Backgrounder

Published by The Heritage Foundation

No. 1826
February 24, 2005

An Agenda for Increasing State and Local Government Efforts to Combat Terrorism

James Jay Carafano, Ph.D., Paul Rosenzweig, and Alane Kochems

State and local governments have a critical role to play in combating terrorism, but too much emphasis has been placed on preparing them to respond to terrorist acts and not enough on enhancing their ability to prevent attacks on U.S. citizens. The Department of Homeland Security (DHS) should address this imbalance by establishing a national program to enhance state and local capacity to fight terrorism.

While the Bush Adminstration's effort to consolidate the Law Enforcement Terrorism Prevention Program grants into the general state grant program is worthwhile, part of what relaces it should be a set of targeted initiatives. Specifically, such a plan would focus on improving information analysis capabilities, strengthening the means of state and local law enforcement to conduct terrorism-related immigration investigations, maintaining strong legal authority for information sharing, and establishing a template for state intelligence operations. Any national effort must also respect the principles of federalism.

The DHS should implement this plan with support from the Department of Justice (DOJ), and establishing an agenda for these efforts ought to be one of the first priorities for the new Secretary of Homeland Security.

Building a National Homeland Security System

Strategic threats such as transnational terrorism require well-thought-out and well-designed strate-

Talking Points

- The best way to respond to a terrorist attack is to prevent it from ever happening. States and local governments can assist significantly in prevention and do it in a way that respects the principles of federalism and American citizens' constitutional rights and privacy.
- The Department of Homeland Security should establish a national plan aimed at enhancing state and local capacity to fight terrorism.
- The plan should focus on improving information analysis capabilities, strengthening the means of state and local law enforcement to conduct terrorism-related immigration investigations, maintaining strong legal authority for information sharing, and establishing a template for state intelligence operations.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/bg1826.cfm

Produced by the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

gic responses. As one of its first initiatives, the Administration developed a national homeland security strategy. The strategy identifies six major mission areas:

1. Intelligence and warning,
2. Emergency preparedness and response,
3. Domestic counterterrorism,
4. Critical infrastructure and key asset protection,
5. Defense against catastrophic threats, and
6. Securing the borders and transportation system.[1]

State and local governments have a major role to play in the first three areas.

Building the right homeland security system to support the strategy will take time. Any homeland security system must be national, not just federal. To be truly comprehensive, the system must have a strong state and local component. State and local participation is important for two reasons. First, it protects the principles of federalism. Second, it ensures that the system is sustainable over the long term both because it has financial support and because states "buy in" to its importance. However, this also means that state and local governments must fulfill their responsibilities and obligations.

The current effort to create a national homeland security system has encountered a number of difficulties. As the Gilmore Commission noted, "a lack of clear strategic guidance from the Federal level about the definition and objectives of preparedness and how States and localities will be evaluated in meeting those objectives" has led to inconsistent preparedness levels and the creation of divergent plans.[2]

Another problem is the lack of intelligence and information sharing.[3] This comes in a number of different forms. Exchanges of classified information inevitably raise concerns because many of the individuals involved in homeland security lack security clearances. Private industry is hesitant to share proprietary and sensitive business information. In addition, information tends to travel in only one direction—from the states to the federal government—instead of being exchanged.

The federal government's first and highest priority should be to invest in creating a truly national system of homeland security—not merely in supplementing the needs of state and local governments. Federal efforts should focus on programs that will make all Americans safer. That includes providing state and local governments with the capability to integrate their counterterrorism, preparedness, and response efforts into a national system as well as expanding their capacity to coordinate support, share resources, and exchange and exploit information. In addition, the federal government should improve its own capacity to increase situational awareness of national homeland security activities and to shift resources where and when they are needed.

Misplaced Priorities

The federal government is not close to producing the system that America needs. Current programs place too much emphasis on response and expanding the capacity of local emergency responders. Instead, funding should go to creating a truly national prevention system with a robust capability for state and local intelligence, early warning, and domestic counterterrorism.

The Administration has undertaken significant efforts to reshape federal programs to match the national strategy. For instance, Homeland Security Presidential Directive 7 (HSPD–7) established "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."[4] However, in many respects, investments in state

1. Office of Homeland Security, *National Strategy for Homeland Security*, July 2002, pp. viii–x, at *www.whitehouse.gov/homeland/book/nat_strat_hls.pdf* (December 14, 2004).
2. Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *V. Forging America's New Normalcy: Securing Our Homeland, Preserving Our Liberty* (Arlington, Va.: RAND Corporation, 2003), p. 5.
3. *Ibid.*, pp. 5–6.

and local programs still reflect pre–September 11, 2001, policies and focus on crisis response and emergency responder capabilities.

Even prior to 9/11, there were preparations for responding to terrorist attacks. Regrettably, much of the funding was spent haphazardly on individual initiatives, some of which were poorly conceived and managed. Most programs bore little relation to one another. One comprehensive analysis concluded that programming "mushroomed without supervision, evaluation, or coordination, resulting in a confusing mess."[5]

The Defense Against Weapons of Mass Destruction Act of 1996 established the Domestic Preparedness Program (DPP), which epitomized this poor resource management. The legislation required the Army to teach first responders in the 120 largest U.S. cities how to counter unconventional terrorism; however, the implementation was problematic.[6]

> Federal authorities preached the importance of local response agencies working hand-in-hand and claimed that they would do so themselves, but front-line rescuers got the distinct impression that the federal agencies were locked in an intense competition for terrorism preparedness missions and money.[7]

In addition, state and local communities had difficulty determining which agency was in charge and what the overarching plan was. Local politics also hindered the programs.

Despite efforts after 9/11 to remedy the situation, money is still wasted on building response capacity. For instance, the DHS Inspector General reported that states handle first responder grants differently. States may use population, threat, risk, or the governor's discretion to disburse funds.[8] As Governor Mitt Romney (R–MA), co-chairman of the National Governors Association's homeland security efforts, has argued, "[W]e need to maximize our nation's investment in information and intelligence sharing."[9] Many states are focusing too much effort on preparing to respond when the most important investment would be in preventing terrorist attacks.

This is not to argue that the federal government should direct how states and local governments implement their homeland security plans. One size cannot fit all. On the other hand, the purpose of federal assistance to states should not be simply to provide them with entitlements to expand their capacity to respond to a terrorist attack.

Federal efforts should focus on initiatives that will make all Americans safer. These include providing state and local governments with the capability to integrate their counterterrorism, preparedness, and response efforts into a national system and expanding their capacity to coordinate support and share resources. Congress and the Administration should develop an approach that respects federalism, protects civil liberties, and effectively allocates federal monies while improving state and local capabilities for intelligence, early warning, and domestic counterterrorism.

Fundamentals for a National Initiative

To address the issue of misplaced priorities, America needs a national plan that is geared to

4. George W. Bush, "Critical Infrastructure Identification, Prioritization, and Protection," Homeland Security Presidential Directive HSPD–7, December 17, 2003, at *www.whitehouse.gov/news/releases/2003/12/20031217-5.html* (February 16, 2005).
5. Amy E. Smithson and Leslie-Anne Levy, "Ataxia: The Chemical and Biological Terrorism Threat and the U.S. Response," Stimson Center *Report* No. 35, October 2000, p. 113, at *www.stimson.org/cbw/pubs.cfm?id=12* (December 20, 2004).
6. *Ibid.*, pp. 120, 163, and 165.
7. *Ibid.*, p. 168.
8. Department of Homeland Security, Office of Inspector General, *An Audit of Distributing and Spending "First Responder" Grant Funds*, OIG–04–15, March 2004, p. 12.
9. Mitt Romney, testimony before the Committee on Governmental Affairs, U.S. Senate, May 5, 2003.

state and local communities and focused on preventing the next terrorist attack. It should enhance information analysis capabilities, strengthen the capacity to conduct terrorism-related immigration investigations, provide strong legal authorities to support information sharing, and establish a template for state intelligence operations.

An Information and Intelligence Sharing Network. The Intelligence Reform and Terrorism Protection Act of 2004, commonly known as the 9/11 Reform Bill, mandated that the President establish an "information sharing environment" (ISE) to distribute intelligence regarding terrorism to appropriate federal, state, local, and private entities. Section 1016 of the bill requires designating an organizational and management structure to establish and maintain the ISE and reporting back to Congress within one year on the plans for implementation. The law also calls for creation of an Information Sharing Council to advise the President and the ISE program manager on developing policies, procedures, guidelines, roles, and standards for establishing and maintaining the ISE.

Over the long term, the ISE could provide critical capabilities for enhancing the role of state and local agencies in counterterrorism operations. To ensure that they appropriately access and contribute to the ISE, state and local representatives should be given key positions in the Information Sharing Council to ensure that their needs and potential contributions are adequately addressed.

Enhancing Information Analysis Capabilities. In the meantime, improving the ability of state and local law enforcement need not wait until the ISE becomes fully operational. Some shortfalls can be addressed right now. Enhanced information analysis capabilities are critical for counterterrorism operations. Often, the challenge in investigations is making sense of the information available and seeing how the pieces fit together. The right data analysis tools can assist an investigator in assembling a complete picture by allowing for more effective and efficient searches of government databases (e.g., a federated search engine or automated search agent); graphically displaying links among various pieces of information; and applying algorithms to selected data to find patterns. Data analysis capabilities enable investigators to sort through the deluge of information and organize the relevant bits into a coherent mosaic.

Technologies that can provide enhanced analytic capabilities are already available. Information analysis is a growing field, with both mature technologies and technologies still in the early research and development stages. For example, two rapidly developing programs are the Multistate Anti-Terrorism Information Exchange Information Sharing (MATRIX) program[10] and the Intelligence Data Analysis System (IDAS).

The MATRIX program was a proof-of-concept pilot created to facilitate timely information sharing and exchange of terrorist and criminal information among law enforcement members.[11] Specifically:

> [MATRIX] is the law enforcement equivalent of an Internet search engine that accesses criminal, public, and commercial databases. It was designed as an automated resource to reduce the research/turnaround time involved with following up or verifying information during an investigation.[12]

10. The DHS Privacy Office will issue a report shortly that examines MATRIX and DHS's role in the program. Department of Homeland Security, Privacy Office, *Report to Congress, April 2003–June 2004*, p. 18, at *www.dhs.gov/interweb/assetlibrary/privacy_annualrpt_2004.pdf* (February 3, 2005).
11. This project initially included a component called the "High Terrorist Factor," which supposedly could identify likely terrorists based on demographic and behavior data. This feature reportedly has been dropped because it used intelligence to which law enforcement officers do not normally have access and because of privacy abuse concerns. See Harold C. Relyea and Jeffrey W. Seifert, "Information Sharing for Homeland Security: A Brief Overview," Congressional Research Service *Report for Congress*, updated September 30, 2004, pp. 11–12.
12. Multistate Anti-Terrorism Information Exchange, "Frequently Asked Questions," at *www.matrix-at.org/faq.htm* (August 18, 2004).

The MATRIX program enables data analysis with an application called Factual Analysis Criminal Threat Solution (FACTS), which combs through existing nonintelligence data sources.[13] FACTS integrates the diverse data from different storage systems in an attempt to identify, develop, and analyze information related to terrorist or criminal activities.[14]

The two key components of the FACTS application are (1) the ability to access data from numerous databases and (2) an interactive interface that assists with intuitive analysis and data presentation.[15] The available data sources include public records (e.g., property ownership, pilot licenses, vessels registered with the Coast Guard, sex offender lists, corporation filings, terrorist watch lists, and bankruptcies); generally available commercial databases (e.g., telephone directory assistance); and historically available law enforcement files (e.g., criminal history, correction department documentation and images, motor vehicle registration, and driver's license information and images).[16] The pilot project has limited the use of FACTS to data requests that are "directly related to a law enforcement agency's active criminal investigation and operational case or…a response to a confirmed lead that requires follow-up to prevent a criminal act."[17]

IDAS relies on a commercial, off-the-shelf, open architecture that can interact with a variety of systems. The system's "data fusion capability gathers, correlates, disseminates, and updates intelligence from multiple, designated sources through intelligent agents that are individually tasked by analysts."[18] IDAS is portrayed as a way to find, correlate, and share actionable intelligence. It is a system of systems that has automated some of the more labor-intensive portions of research. The system has a common interface for accessing various internal and external databases and systems. Analysts can also share data among participating member agencies and across various security levels.

Some features of IDAS include:[19]

- "Common systems interface,"
- "Passive and active triggers for analyst action,"
- "Intelligent agents for data collection and automation,"
- "Multi-INTEL fusion and data mining,"
- "Hidden and non-obvious relationship discovery,"
- "Multi-level security,"
- "Collaboration aids and tools,"
- "Case management and reports,"
- "Operational and environmental adaptability,"
- "Modularity for force-wide deployment,"
- "Integration of legacy systems," and
- "Rapid, reliable decision-support tools."

The system is not currently operational. To establish an initial capability would cost about $2.1 million, not including data sources and access privileges.

Systems like MATRIX and IDAS have significant policy implications. There are legitimate concerns about data protection, individual privacy, and civil liberties. There are also worries about the accuracy of the data in the databases that these systems use. Data analysis technologies can be developed in a manner that allows for effective systems that create minimal risks to civil liberties. However, the system must be crafted carefully, with built-in safeguards to guard against error and abuse.

13. Multistate Anti-Terrorism Information Exchange, "FACTS Defined," at *www.matrix-at.org/FACTS_defined.htm* (November 5, 2004).
14. *Ibid.*
15. See Multistate Anti-Terrorism Information Exchange, "Frequently Asked Questions."
16. *Ibid.*
17. Multistate Anti-Terrorism Information Exchange, "Factual Analysis Criminal Threat Solution (FACTS): Privacy Policy," December 2003, p. 4, at *www.matrix-at.org/privacy_policy.pdf* (August 18, 2004).
18. Lockheed Martin Corporation, "Intelligence Data Analysis System (IDAS)," project description, 2003.
19. *Ibid.*

Establishing federal guidelines for use of these technologies is one way to counter these concerns. Such guidelines should include the following elements:

- Every deployment of federal data-mining technology should require authorization by Congress;
- Agencies should institute internal guidelines for using data analysis technologies, and all systems should be structured to meet existing legal limitations on access to third-party data;
- A Senate-confirmed official should authorize any use of data-mining technology to examine terrorist patterns, and the system used should allow only for the initial query of government databases and disaggregate personally identifying information from the pattern analysis results;
- To protect individual privacy, any disclosure of a person's identity should require a judge's approval;
- A statute or regulation should require that the only consequence of being identified through pattern analysis is further investigation;
- A robust legal mechanism should be created to correct false positive identifications;
- To prevent abuse, accountability and oversight should be strengthened by including internal policy controls, training, executive and legislative oversight, and civil and criminal penalties for abuse; and
- The use of data-mining technology should be strictly limited to terrorism-related investigations.[20]

States and localities should establish regional systems to share information and data analysis capabilities. The federal government should also pay for the services used in support of federal counterterrorism investigations that are approved by the relevant Joint Terrorism Task Force (JTTF).

Strengthening Immigration Investigations. Terrorist investigations involving immigration violations are another area in which much could be done immediately to improve the role of state and local law enforcement. Domestic counterterrorism comprises law enforcement efforts primarily by the Federal Bureau of Investigation and U.S. Immigration and Customs Enforcement to identify, prevent, and prosecute terrorists. As one of the authors has noted:

> The guiding principle for enhancing this critical mission area should be adopting programs that expand the capacity to conduct counterterrorism operations without impinging on civil liberties or detracting from other law enforcement priorities.[21]

One way to do this is by forming cooperative relationships among federal, state, and local law enforcement agencies for immigration investigations related to terrorism. While using state and local law enforcement officers to enforce federal immigration laws has been controversial, such programs may be appropriate for some states and localities.

In June 2002, the Immigration and Naturalization Service (INS) and the State of Florida created a pilot program that could serve as a model for enhanced and appropriate cooperation. The program trained selected state and local law officers to assist in domestic counterterrorism immigration investigations. The Florida officers were required to be members of the state counterterrorism task force and could engage in these activities only when taking part in counterterrorism operations supervised by the federal INS officers.[22] When the INS became part of the DHS, the program's memorandum of understanding was renewed.

The Florida pilot program represents an ideal model for the limited and appropriate use of state and local support in expanding the DHS's investi-

20. Paul Rosenzweig, "Proposals for Implementing the Terrorism Information Awareness System," Heritage Foundation *Legal Memorandum* No. 8, August 7, 2003, at *www.heritage.org/Research/HomelandDefense/lm8.cfm*.

21. James Jay Carafano, "The Homeland Security Budget Request for FY 2005: Assessments and Proposals," Heritage Foundation *Backgrounder* No. 1731, March 5, 2004, p. 7, at *www.heritage.org/Research/NationalSecurity/bg1731.cfm*.

22. *Ibid.*, p. 8.

gatory capacity. Congress should provide sufficient resources to allow the DHS to offer similar programs to other states and U.S. territories. Congress should also appropriate funds to sustain training and support for these programs.

Establishing a Regional Framework. Establishing a regional DHS network as required by the Homeland Security Act of 2002 would also enhance the ability of federal agencies to work more effectively with their partners in state and local government. Under the regional framework, the DHS will establish field offices to coordinate with the states.[23]

The first priority of this regional organization should be to support the flow of information and to coordinate training, exercises, and professional development for state and local governments and the private sector. The structure's key operational mission should be to enhance prevention, preparedness, response, and critical infrastructure protection at the regional level, as well as to coordinate activities like intelligence sharing and early warning with the Justice Department's regional JTTFs.

Regional offices should also improve situational awareness and transparency among homeland security actors by promoting information sharing among them. Increased data exchanges could occur both electronically, through an expansion of the horizontal communication provided by the Joint Regional Information Exchange System (JRIES) and related networks, and in person through additional opportunities for personal encounters. People involved with homeland security at the state and local levels—including first responders, public health experts, and law enforcement officials—have diverse backgrounds and expertise, so their approaches to these issues (as well as their insights regarding them) are likely to differ. State-level actors in particular could benefit from more frequent interaction with their nearby colleagues given that many counterterrorism operations could easily spill across state boundaries.

A Template for State Intelligence Operations. State and local law enforcement agencies have a key role to play in preventing terrorist attacks. They represent approximately 95 percent of America's law enforcement counterterrorism capability. However, they have only limited resources and therefore need to target their efforts based on intelligence and risk assessment. Federal, state, and local authorities should work together with the private sector to assess threats, vulnerabilities, and consequences. To guide these assessments, the federal government should establish a continuity-based methodology and provide a single point of contact for states and localities.

Since 9/11, state and local authorities have become greater consumers of actionable intelligence from the federal government. The federal government should develop a reliable and well-organized mechanism for getting information to those who need it. In creating any such process, the federal government should realize that law enforcement agencies are not the only consumers of intelligence. Emergency medical service, public health, public works, and transportation agencies, as well as the private sector, all need various levels of detailed information.

One hindrance to sharing information is classification. The federal government should work to declassify as much information as possible instead of requiring security clearances for intelligence consumers. Forcing states and localities to incur the costs of the security clearance process is an undue burden since these entities are helping the federal government to protect the nation. In addition, there need to be protocols to protect sensitive business information if the private sector is to be involved. In the words of the Homeland Security Advisory Council, "The emphasis *should* be on establishing the processes, protocols and systems to facilitate the sharing of intelligence/information between those who collect it and those who need it."[24]

Information collection and intelligence distribution do not travel in only one direction. While states

23. Edwin Meese III, James Jay Carafano, and Richard Weitz, "Organizing for Victory: Proposals for Building a Regional Homeland Security Structure," Heritage Foundation *Backgrounder* No. 1817, January 21, 2005, at *www.heritage.org/Research/HomelandDefense/bg1817.cfm*.

and localities need to receive information from the federal government in a timely manner, they are also among the greatest collection forces available to the federal government. In the course of many routine interactions, law enforcement officers gather information that could indicate terrorist activities. The federal government should create guidelines to standardize domestic intelligence and information activities and to describe its intelligence requirements during all threat environments.

A number of information-sharing architectures are in use, but there are great irregularities among the various systems and in the members' capabilities. There should be a national system with capabilities guidelines and with members that meet a minimum capability level. One option would be to use the National Criminal Intelligence Sharing Plan as a foundation for creating an all-source, multidisciplinary national information-sharing system.

In all aspects, all of the parties involved need to confer with each other on how the processes and programs are working. Improvements need to be made where possible, although a national information-sharing system will inevitably struggle with the expectation that it should be all things to all people. In addition, the federal government should collect and distribute best practices.

What the Administration and Congress Should Do

State and local governments need a more balanced approach to homeland security. The Administration and Congress can help them achieve that balance with a comprehensive package of initiatives. Specifically, the Administration should:

- Move aggressively to implement the ISE in consultation with state and local governments,
- Fund the use of data mining in support of federal counterterrorism investigations that are approved by the relevant Joint Terrorism Task Force,
- Establish guidelines for the appropriate use of data-mining technologies in support of federal investigations,
- Implement a regional DHS as soon as practicable, and
- Collect and distribute best practices for state intelligence operations.

For its part, Congress should:

- Authorize the deployment of federal data-mining technologies,
- Fully fund the expansion of the 287(g) program for conducting terrorism investigations related to immigration violations, and
- Support the implementation of the ISE and the DHS regional framework.

Conclusion

The best way to respond to a terrorist attack is to prevent it from ever happening. States and local governments can assist significantly in prevention and do it in a way that respects the principles of federalism and American citizens' constitutional rights and privacy. A sensible package of initiatives from the Administration and Congress would facilitate these state and local efforts.

—James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation. Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation and Adjunct Professor of Law at George Mason University. Alane Kochems is a Research Assistant in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

24. Homeland Security Advisory Council, *Intelligence and Information Sharing Initiative: Final Report*, December 2004, p. 24, at *www.dhs.gov/interweb/assetlibrary/HSAC_IntelInfoSharingReport_1204.pdf* (February 14, 2005); emphasis in original.