

108th Congress }
1st Session }

COMMITTEE PRINT

{ S. PRT.
108-33 }

STATE AND LOCAL OFFICIALS:
STILL KEPT IN THE DARK
ABOUT HOMELAND SECURITY

R E P O R T

PREPARED BY THE

MINORITY STAFF

OF THE

COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE



AUGUST 13, 2003

U.S. GOVERNMENT PRINTING OFFICE

88-843 PDF

WASHINGTON : 2003

COMMITTEE ON GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

| | |
|-------------------------------|----------------------------------|
| TED STEVENS, Alaska | JOSEPH I. LIEBERMAN, Connecticut |
| GEORGE V. VOINOVICH, Ohio | CARL LEVIN, Michigan |
| NORM COLEMAN, Minnesota | DANIEL K. AKAKA, Hawaii |
| ARLEN SPECTER, Pennsylvania | RICHARD J. DURBIN, Illinois |
| ROBERT F. BENNETT, Utah | THOMAS R. CARPER, Delaware |
| PETER G. FITZGERALD, Illinois | MARK DAYTON, Minnesota |
| JOHN E. SUNUNU, New Hampshire | FRANK LAUTENBERG, New Jersey |
| RICHARD C. SHELBY, Alabama | MARK PRYOR, Arkansas |

MICHAEL D. BOPP, *Staff Director and Chief Counsel*

JOYCE RECHTSCHAFFEN, *Minority Staff Director and Counsel*

MICHAEL L. ALEXANDER, *Minority Professional Staff Member*

BETH M. GROSSMAN, *Minority Counsel*

AMY B. NEWHOUSE, *Chief Clerk*

CONTENTS

| | Page |
|--|------|
| Executive Summary | 1 |
| Background | 1 |
| Recommendations | 2 |
| Introduction | 5 |
| Defining the Challenge | 6 |
| The Role of the Department of Homeland Security | 8 |
| An Urgent Agenda For Reform: State and Local Information Needs and How to Meet Them | 11 |
| <i>A Place at the Table</i> | 11 |
| <i>Timely Threat and Watch List Information</i> | 11 |
| <i>Two-Way Flow</i> | 13 |
| <i>Security Clearances</i> | 15 |
| <i>Special Case of Special Needs: Fire Fighters</i> | 18 |
| <i>Threat Advisory System</i> | 19 |
| Recommendations: Repairing the Federal-Local Information Breach | 20 |

STATE AND LOCAL OFFICIALS: STILL KEPT IN THE DARK ABOUT HOMELAND SECURITY

EXECUTIVE SUMMARY

BACKGROUND

America's safety demands that state and local officials, especially law enforcement and public safety professionals—our front line defenders—are fully engaged in the war against terrorism. Yet almost 2 years after the September 11, 2001 terrorist attacks, Governmental Affairs Committee (GAC) Minority staff found that these officials are being asked to fight the war against terrorism with incomplete and unreliable access to one of the most potent weapons in the homeland security arsenal: information.

State and local first responders and first preventers still do not systematically receive from the Bush Administration the information they need to prevent or respond to another catastrophic terrorist attack, nor does vital information flow effectively from them to the federal government. These information gaps pose a significant challenge for the federal government and leaves the American people at unacceptable risk.

This report contains the results of a staff investigation conducted at the request of Senator Joe Lieberman, Ranking Member of the Governmental Affairs Committee. Senator Lieberman asked GAC Minority staff to review the information needs of state and local officials and assess the progress of the Bush Administration in meeting those needs. Staff interviewed officials on the front lines in the fight against terrorism, while also reviewing reports, hearings, and other public information.

State and local officials told staff that what they want most is to have a seat at the table as the administration grapples with homeland security protection. They need reliable and timely information about terrorist threats, individuals on federal terrorist watch lists, and investigations of suspected terrorists in their jurisdictions. Several officials told staff there is currently no effective mechanism for allowing hundreds of thousands of local law enforcement officials to systematically provide information to, or receive information from, the federal government. And, the federal government has barely even acknowledged the information needs of our nation's local fire fighters. This is extremely troublesome, especially because fire fighters nationwide are most communities first line of defense against conventional, chemical, radiological, and biological attacks.

State and local officials also expressed frustration with the time it takes for them to receive security clearances necessary for access to classified information. And they believe that changes are needed in the color-coded Homeland Security Advisory System—a key piece of the federal government’s strategy to communicate with state and local officials, as well as the public, about terrorist threats.

Information that allows state and local officials to deter, prevent, mitigate, prepare, and if necessary respond to acts of terrorism—homeland security information—is difficult to quantify or define because it includes many different categories of information that is of varying interest to a host of different state and local officials. It ranges from publicly available information—for example about available federal resources to bolster homeland defenses—to highly classified intelligence information about terrorists available only to those with appropriate security clearances. Yet, understanding and systematically fulfilling these varying information needs—while also ensuring that state and local officials can provide information to the federal government—is crucial to our homeland defense.

The commitment has been made on paper. The administration’s “National Strategy on Homeland Security” released in July 2002 included information sharing and systems as one of “four foundations” of homeland security success. And several provisions in the Homeland Security Act of 2002 establish Congress’ intent to create a new paradigm of information sharing between the federal government and state and local agencies and officials.

But the Bush Administration’s rhetoric about making information sharing and systems a key to homeland security success has not translated into the kind of aggressive actions necessary to fundamentally change the status quo and protect the American people. The result of this lack of leadership is that many state and local officials—who also often lack the funding, training, and technology to counter terrorism—are left, if not entirely blind, straining to see the terrorist threat and how to respond to it.

RECOMMENDATIONS

The Bush Administration must act now and forge an effective partnership with state and local officials. It must provide the aggressive leadership necessary to replace state and local officials’ blindfolds with binoculars and to provide them with a seat at the homeland security table. Implementing the following recommendations will facilitate the information sharing necessary to create such a partnership:

1. Make Consolidated Federal Watch Lists Available to State and Local Law Enforcement Agencies

The President should immediately issue an Executive Order to consolidate terrorism watch lists; the Department of Homeland Security should oversee the consolidation of all federal terrorism watch lists and provide state and local law enforcement officials the ability to check names against a consolidated list by the end of this year. Sufficient resources must be made available, and senior officials held accountable for getting the job done.

2. Build Information Bridges Between States and Localities

DHS should encourage the creation of national and regional task forces (including multi-state task forces) as necessary (over the next year) to coordinate information sharing needs, bringing together state and local officials, including fire fighters, emergency management professionals, and police officers, as well as federal officials. These Task Forces should provide state and local officials a permanent “seat at the table” to ensure that information needs are addressed at all levels. DHS’s Office of State and Local Government Coordination should also create a best practice database allowing localities to share and compare solutions to homeland security problems.

3. Overhaul the Security Clearance Process

Provide the resources necessary to expedite security clearances for designated state and local officials—including appropriate fire officials—as nominated by governors and approved by DHS. Immediately assess the feasibility of requiring agencies to proactively recognize clearances issued by others for state and local officials, unless there are compelling security or law enforcement reasons not to do so. Establish a task force to review the security clearance process for state and local officials and report back in 6 months on ways to modernize it so that it meets the nation’s needs in the war against terrorism.

4. Create In-State 24-Hour Command Centers

Expedite the establishment of 24-hour operations centers in each state to provide connectivity and information sharing between the nation’s 650,000 local law enforcement officers and federal agencies.

5. Refine the Homeland Security Threat Advisory System

Immediately refine the Threat Advisory System to provide state and local officials specific information about terrorist threats and detailed guidance on how to respond to those threats. Put in place secure communications systems to inform key homeland security officials across the country of changes in the alert level and other information so they can start putting in place heightened protective measures.

6. Sharpen the DHS Office of State and Local Government Coordination (OSLGC)

Immediately equip OSLGC adequately and task it with overseeing state and local information sharing issues. The OSLGC must make it a priority to ensure that DHS and other federal agencies meet the information needs of state and local officials.

7. Judge Federal Officials Based on How Well They Share Information

Immediately revise federal agencies’ performance management systems to reward information sharing. Senior officials should be evaluated, in part, on their success or failure in breaking down barriers to sharing information. Bonuses should be dependent, in part, upon making measurable progress in improving information shar-

ing systems and processes, and special awards should be given to employees who demonstrate exemplary leadership and results in overcoming obstacles to sharing homeland security information.

8. Make Sharing Homeland Security Information a Top Priority

Immediately make sharing homeland security information with state and local officials a high priority for DHS and other key agencies; assign the Deputy Secretaries or Chief Operating Officers responsibility for overseeing implementation, monitoring, and reporting on agency progress.

INTRODUCTION

Since September 11, 2001, a consensus has emerged that to successfully defend against terrorism, federal agencies and officials must much more effectively share homeland security information with their state and local counterparts and receive from the “front lines” the vital information only those state and local officials can provide.

Numbers alone illustrate the need for successful collaboration. Some 11 million law enforcement officials and first responders—police officers, firefighters, public health professionals, emergency medical technicians, and others—are spread throughout America, with advanced training, intimate knowledge of their communities, and their ears always to the ground. In contrast, far fewer federal personnel are involved in homeland security. Many of these federal personnel—some 170,000—now work for the new Department of Homeland Security (DHS); approximately 11,500 work as FBI agents. But relatively few federal employees are “on the beat,” day after day, and in a nation this size, they constitute nowhere near the army needed to defend against the enemy in this unprecedented war on our home front. To the extent that we have a homeland security army, the overwhelming majority of foot soldiers on the front lines are from state and local governments.

The homeland security information they need is difficult to define precisely, or to quantify, because it includes many different categories of information that is of varying interest to a host of different state and local officials. It ranges from publicly available information—for example about available federal resources—to highly classified intelligence information available only to those with appropriate security clearances. It could be information about “best practices” in a given homeland security area that should be widely shared among elected officials, or sensitive, yet unclassified information of primary interest to law enforcement officials. Understanding and systematically fulfilling these varying information needs is crucial to homeland defense.

The Bush Administration does appear to be aware of the problem. In his letter accompanying the release of *The National Strategy for Homeland Security* in July 2002, President Bush states: “This is a national strategy, not a federal strategy.”¹ The strategy identifies “information sharing and systems” as one of four foundations essential to its success.

Despite this recognition, however, real progress has been slow. In October 2002, a non-partisan task force on homeland security sponsored by the Council on Foreign Relations and led by former Senators Gary Hart and Warren Rudman released its final report, “America Still Unprepared, Still in Danger.” It warned that 650,000 state and local law enforcement officers “continue to operate in a virtual intelligence vacuum, without access to terrorist watch lists provided by the U.S. Department of State to immigration and consular officials.”²

¹ George W. Bush, *National Strategy for Homeland Security*, introductory letter, July 2002. (<http://www.whitehouse.gov/homeland/book/nat-strat-hls.pdf>)

² Council on Foreign Relations, *America—Still Unprepared, Still in Danger*, October 2002, at 2. (<http://www.cfr.org/pdf/Homeland—TF.pdf>)

Because America's safety demands that state and local officials are fully engaged as quickly as possible in the fight against terrorism, Senator Lieberman asked staff for the GAC Minority to review the information needs of state and local officials and the progress the Bush Administration was making in meeting those needs. GAC staff subsequently interviewed officials who are on the front lines in the fight against terrorism, and reviewed reports, hearings, and other public information.

It quickly became clear that most police officers, fire fighters, and other first responders and first preventers continue to operate without the information they need from the federal government and have yet to be fully integrated into the President's recommended "national strategy" for homeland security. Though some progress has been made, the Bush Administration's stated commitment to making information sharing and systems one of its four foundations of homeland security success has thus far not been matched by the kind of action necessary to fundamentally change the status quo.

A considerable amount of attention is necessarily focused, at the moment, on establishing information sharing systems within DHS. The administration faces a tremendous challenge integrating information systems and sharing information just among the agencies being merged into the Department. However, this is not an "either/or" challenge. Federal agencies, led by DHS, must simultaneously and aggressively forge a new culture, along with effective processes and systems, for sharing information with state and local officials. But thus far, the leadership necessary to fully bridge some crucial information gaps has not been forthcoming.

The result of this lack of leadership by senior officials in the administration is that many state and local officials—who also all too often lack the funding, training, and technology to counter terrorism—are left, if not entirely blind, straining to see the terrorist threat and how best to respond to it.

DEFINING THE CHALLENGE

To defeat an enemy that operates on and targets our home soil, information must swiftly and reliably flow downstream from federal agencies to those officials in states and local communities who can act upon it. It must flow up—from states and localities to federal officials. It must move sideways—from states and localities to other states and localities that need vital information. And, at the same time, it must flow horizontally among the numerous federal agencies with homeland security responsibilities.

The reluctance of the federal intelligence community to allow information specific to the attacks of September 11, 2001 to flow downstream has been well documented. In December 2002, the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence Joint Inquiry (Joint Inquiry), stated:

Serious problems in information sharing . . . persisted, prior to September 11, between the Intelligence Community and relevant non-Intelligence Community agencies. This included other federal agencies as well as state and

local authorities. This lack of communication and collaboration deprived those other entities, as well as the Intelligence Community, of access to potentially valuable information in the “war” against Bin Ladin.³

An October 2002 report, “Protecting America’s Freedom in the Information Age,” prepared by a task force organized by the Markle Foundation, made clear that many months after the September 11 attacks, such problems still persisted:

Several federal agencies have relationships with state and local actors: the FBI and other federal law enforcement agencies communicate regularly with law enforcement personnel; FEMA has ties to state and local first responders; the Department of Health and Human Services interacts with the public health community. But sharing is ad hoc and inconsistent. The local entities often do not know what to share or with what federal agency they should share it. federal agencies often resist sharing information with state and local entities because of concerns about operational security and the potential for leaks.⁴

Cultural obstacles reinforce structural ones. At a GAC hearing on February 14, 2003, former Virginia Governor James Gilmore, who chairs the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, cited a “supreme and total distrust by the federal government authorities of the states and locals. The idea of sharing sensitive information with a police chief of a major jurisdiction or the governor of a state is anathema,” said Gilmore. “Progress is being made, but they are trying to break a cultural barrier and it is going to require dramatic leadership at the executive and congressional level to make that happen.”⁵

The International Association of Chiefs of Police (IACP) has also called attention to the anti-sharing cultures in federal agencies, and reports more specifically:

In some cases real, and in others only perceived, the hierarchical organization of law enforcement and intelligence agencies . . . leads to organizational incentives against intelligence sharing and even anti-sharing cultures. At best, the disaggregation of activity means that managers in one agency might not imagine that others would find their intelligence data useful. At worst, the structure creates an “us” versus “them” mentality that stands in the way of productive collaboration.⁶

³Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence Joint Inquiry into the Terrorist Attacks of September 11, 2001, *Final Report*—Part 1, December 10, 2002, at 8.

⁴Markle Foundation, *Protecting America’s Freedom in the Information Age*, A Report of the Markle Foundation Task Force, October 2002, at 70. (<http://www.markletaskforce.org/documents/Markle—Full—Report.pdf>) (Hereinafter “A Report of the Markle Foundation Task Force.”)

⁵Governor James Gilmore, Testimony, *Consolidating Intelligence Analysis: A Review of the President’s Proposal to Create a Terrorist Threat Integration Center*, Hearing Before the Governmental Affairs Committee, (S. Hrg. 108–54), February 14, 2003, at 20 (Printed Hearing Record Pending). (Hereinafter “Gilmore testimony, GAC Hearing, February 14, 2003.”)

⁶International Association of Chiefs of Police Criminal Intelligence Sharing Summit, Report Draft, March 2002, at 5.

Clearly, the Bush Administration must provide the aggressive leadership necessary for federal, state, and local governments to meet the challenge of sharing homeland security information with those who need it to secure our nation. As the Markle report noted, the intelligence and other information critical to homeland security “will come from across the country and around the world,” and while Washington, D.C. is a “critical node in that network,” it is “only one of many.” The report states: “To bring together this far-flung community of analysts and operators working directly on the problem is the real challenge.”⁷ It is a challenge from which we must not shrink.

THE ROLE OF THE DEPARTMENT OF HOMELAND SECURITY

In passing the Homeland Security Act of 2002 (P.L. 107–296) (HSA or Act), Congress recognized the need for focused, sustained, and committed leadership to build better bridges between the federal government and state and local officials. The Act charges the Secretary of Homeland Security with facilitating the sharing of information between the federal government, state and local government personnel, and the private sector.⁸

Three specific mandates in the Act are particularly relevant. First, the HSA establishes an Office of State and Local Government Coordination (OSLGC) in the Office of the Secretary and makes it responsible for: coordinating the activities of the Department relating to state and local government; assessing and advocating for the resources needed by state and local government to implement the national strategy; providing state and local government with regular information, research, and technical support; and developing a process for receiving meaningful input from state and local government to assist the development of the national strategy.⁹

Second, the HSA requires the President to prescribe and implement procedures for federal agencies to share homeland security information with other agencies—including DHS—and with appropriate state and local personnel. These procedures are to address both classified and unclassified information. Each federal agency is required to designate one official to administer these provisions. The President is required to report to Congress on the implementation of these procedures, with recommendations to increase the effectiveness of sharing information between federal, state, and local entities, not later than November 25, 2003.¹⁰ The Bush Adminis-

⁷ A Report of the Markle Foundation Task Force, at 11.

⁸ Homeland Security Act, Sec. 102(c). In addition to this requirement, Executive Order 13228 which established the Office of Homeland Security in October 2001 requires the Office to “coordinate the strategy of the executive branch for communicating with the public in the event of a terrorist threat or attack within the United States. The Office also shall coordinate the development of programs for educating the public about the nature of terrorist threats and appropriate precautions and responses.” (Executive Order 13228, Sec. 3(i) (October 8, 2001), 66 Fed. Reg. 51812 (October 10, 2001)).

⁹ Homeland Security Act, Sec. 801.

¹⁰ Homeland Security Act, Sec. 892. The Homeland Security Act recognizes the disparate and complex requirements for information in the fight against terrorism. Sec. 892(b)(1) states: “Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection (a), together with assess-

tration first issued an Executive Order delegating responsibility for prescribing the required procedures on July 29, 2003—9 months after the Act was passed, and 3 months before it is to report on its progress to the Congress.¹¹

Finally, the HSA also charges the intelligence unit within DHS with broad responsibilities for sharing homeland security information. These include: making recommendations to improve information sharing; administering the Homeland Security Advisory System; exercising primary responsibility for public advisories related to threats to homeland security; and providing advice about appropriate protective measures and counter measures to state and local government agencies and authorities, the private sector, other entities, and the public.

The Information Analysis and Infrastructure Protection Directorate (IAIP) of the new Department was created specifically to establish a central location to integrate, analyze, and disseminate intelligence information related to terrorist threats across all levels of government, especially including state and local governments.¹² The HSA also makes the IAIP responsible for “coordinating training and other support to the elements and personnel of the Department, other agencies of the federal government, state and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.”¹³

Rather than follow the mandate of the HSA and the recommendation of the Joint Inquiry to create an all-sources intelligence center within DHS,¹⁴ the administration has created a Terrorist Threat Integration Center (TTIC) that reports to the Director of Central Intelligence. Senator Lieberman, among others, has

ments of the credibility of such information.” Sec. 892(b)(2) further provides that each information system shall “(A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ; (B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient’s need to know such information; (C) be configured to allow the efficient and effective sharing of information; and (D) be accessible to appropriate State and local personnel.”

¹¹Executive Order 13311, “Homeland Security Information Sharing,” (July 29, 2003) assigns to the Secretary of Homeland Security most of the President’s responsibilities under Section 892 of the Act. Other functions are delegated to the Attorney General and the Director of Central Intelligence. 68 Fed. Reg. 45149 (July 31, 2003); see also <http://www.whitehouse.gov/news/releases/2003/07/20030729-10.html>.

¹²Homeland Security Act, Sec. 201(d)(8) and (9). The Act makes the Under Secretary for Information Analysis and Infrastructure Protection responsible, among other things, for reviewing, analyzing, and making “recommendations for improvements in the policies and procedures governing the sharing of law enforcement information, intelligence information, intelligence-related information, and other information relating to homeland security within the federal government and between the federal government and state and local government agencies and authorities.” The Under Secretary is also responsible for disseminating, “as appropriate, information analyzed by the Department within the Department to other agencies of the federal government with responsibilities relating to homeland security, and to agencies of state and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.”

¹³Homeland Security Act, Sec. 201(d)(16).

¹⁴*Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence Joint Inquiry into the Terrorist Attacks of September 11, 2001, Final Report—Recommendations*, December 10, 2002, at 4. The Joint Inquiry recommended that Congress and the Administration “ensure the full development within the Department of Homeland Security of an effective all-source terrorism fusion center that will dramatically improve the focus and quality of counter terrorism analysis and facilitate the timely dissemination of relevant intelligence information, both within and beyond the boundaries of the Intelligence Community.”

strongly criticized this decision for yielding to current cultural barriers rather than challenging them—and expressed concern that this arrangement may reinforce, rather than break down, information sharing walls with state and local officials. In a letter to President Bush on April 29, 2003, Lieberman wrote: “The fundamental problem is that by placing the TTIC under the command of the Central Intelligence Agency and not the Department of Homeland Security, it will be removed from our government’s daily efforts to improve domestic defenses, constrained by cultural and institutional rivalries between the CIA and the FBI, isolated from state and local governments, and unaccountable to the nation’s top homeland security official.”

Secretary Ridge defended the administration’s decisions relative to TTIC in a letter dated June 17, 2003—but, among other issues, he failed to adequately address one of Senator Lieberman’s key concerns: as constituted, the TTIC, under the Director of Central Intelligence, would not effectively incorporate state and local law enforcement into anti-terror intelligence activities. In a response, Senator Lieberman noted that one of the primary lessons from the September 11, 2001 attacks is that individuals outside the intelligence community, and even outside the federal government, might hold crucial pieces to the terrorist puzzle. He added, “we will have a much better chance of stopping attacks if the threat analysis center effectively integrates and utilizes the knowledge, skills, and information of those [including state and local law enforcement] outside the intelligence community.”¹⁵ The provisions in the HSA demonstrate Congress’ intent to create a new paradigm of information sharing between the federal government, state, local agencies, and officials.

In addition to the HSA, the President’s National Strategy for Homeland Security, the National Strategy to Secure Cyber Space, and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets also acknowledge the importance of information sharing and identify key responsibilities for DHS. For example, the National Strategy for Homeland Security cites the need for DHS to “integrate information sharing across state and local governments, private industry, and citizens.”¹⁶

To solve these information challenges, federal officials must be held accountable for overcoming traditional thinking that places federal agencies at the top of the hierarchal organizational pyramid with non-federal agencies viewed as untrustworthy or otherwise not suited to be full partners in the effort to secure the nation. Organizational incentives against intelligence sharing must be swiftly identified and discarded. Perhaps most important, as Congress clearly intended, the President, the Secretary of Homeland Security, and other senior administration officials must provide the leadership necessary to ensure that barriers to sharing information are systematically overcome.

¹⁵ Joseph I. Lieberman, letter to Secretary Tom Ridge, July 1, 2003.

¹⁶ Office of Homeland Security, *National Strategy for Homeland Security*, July 2002, at 57. See also General Accounting Office, GAO-03-715T, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, testimony of Robert F. Dacey and Randolph C. Hite Before the Committee on Government Reform, House of Representatives, May 8, 2003, at 25–26 (discussing the information-sharing responsibilities for DHS identified by each of the national strategy documents).

AN URGENT AGENDA FOR REFORM: STATE AND LOCAL INFORMATION NEEDS AND HOW TO MEET THEM

A Place at the Table

Governors, mayors, county officials, law enforcement officers, fire officials, medical, emergency management officials, and public health officials have general information needs in common, but also many demands that diverge significantly. For this reason, the Secretary must first and foremost ensure that state and local officials are fully included in the Department's decisionmaking process. Indeed, state and local officials told us that what they want most is to have a seat at the table as the administration grapples with homeland security protection.

For example, Major General Timothy Lowenberg, the Adjutant General of the State of Washington and the state's homeland security director, said that while he was included in discussions that helped shape the initial, broad national homeland security strategy (which the administration released in July 2002), he had not been consulted in the development of subsequent strategies on physical infrastructure security and cyber security, which were released in February 2003. Expressing a common refrain among those interviewed by Committee staff, Lowenberg said, "The only way the procedures [for information sharing] will be meaningful is if they bring us in."¹⁷

"Bringing them in" means more than occasional conference calls or interaction with federal officials based on personal relationships. State and local homeland security professionals interviewed by GAC staff emphasized the need for systematic and institutionalized communication and cooperation with federal officials. Yet these officials—especially law enforcement officers—more often credited personal relationships with federal officials (where they existed) rather than any well-developed system for sharing information with facilitating their exchange of information with the federal government to date.¹⁸ This is consistent with the findings of a November 2002 forum of federal and state law enforcement officials convened by the Police Executive Research Forum, a non-profit organization of law enforcement professionals. Participants in the forum "acknowledged that barriers to information exchange exist in all law enforcement agencies, and at every level," and emphasized the importance of making information sharing strategies intrinsic to organizations, not based on personal relationships.¹⁹

Timely Threat and Watch List Information

Localities and states need reliable and timely information about terrorist threats, about individuals on federal terrorist watch lists,

¹⁷ Staff Interview with Timothy Lowenberg, Adjutant General State of Washington, February 25, 2003 ("Lowenberg February 2003 Interview").

¹⁸ Staff Interview with John Skinner, Director, Intelligence Section, Baltimore Police Department, February 12, 2003 ("Skinner Interview"); Staff Interview with Karen Walton, Chief Operating Officer and other officials, New Haven, CT, March 5, 2003 ("Walton Interview"); Staff Interview with Benjamin Barnes, Director, Office of Public Safety, Health and Welfare, Stamford, CT, March 7, 2003.

¹⁹ Gerald R. Murphy and Martha R. Plotkin, Police Executive Research Forum, *Protecting Your Community From Terrorism: The Strategies for Local Law Enforcement Series*, March 2003, at 7.

as well as about the investigations of suspected terrorists within their jurisdictions.

Local law enforcement officials with whom GAC staff spoke described examples of being left out of the intelligence and information loop. Sheriff Ralph Ogden of Yuma County, Arizona, said he receives far too little information from federal intelligence on threats to specific targets or facilities in his jurisdiction.²⁰ Sheriff David Huffman of Catawba County, North Carolina told staff: “We need the details of the particular incident that caused the [terrorist threat] alert to be given in the first place.”²¹

Major General Lowenberg of Washington State told GAC staff that he too lacked sufficient intelligence and threat information from the federal government.²² Just as importantly, Lowenberg explained that state public health officials especially lack secure methods to communicate with the federal government. For example, he explained that, were the Centers for Disease Control or the Plum Island Animal Disease Center to confirm the presence of a plague, there would be no way to communicate that information to states except through open source, unsecured transmission methods. He said that, to date, there simply has been “no provision”—in terms of prioritization or resource allocation—for a secure communications infrastructure to share information about such biothreats with public health officials.²³

Some of the most vital streams of information to which state and local officials are not now privy are the 12 terrorism watch lists separately maintained by the State Department and 8 other federal agencies. Watch lists are basically automated databases—supported by analytical capabilities—that contain a wide variety of identifying data such as name, date of birth, and biographical data about suspected terrorists.²⁴ When utilized effectively, watch lists can be effective tools to keep terrorists out of our country or find them once they are inside our borders. In fact, we know today that 2 of the 19 September 11 hijackers should have been placed on the watch list as long as 20 months before the attacks.

However, as these databases are currently constituted, local officials cannot efficiently access them to detect potential terrorists once they may be within America’s borders. The reason is simple: nearly 2 years after September 11, the Bush Administration has yet to consolidate and integrate the watch lists maintained by different agencies, much less systematically share the information on them with appropriate state and local officials. Consequently, when making routine stops, police officers cannot search a consolidated federal watch list to determine whether an individual is suspected of terrorism.

²⁰ Staff Interview with Ralph Ogden, Sheriff, Yuma County, Arizona, February 24, 2003 (“Ogden Interview”).

²¹ Staff Interview with David Huffman, Sheriff, Catawba County, North Carolina, February 25, 2003.

²² Lowenberg February 2003 Interview, note 17 above.

²³ Staff Interview with Timothy Lowenberg, Adjutant General State of Washington, May 20, 2003 (“Lowenberg May 2003 Interview”).

²⁴ General Accounting Office, GAO-03-322, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, April 2003, at 3. (Hereinafter “GAO Report, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*”)

In an April 2003 briefing on the efforts to consolidate the information on these lists and make them available to local law enforcement agencies, GAC staff was informed that the administration has yet to even make a formal policy decision to consolidate the lists—despite the fact that CIA Director George Tenet testified to Congress twice, in June and October of last year, that a national watch list center was being created that would correct the failures and lapses of the past.²⁵

An April 30, 2003 report by the General Accounting Office (GAO) confirmed the lack of progress. GAO said that much of the data contained in the watch lists is still not being shared among federal agencies, much less with state and local law enforcement agencies. GAO found that terrorist watch lists compiled by nine federal agencies are frequently incompatible with one another and cannot be merged or compared easily. In addition, GAO stated that the agencies reported that they received no direction from the White House Office of Homeland Security identifying the needs of the government as a whole in this area. As a result, “Federal agencies do not have a consistent and uniform approach to sharing watch list information.”²⁶ In July 2003, a senior administration official reported to GAC Minority staff that there had been no progress towards consolidating the watch lists.

To protect the American people, state and local officials need access to this information—and from a single source. For example, Sheriff Ogden said he needs a “clearinghouse for federal databases, a one-stop-shop” where he can get information about deportations, prosecutions, and apprehensions by the Border Patrol. Now, he and other local law enforcement officials around the country have to try and access many different databases. However, they need the ability to find out immediately if someone who has been stopped in their jurisdiction is of interest to other agencies.²⁷

Two-Way Flow

Local officials can and must be much more than recipients of information. Our 650,000 law enforcement officers nationwide should be leveraged by the federal intelligence and law enforcement authorities as hunters and gatherers of intelligence—as “force-multipliers.” After all, these local officials know the people and vulnerabilities within their communities; they know the norms and consequently understand what is not normal; and they encounter individuals during routine activities that may also be of legitimate interest to federal agencies. Any successful information sharing strategy, therefore, must focus both on pushing vital counter terrorism intelligence and information quickly and effectively upstream from the thousands of state and local officials to the feds, as it does sending data downstream.

²⁵ George Tenet, written testimony, Senate Select Committee on Intelligence and House Permanent Committee on Intelligence Joint Inquiry into the September 11, 2001 Terrorist Attacks, June 18, 2002, at 19, and October 17, 2002, at 18. (Testimony available in the Governmental Affairs Committee files.)

²⁶ GAO Report, *Information Technology, Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, note 24 above, at 17.

²⁷ Ogden Interview, note 20 above.

Yet, several officials told us there is currently no effective mechanism allowing hundreds of thousands of local law enforcement officials to systematically provide information to or receive information from the federal government. To fix this serious flaw, in February Senator Lieberman called for the establishment of a 24-hour operations center in each state that would serve as a conduit for sending information from local officials to the federal government and back—a suggestion made by James Kallstrom, formerly a 28-year veteran of the FBI and currently Senior Executive Vice President at MBNA Bank America and Senior Advisor for Counter Terrorism to the Governor of New York. Kallstrom contends that the vast majority of the nation’s local law enforcement officers “are virtually not a part of the war against terrorism.”²⁸

To facilitate communication with local law enforcement, the FBI has established some 66 Joint Terrorism Task Forces (JTTFs) around the country, which typically consist of representatives of federal, state, and local law enforcement agencies working together to deter, counter, or respond to acts of terrorism. The JTTFs play an important role in allowing law enforcement information to be exchanged and investigations to be coordinated across different jurisdictions and levels of government. However, GAC staff was informed by some officials that while JTTFs are useful, they do not provide information to many state and local law enforcement officials who are critical in the war against terrorism. JTTFs are not helpful to many of the police officers who must be engaged in combating terrorism because the classified information JTTFs handle cannot be shared with those who lack security clearances; and systems to declassify, where appropriate, and share the information are not in place.

For example, in New York State, JTTFs include about 250 police officers. However, approximately 69,000 others are not part of the task forces. Kallstrom believes that we need to “train and provide relevant information to the rest of the cops.” He said that nationally, “we’re not asking or tasking or allowing 99.9% of police to have any impact in counter terrorism.”²⁹

The federal government must also take steps to facilitate the flow of homeland security information among other jurisdictions. Terrorist attacks pay no heed to distinctions or boundaries between state and local jurisdictions. However, to protect the public, state and local governments must overcome walls of separation among themselves. For example, Major General William Cugno, the Adjutant General of Connecticut who has lead agency responsibility for developing and coordinating counter terrorism and domestic preparedness for the state, said that even though Connecticut is next to New York, there is currently no forum where officials of the two states can systematically share emergency operations and management information. Although both states participate in and share information through national organizations, such as the National Emergency Management Association and the Adjutant General’s Association, Cugno said more direct participation and interaction is lacking. He noted, for example, that while Connecticut would be

²⁸ Staff Interview with James Kallstrom, Senior Advisor for Counter Terrorism to the Governor of New York, February 27, 2003 (“Kallstrom Interview”).

²⁹ *Id.*

greatly affected by an evacuation of New York City, there are no coordinated efforts, resources, or requirements that would include Connecticut in New York's evacuation planning.³⁰ With over 50,000 state and local jurisdictions in America, the task of coordinating various domestic defense information requirements demands strong federal leadership.

The Markle Foundation recommends establishing task forces that include "all key actors from the federal, state and local governments and the private sector to facilitate local, real and virtual communities" and a central leadership role for the DHS.³¹ The report states:

First, states must begin organizing themselves to gather and share information more effectively. Second, the federal government needs one entity responsible for coordinating its role in this effort. . . . There currently is no coordinated strategy in the federal government for interaction with state and local entities.³²

A critical need is for mechanisms to ensure that state and local jurisdictions do not waste precious time and resources by unnecessarily reinventing the wheel. For example, Jack Weiss, a Los Angeles City Councilman, told GAC staff that local officials are often left to figure out complex homeland security challenges without the benefit of knowing what is happening in other areas. He believes OSLGC at DHS should help overcome this challenge by actively facilitating the sharing of best practices.³³

Security Clearances

The challenge of sharing homeland security information with state and local officials cannot be met without dramatic changes in the procedures the government now uses to grant security clearances. The security clearance process—designed to determine access on a need-to-know basis to classified national security information—has been focused mostly on federal employees, applicants, and contractors. Until now, state and local officials haven't had a significant place in the process. But the war on terrorism has changed the landscape. According to the Congressional Research Service (CRS), addressing this new situation means providing official security clearances for non-federal officials and elected public officials at any level as standard policy, requirements that are "unprecedented in their scope."³⁴ A report by CRS explains:

Because of the absence of standardized security clearance requirements, high-ranking state and local public officials—mayors, municipal chiefs of police, county execu-

³⁰ Staff Interview with William Cugno, Adjutant General State of Connecticut, May 29, 2003.

³¹ A Report of the Markle Foundation Task Force, note 4 above, at 51.

³² *Id.*, at 75.

³³ Staff Interview with Jack Weiss, Los Angeles City Councilman, February 5, 2003. Some of the other officials with whom GAC staff spoke noted that some best practices information was already being collected by disparate organizations, including police and firefighters' associations and the National Governors Association's Center for Best Practices. OSLGC could play an important role in pulling this information together in one place.

³⁴ Frederick M. Kaiser, Congressional Research Service, *Access to Classified Information: Seeking Security Clearances for State and Local Officials and Personnel*, Government Information Quarterly, forthcoming Summer 2003. (Hereinafter "Frederick M. Kaiser, CRS, *Access to Classified Information*").

tives, sheriffs, and even governors, in some instances—have been denied certain information; and those who have received it may not have been able to share it with their colleagues, even officials who otherwise outranked or supervise them. This condition has existed, in large part, because their need for classified national security information has been narrow and circumscribed—confined, for instance, to nuclear weapons facilities or certain defense establishments within their jurisdictions. The heightened priority to combat terrorism, by contrast, has broadened the boundaries.³⁵

The National Governors Association’s Center for Best Practices has also cited the need for expanded access to information, stating: “Governors and other high-ranking officials must receive timely and critical intelligence related to terrorist threats. Granting security clearances to certain state and local personnel using a compartmented, need-to-know system would facilitate securing sharing of critical intelligence.”³⁶

Congress recognized this necessity in the HSA, which states, “The needs of state and local personnel to have access to relevant homeland security information to combat terrorism must be reconciled with the need to preserve the protected status of such information and to protect the source and methods used to acquire such information.” The HSA notes that granting security clearances to certain state and local personnel is one way to facilitate the sharing of information regarding specific terrorist threats among federal, state, and local levels of government.³⁷ The Act requires the President to prescribe procedures under which federal agencies may share classified homeland security information with appropriate state and local personnel, and expresses the sense of the Congress that such procedures may include “carrying out security clearance investigations with respect to appropriate State and local personnel.”³⁸

GAC staff interviews with state and local officials revealed their continuing frustration over the lack of security clearances and therefore, their limited access to classified information.

The problem has reached as high as governors’ mansions. Former Virginia Governor Gilmore testified at a Joint Inquiry hearing on October 1, 2002 that, in his 4 years as Governor (1998–2002), he never received any intelligence or law enforcement information regarding terrorists and never received a security clearance that would have allowed him to be briefed on possible terrorist plots.³⁹

A leading emergency management official in one state provided a stark example of why urgent change is needed: a critical private sector asset whose disruption by terrorists would cause tremendous damage to the nation is located in his state. He is aware of this because he has the appropriate security clearances. Yet, the official

³⁵ *Id.*

³⁶ National Governors Association, *NGA Center for Best Practices, States Homeland Security Priorities*, Issue Brief, August 9, 2002, at 2.

³⁷ Homeland Security Act, Sec. 891(a)(5) and (6).

³⁸ Homeland Security Act, Sec. 892(c)(1) and (2).

³⁹ Governor James Gilmore, Testimony, Senate Select Committee on Intelligence and House Permanent Committee on Intelligence Joint Inquiry, October 1, 2002, unpublished transcript at 135. (Testimony available in the Governmental Affairs Committee files.)

was not able to inform the governor of the vulnerability because more than a year and a half after being elected to office, the governor was still awaiting appropriate clearances.⁴⁰

The security clearance gaps frustrate common-sense efforts to safeguard significant vulnerabilities. According to Major General Timothy Lowenberg, the Adjutant General of Washington State, even if he were to receive classified information about a bio-threat, he would not be allowed to share it with the top public health official in his state because that official does not have the required security clearances. He also noted the irony that, while the Federal Emergency Management Agency (FEMA) has funded equipment for secure audio, video, and data communications in state emergency operations centers, as well as installed secure equipment for governors, in many cases the equipment cannot be used because too few state emergency management officials have clearances.⁴¹

As noted earlier, an important link between state and local law enforcement is the FBI's JTTFs. But their usefulness is limited because governors, mayors, attorneys general, many other law enforcement officers, fire fighters, and others who sometimes need access to classified information are typically not included in JTTFs.

Another problem is how quickly and efficiently the clearances are approved. For years, the security clearance approval process has been beset by bureaucratic complexity and delays which now frustrate the ability of federal officials to leverage the strengths of state and local law enforcement, and vice versa. Reports by CRS, the GAO, the Department of Defense Inspector General, and others have documented a host of concerns, including: a sizeable and growing backlog in background investigations; substantial and rising costs in time and resources associated with such investigations; failure to comply with investigative standards; duplications and delay in adjudications; and continued outdated and disjointed governing authorities and the resulting confusion for both administrators and applicants.⁴²

The Bush Administration asserts that it is making progress in clearing up the backlog of security clearance applications. For example, at a February 26, 2003 GAC hearing, Pasquale J. D'Amuro, Executive Assistant Director of the FBI for Counterterrorism, said that the Bureau had received over 1,200 requests for Top Secret level security clearances from state and local law enforcement officers and approved 936 of them for officers working in the Bureau's JTTFs.⁴³ Governors have also now signed non-disclosure agreements with DHS, allowing them to receive certain classified information over secure equipment that has been installed using grants from FEMA. FEMA is also working on clearances for state homeland security advisors.

However, much more remains to be done. For example, many state and local officials do not realize—until learning it through difficult experience—that a high-level clearance issued by one fed-

⁴⁰ Staff Interview with Emergency Management Official, February 2003.

⁴¹ Lowenberg May 2003 Interview, note 23 above.

⁴² Frederick M. Kaiser, Congressional Research Service Memorandum, *Security Clearance Program: An Overview*, February 27, 2003, at 10.

⁴³ Pasquale J. D'Amuro, Testimony, Senate Governmental Affairs Committee Hearing, *Consolidating Intelligence Analysis: A Review of the President's Proposal to Create a Terrorist Threat Integration Center*, (S. Hrg. 108-54) February 26, 2003, at 58 (Printed Hearing Record Pending).

eral agency does not mean that the individual is cleared for all agencies. A March 2003 report by the Police Executive Research Forum cited the example of one local official who had two federal security clearances, but not one from the FBI. As a result, the FBI would not share classified information with him. Another executive had a Top Secret clearance from the National Guard, but only a Secret clearance from the FBI. The report did note that, as a result of the session, participants learned “that is it possible to have one federal agency transfer its security clearance to another federal agency immediately if the applicant makes a request.”⁴⁴

At a May 15, 2003 GAC hearing, Governor Mitt Romney of Massachusetts recommended that security clearances be standardized—perhaps within DHS—and made reciprocal between agencies and levels of government. Romney also recommended that the process for federal security clearances should be expedited.⁴⁵ Clearly far too little, if any, progress has been made on these recommendations.

Special Case of Special Needs: Fire Fighters

GAC staff found that the federal government has barely even acknowledged the information needs of our nation’s local fire fighters. This is extremely troubling, especially because fire departments nationwide are most communities’ first line of defense against conventional, chemical, radiological, and biological attacks; many of their needs for advanced equipment and training also have not been met; and budgetary strains are stretching the personnel and resources of these departments thinner than ever.

Peter Gorman, a captain in the Fire Department of New York, pointed out that while fire fighters are often the first of the first responders to arrive after an incident, they are typically not brought into the information loop until after they are called upon to respond. Gorman used the example of a potential attack with a “dirty bomb” or the release of poison gas in a subway: if intelligence agencies have reason to believe that such an attack could occur, fire fighters need to know in advance to effectively prepare and deploy resources for the eventuality. He believes that senior fire officials—not just those who have law enforcement powers—should also have top-level security clearances and participate in JTTFs.⁴⁶

Major Marc Bashoor, Commander of the Prince George’s County, Maryland Fire Department’s Special Operations Division, expressed similar sentiments. He agreed that many fire fighters with a need to know are “not in the loop.” Bashoor explained that even though he is head of the County’s hazardous materials and bomb squad, he cannot receive classified intelligence information: for example, he is not eligible to receive classified information about the latest mechanisms terrorists may be using to deliver explosives. He said a fire detective with law enforcement powers represents the

⁴⁴ Murphy and Plotkin, *Police Executive Research Forum Report*, March 2003, at 22.

⁴⁵ Mitt Romney, written testimony, Governmental Affairs Committee Hearing, *Investing in Homeland Security: Challenges Facing State and Local Governments*, (S. Hrg. 108–83), May 15, 2003, at 9. (Printed Hearing Record Pending)

⁴⁶ Staff Interview with Peter Gorman, Captain, Fire Department of New York, February 26, 2003.

department on the JTTF, but that the representative typically cannot share what he learns. Bashoor does not believe fire fighters need information about terrorism investigations (the primary information shared in JTTFs), nor does every fire fighter necessarily need certain intelligence information. But current obstacles, especially lack of security clearances, leave many that do have a need to know out of touch. Bashoor noted that knowledge about the weapons that terrorists plan to use eventually may be shared in training sessions—but it may take “a year or two” before the information is included. Right now, he said, information that would be very useful to bomb squads and hazardous materials teams “just doesn’t get to us.” Bashoor is not aware of any federal initiatives to understand, much less address, these information needs.⁴⁷

Threat Advisory System

The color-coded Homeland Security Advisory System is a key piece of the federal government’s strategy to communicate with state and local officials, as well as the public, about terrorist threats. Yet GAC staff interviews with these officials made clear that, as currently implemented, the present system operates more like a blunt instrument than a sharp information tool. A change in the alert level may now raise officials’ general “level of vigilance,” but without more pointed information on what prompted the change or more specific federal instructions on precise steps that might be taken to protect people from the threat, state and local officials are limited in knowing where to focus their efforts.

Officials in New Haven, Connecticut stressed that they needed a description of the reason the alert level has been elevated and that officials at the local level needed to know what a change in alert status means to them.⁴⁸ As John Skinner, Director of the Intelligence Section of the Baltimore Police Department summed it up, the limited information currently provided by the alert is simply “not actionable.”⁴⁹

Another troubling aspect of the current alert system is how word of it travels—or fails to travel. At an April 9, 2003 GAC hearing on homeland security challenges facing first responders, witnesses—including the Police Chief of Dover Delaware, Fire Chief of Arlington, VA, and a Prince Georges County, MD Fire Captain—all indicated that they first heard the alert level was being raised in March through the news media, rather than through official channels.⁵⁰

After terrorist attacks killed over 75 people in Saudi Arabia and Morocco, the alert level was raised from Code Yellow to Orange, for the fourth time, on May 20, 2003. As CNN reported the news, it noted that officials were at that very moment contacting state and local officials to inform them of the decision. Clearly, the internal distribution channels necessary to fully and timely inform those of-

⁴⁷ Staff Interview with Marc Bashoor, Commander Special Operations Division, Prince George’s County, Maryland Fire Department, May 19, 2003.

⁴⁸ Walton Interview, note 18 above.

⁴⁹ Skinner Interview, note 18 above.

⁵⁰ Jeffrey Horvath, Ed Plaugher, Chauncey Bowers, Testimony, Governmental Affairs Committee Hearing, *Investing in Homeland Security, Challenges on the Front Lines*, (S. Hrg. 108–82), April 9, 2003, at 31.

officials with key homeland security responsibilities about heightened terrorist threats still have not been established. This leaves local officials in a reactive, not proactive, mode from the very start.

RECOMMENDATIONS: REPAIRING THE FEDERAL-LOCAL INFORMATION BREACH

The Bush Administration must act now and provide the aggressive leadership necessary to replace state and local officials' blindfolds with binoculars and to provide them with a seat at the homeland security table. America needs a proactive, energized, and well-informed front line of defense that works in seamless partnership with the federal government in order to protect its people from terrorism. Implementing the following recommendations will facilitate the information sharing necessary to create such a partnership:

1. Make Federal Watch Lists Available to All State and Local Law Enforcement Agencies.

CHALLENGE: The frontline "first preventers" in the war against terrorism lack simple, streamlined access to the federal databases that are most valuable in the effort to identify and apprehend terrorists.

All units in post-war Iraq were given a pack of playing cards with the names and faces of top officials from Saddam Hussein's regime and the Ba'ath party. Yet, with a constantly changing roster of suspects to potentially apprehend, the frontline soldiers in the war against terrorism here at home are not provided with clear and simple access to federal terrorism watch lists. Twenty-one months after the September 11, 2001 attacks, the administration still has yet to consolidate the 12 watch lists maintained at 9 different agencies, frustrating the efforts of state and local law enforcement, and federal officials, to readily access the information they contain. It is imperative that the administration makes these issues a priority, set a timetable for completion, and ensure accountability.

RECOMMENDATION: The President should immediately issue an Executive Order to consolidate terrorism watch lists; the Department of Homeland Security should oversee the immediate consolidation of all federal terrorism watch lists and provide state and local law enforcement officials the ability to check names against a consolidated watch list by the end of this year. Specific goals and timetables must be set, resources made available, and senior officials held accountable for getting the job done.

2. Build Information Bridges Between States and Localities.

CHALLENGE: States and localities still operate far too much as information islands, in relative isolation from their neighbors. Cities, counties, and states also have few resources to learn what their counterparts around the country are doing to effectively protect their localities.

To ensure that homeland security information is shared effectively, the federal government must also help to establish mechanisms to build information bridges among states, and among states and localities. This includes ensuring that best practices are documented and shared, facilitating the establishment of mutual aid agreements which cross states and jurisdictions, and providing fora where state and local officials can work closely with each other, and with federal officials, to identify and systematically address all homeland security information sharing needs.

RECOMMENDATION: Charge DHS with encouraging, over the next year, the creation of national and regional task forces (including multi-state task forces) as necessary. These task forces should bring state and local officials, including fire fighters, emergency management professionals, and police officers, as well as federal officials, together to coordinate their information sharing needs and provide state and local officials a permanent seat at the table to ensure that information needs are addressed at all levels. DHS's Office of State and Local Government Coordination should also create a best practices database allowing localities to share and compare solutions to homeland security problems.

3. Overhaul the Security Clearance Process

CHALLENGE: Many state and local officials who need high-level information access lack the necessary federal security clearances to do what their job—and our safety—demands.

The current processes for providing security clearances are burdened by backlogs; various agencies do not routinely recognize clearances issued by others; and key state and local officials must often wait months before a clearance is granted. In essence, the security clearance process that served our nation when the primary threats were abroad must be reoriented to address information sharing challenges in the war against terrorism.

RECOMMENDATIONS: Provide the resources necessary to expedite clearances for designated state and local officials—including appropriate fire officials—as nominated by governors and approved by DHS. Immediately assess the feasibility of requiring agencies to proactively recognize clearances issued by others for state and local officials, unless there are compelling security or law enforcement reasons not to. Establish a task force to review the security clearance process for state and local officials and report back in 6 months on ways to modernize it so that it meets the nation's needs in the war against terrorism.

4. Create In-State 24-Hour Command Centers

CHALLENGE: States lack a single point of contact for both receiving “downstream” information needs

and pushing intelligence and other information “upstream.”

New York’s Counter Terrorism Advisor, James Kallstrom, has urged creation of 24-hour command centers in each state to serve as hubs merging police on the front lines with state and federal agencies, especially DHS. Construction of such a center is now underway in New York. Similarly, the State of Georgia, with some federal funds from the Justice Department, has created the Georgia Information Sharing and Analysis Center. Its priority is to organize existing state and local law enforcement resources into a statewide intelligence gathering and sharing network.⁵¹ As Kallstrom points out, to be effective, these centers must be closely coordinated with federal agencies through DHS.⁵²

RECOMMENDATION: Expedite the establishment of 24-hour operations centers in each state to provide connectivity and information sharing between the nation’s 650,000 local law enforcement officers and federal agencies.

5. Refine the Homeland Security Threat Advisory System

CHALLENGE: The current advisory system offers little guidance to local officials on what specific steps they should take to guard against specific threats.

The Homeland Security Advisory System, which the administration itself admits is still a work in progress, may raise and lower officials’ general level of vigilance, but without more specific information or instructions from the federal government on precise steps that might be taken to protect people from the threat, state and local officials do not know where to focus their efforts. The system should be revamped so that officials are provided with actionable intelligence. DHS also needs to ensure that officials at the state and local level with a need to know have a swift and reliable channel to receive information so that they can start putting in place heightened protective measures.

RECOMMENDATIONS: Immediately refine the Threat Advisory System to provide state and local officials specific information about terrorist threats and detailed guidance on how to respond to those threats. Put in place secure communications systems to inform key homeland security officials across the country of changes in the alert level.

6. Sharpen the DHS Office of State and Local Government Coordination

CHALLENGE: Strong and consistent leadership is necessary to overcome cultural barriers to sharing information with state and local officials. DHS must make this an explicit priority, especially for the Office of State and Local Government Coordination.

⁵¹State of Georgia, Department of Public Safety, October 9, 2002. (<http://www.gahomeland-security.com>)

⁵²Kallstrom Interview, note 28 above.

While the office is now functioning, its overall budget, staff resources, plans, and priorities are as yet unclear. The office has not yet demonstrated a clear capacity to foster the kind of fundamental changes necessary to create a new information-sharing paradigm. The administration must act to ensure that OSLGC receives sufficient staff and budgetary resources, and bureaucratic clout, to vastly improve the sharing of information with state and local governments. The office must work closely with the Information Analysis and Infrastructure Protection Directorate—which is responsible for disseminating intelligence analysis to state and local officials, and coordinating training and other support to these officials to assist them as information sharers and consumers—to ensure that this vital national priority is addressed.

RECOMMENDATION: Immediately equip OSLGC for, and task it with, overseeing state and local information sharing issues. The OSLGC must make it a priority to ensure that DHS and other federal agencies meet the information needs of state and local officials.

7. Judge Federal Officials Based on How Well They Share Information

CHALLENGE: To overcome cultural and other barriers to effectively sharing information with states and localities, DHS and other agencies must hold senior officials accountable for achieving results while providing positive incentives to motivate change.

Without changing the system of accountability—so that agency officials' performance is graded, in part, based on how well they share—it will be impossible to fundamentally change the status quo. When Governor Gilmore testified before GAC about the proposed Terrorist Threat Integration Center, he stated: "There is going to have to be an understanding that information of this type of sensitive nature is going to have to be shared. If it is not shared, then there should be penalties connected with the non-sharing."⁵³ Agencies seeking to improve the sharing of information have also learned that employees must be positively motivated and are establishing incentives to achieve results—including employee recognition programs.⁵⁴

RECOMMENDATION: Immediately revise federal agencies' performance management systems to reward information sharing. Senior officials should be evaluated, in part, on their success or failure in breaking down barriers to sharing information. Bonuses should be dependent upon making measurable progress in improving information sharing systems and processes and special awards should be given to employees who demonstrate exemplary leadership

⁵³ Gilmore testimony, GAC Hearing, February 14, 2003, note 5 above.

⁵⁴ Sara Michael, "Knowledge Hoarding: Agencies find incentives can encourage the reluctant to share what they know." *Federal Computer Week*, April 28, 2003.

and results in overcoming obstacles to sharing homeland security information.

8. Make Information Sharing a Priority, Track and Monitor Progress

CHALLENGE: Meeting the complex challenge of sharing homeland security information with state and local officials requires sustained and focused leadership by the Secretary of Homeland Security and other top administration officials.

The Bush Administration has cited five government-wide goals, and several agency-specific goals, in its so-called “management agenda” that identifies its top priorities for federal agencies. These agenda items—including counterproductive ideas like establishing mandatory quotas for systematically privatizing federal employees’ jobs—receive high-level attention from senior administration officials. The chief operating officers in each agency, typically the Deputy Secretaries, have been delegated responsibility for the agenda, and progress is tracked by periodically grading agencies’ performance as green (indicating successful progress is being made); yellow (indicating mixed results); and red (for unsatisfactory performance). The challenge of sharing homeland security information, which the Bush Administration has identified in its national strategy and is vital to governments’ ability to protect the American people, must be elevated to the highest priority status within the administration. Progress must be systematically monitored and tracked—and agencies should be graded on their performance.

RECOMMENDATION: Make sharing homeland security information with state and local officials a high priority for DHS and other key agencies; assign the Deputy Secretaries or Chief Operating Officers responsibility for overseeing implementation, monitoring and reporting on agency progress.

