will allow businesses to share the risk. This is in-line with the Money Laundering Suppression Act which urges states to pass uniform money laundering statutes. The strategy also calls for a review of state quarantine provisions and authorities.

II. Science and Technology

"The Federal government needs to find better ways to harness the energy, ingenuity, and investments of private entities for [homeland security] purposes." As mentioned, the National Strategy calls for increased research into budding technologies to counter weapons of mass destruction, devices to detect hostile intentions, and viable biometric technology for identification purposes. Towards this end the proposal calls for a National Laboratory for Homeland Security to be located at the Nuclear Security Administration Laboratories.

Technology standards would be set by DHS, and would establish protocols for certification of state and local government and private sector technologies. The program also mentions the establishment of a "high-risk, high-payoff" homeland security research initiative.

III. Information Sharing and Systems

The strategy bases its information sharing and systems section on five principles: the balance of security with privacy; the homeland security community viewing federal, state, local and private sector involvement as one entity; the use of information for multiple purposes; the accurate keeping of a record's database; and the use of architecture of homeland security information as a dynamic tool.

The Critical Infrastructure Assurance Office would be created to implement these principles within the federal government for inter-agency structures. Likewise, the strategy urges state and local governments to use secure internet connections to exchange

data with the government, along with the adoption of common "meta-data" standards for electronic communications. The aggregate data would provide a broader picture of possible and suspected terrorist activity, perhaps adequate for detecting patterns and anomalies in time to prevent catastrophe.

For public disclosure of important information, the strategy recommends a "reverse 911" program where calls are placed to private citizens alerting them of potential threats, and instructing them in the proper course of action. For law enforcement personnel, Project SAFECOM, a wireless tactical infrastructure program, is encouraged.

IV. International Cooperation

Besides the cooperative efforts on internet and cyber terrorism, additional international initiatives include measures towards uniform standards for international documents, increased security of shipping containers, aid to foreign nations combating terrorism, burden sharing with other countries in response to attacks, and a review of international law to identify areas where improvement towards the defeat of terrorism can be made. The strategy encourages the use of Mutual Legal Assistance Treaties (MLATs) which allow the exchange of evidence permissible at trial.

Costs of Homeland Security and Priorities

This section outlines the economic and non-economic costs of the homeland security strategy. The allocation of costs will be guided by four principles: a reliance on cost-benefit analyses for maximizing outputs; a deference to market policies where best

equipped to deal with the needs of the country—government action will only be taken in areas where markets cannot provide the essential services; deference to federalism principles and cost sharing with the states; utilizing regulation as an incentive for cost minimization, and rewards for innovation. The strategy does not go into the specifics of how these principles will govern actual policy development, but stresses that these foundations will dictate the decisions regarding implementation.

The strategy predicts that the Fiscal Year 2003 costs of homeland security will weigh in at approximately $38 billion in federal funds. $24 billion will result from reductions in consumption, while the remaining $14 billion is scheduled from reduced private sector investments. State and local governments will also carry costs of improving their preparedness; these figures may be high as most states have little-developed response measures already in place.

The Strategy lists as its 2003 and 2004 priorities the following:

FY 2003:

-support for first responder teams: $3.5 billion
-defenses against bio-terrorism: $5.9 billion (an increase of $4.5 billion)
-border security and enforcement: $11 billion (an increase of $8.8 billion)
-information gathering and assessment: increased by $722 million

FY 2004:

-enhancement of analytical capabilities of the FBI
-creation of enhanced border security programs ("smart borders")
-shipping container security development
-Coast Guard re-capitalization
-immunization development and stockpiling for biological agents
-information sharing within federal levels

Potential Criticisms and Responses to National Strategy

Because of the necessarily broad scope and magnitude of the new policy proposals for homeland defense, some concerns have been raised from a number of

different groups as to the degree to which some measures extend. Particular areas question the role of civil liberties in investigatory procedures, while others wonder about the seemingly large increase in the federal government.

The formation of the DHS itself has raised concerns about broadening the size of the national government. With its twenty-two agency umbrella, the DHS is predicted to encompass an organization of roughly 170,000 employees nationwide, equipped with a budget of $37.4 billion. However, the DHS is not merely adding another 170,000 new employees to the federal employment pool, but rather is reorganizing existing resources—some of which are duplications of work done at another agency—in an effort at streamlining the security community's operations. Information sharing becomes much easier, coordination of special projects across agencies falls under the auspices of a central administration, and clear guidelines are created for interrelated operations that is lacking under the autonomous structure.

The proposed use of military in domestic operations has also been part of the criticism of the strategy. To allow such intervention, the abandonment of the Posse Comitatus Act of 1878 must occur—that act proscribing the use of military in domestic law enforcement capacities. Fears of military interventionism may discount the type of circumstances that would predicate their usage. The strategy further asserts that domestic preparedness and response efforts would benefit from greater input from military experience and advice.

Federalism claims might be raised with the government's leadership role in coordinating state and local programs. State Incident Management Plans, certification for state responders, and acquisitions of communications equipment are all tied to federal

grant monies. In response, the Administration proposes that its aversion to the creation of separate and specialized coordinating bodies for states and every functional area represents the recognition of the similarity between such a program and its predecessor. Too much control and too many separate federal agencies led to inefficient allocation of resources and the passing by of specialized knowledge by regional operatives.

Private sector concerns look to the voluntary disclosure principles and the background searches on personnel charged with the operation of critical infrastructure. Firms question the extent to which the voluntarily provided materials may be detrimental to the operation of their businesses (i.e., revelation of trade secrets, loss of competitive advantage, exposure to liability). The Administration assures that good faith disclosures will not expose the firms to any of the detrimental effects, and would be a purely cooperative venture for one specific goal of security. Private companies also express hesitancy, based on privacy concerns, about subjecting their employees to searching background checks.

Numerous times, the strategy mentions the storage and use of biometric identifiers. This information (fingerprints, retinal and iris scans, facial patterns) raises concerns over identity theft and privacy infringement. In response, the strategy counterclaims that a comprehensive database of biometric information is necessary to accurately verify the identities of terrorists before they can commit significant harm. Additionally, due to the remarkably individualized nature of these types of information, theft and replication are highly unlikely based on technology currently available.

The creation of Operation TIPS, which provides a channel for private citizens to alert the government as to suspected terrorist activity, has been viewed with skepticism

by some civil liberties organizations. Fears of neighbors spying on neighbors have been alleged as the result of such a policy. President Bush, however, assuages such fears and believes that individuals compose the largest first alert network in the nation. The program merely allows the channels to be set in place for reasoned review of suspicious activity. Much of this already exists as private citizens alert proper authorities when they believe dubious activity is occurring.

Finally, addressing the issue of unanimously adopted standards for drivers licenses, opponents claim that such document uniformity is tantamount to a national identification card. However, the program is voluntary at the state level, accompanies no tracking provisions by the federal government, and is designed to hinder the production of false documents by terrorists illegally moving about the country.