William O. Jenkins
U.S. Government Accountability Office

Academic–Practitioner Exchange

Collaboration over Adaptation: The Case for Interoperable Communications in Homeland Security

William O. Jenkins is the director of homeland security and justice issues for U.S. Government Accountability Office. He has been with the GAO since 1979. Among other areas, he is responsible for the GAO's work on emergency preparedness and response.
E-mail: jenkinswo@gao.com.

Analogizing the U.S. Department of Homeland Security to a corporate conglomerate consisting of multiple, formerly independent operating units with little in common and even less history of cooperation, this response to Professor Charles Wise prescribes the "bitter medicine" of interoperable communications. The critical function of assuring homeland security and disaster preparedness cannot depend on the uncertain trajectory of adaptive response.

Professor Wise identifies a number of challenges that have faced and continue to face the U.S. Department of Homeland Security (DHS), including shared responsibilities with other federal agencies over which it has no authority; a mix of agencies within the DHS that have diverse missions and cultures; the challenge of defining and obtaining support for a clearly understood set of missions and goals whose achievement necessarily requires integrating the efforts of federal, state, local, and tribal governments, nonprofit entities, and the private sector; and the need for an adaptive approach to an ever-changing environment marked by uncertainty. As Professor Wise notes, few of the department's challenges were unexpected.

In many ways, the DHS's challenges are similar to those of corporate conglomerates that attempt to meld a number of disparate entities and business lines into a single corporation, with the goal of leveraging the strengths of the individual entities to create a stronger, more profitable corporation. Even the merger of similar entities (e.g., two airlines) poses challenges in melding different corporate cultures and such things as personnel and seniority systems, reservation systems, and so forth. In assessing success, corporations usually focus on a single measurable outcome: per-share profits. There is no comparable, easily measured outcome for the DHS, nor is it easy to get consensus on what the outcome measures should be and how they might be measured.

Like corporate conglomerates, some of the agencies merged into the DHS have little in common—for example, the Coast Guard and Secret Service. The Coast Guard's mission includes search and rescue, drug interdiction, and maritime safety, including cruise ship inspections. The Secret Service is responsible for the personal protection of the president and vice president and investigating such crimes as currency counterfeiting and financial institution fraud. Yet both the Secret Service and the Coast Guard have intelligence units whose information needs to be consolidated with that of other DHS units to assess threats and risks. This is one small example of the enormous organizational, leadership, and management challenges facing the DHS.

The DHS's original organizational structure included five major directorates: management, science and technology, information analysis and infrastructure protection, border and transportation security, and emergency preparedness and response. Some agencies fell outside these directorates, such as the Coast Guard and Secret Service. From the very beginning, there was debate about the department's organization and its role and mission relative to other federal, state, and local agencies, as well as the missions of the agencies that had been folded into it. That debate continues within Congress and among state and local government officials, nongovernmental entities, and the private sector. Secretary of Homeland Security Michael Chertoff's recent reorganization is unlikely to be the last word on the issue.

The DHS area with which I am most familiar is emergency preparedness and response. Since the initial formation of the DHS, this area has been marked by competition and ambiguity in roles and responsibilities. The Homeland Security Act transferred all of the functions, personnel, and resources of the Federal Emergency Management Agency (FEMA) to the DHS, except for terrorism preparedness. The Office for Domestic Preparedness (ODP), which was transferred from the Department of Justice to the border and transportation security directorate, has focused on terrorism and had responsibility for terrorism

preparedness within the DHS. In the past, FEMA's principal ties were with state and local emergency management directors; the ODP's principal ties were with law enforcement. Reflecting the emphasis on terrorism prevention and response that was a key reason for creating the DHS, the ODP gradually supplanted FEMA as the principal locus of grants and guidance for state and local emergency preparedness and response.

For emergency preparedness and response, the overarching issue is this: Are the nation's first responders able and ready to prevent or mitigate (where possible), respond to, and recover from major emergency incidents—regardless of their cause—with well-planned, well-coordinated, and effective efforts among multiple first-responder disciplines, multiple jurisdictions, and levels of government? If not, what are the most critical gaps, and how can they best be effectively addressed?

Addressing this issue requires answering four seemingly simple questions:

1. What is important—that is, what are our priorities?
2. How do we know what is important?
3. How do we measure, attain, and maintain success?
4. How do we make trade-offs given limited resources—that is, how much security and capability are we willing to pay for?

Emergency preparedness and response responsibilities are highly decentralized among thousands of jurisdictions and disciplines, public and private. For the most part, these jurisdictions and disciplines have historically operated with little central direction or guidance. As Professor Wise's article suggests, this highly decentralized structure means that extensive consultation and cooperation among many, many players, public and private, are required to reach agreement on how to identify and define what is important, measure success, make necessary trade-offs, and build and maintain the needed capabilities.

Since the terrorist attacks of September 11, 2001, there has been a continuing debate concerning emergency preparedness and response. Two principal issues have dominated the debate thus far: (1) the balance between preparing for emergencies caused by terrorist attacks and those caused by accidental or natural disasters; and (2) the appropriate role of federal, state, local, and tribal governments and nongovernmental entities in prevention, preparedness, response, and recovery, including setting standards and requirements and funding appropriate equipment, personnel, training, assistance, and sustainment costs.

The DHS has developed four principal policy documents—the first three of which Professor Wise discusses—to guide the identification, assessment, and measurement of emergency prevention, preparedness, response, and near-term recovery capabilities:

1. The National Response Plan
2. The National Incident Management System
3. The National Preparedness Goal
4. The National Infrastructure Protection Plan

The National Infrastructure Protection Plan was issued in draft form in November 2005. Its purpose is to bring together all levels of government and the private sector to identify and appropriately protect critical infrastructure and other key resources. According to the DHS, together with the National Response Plan, the National Infrastructure Protection Plan will provide a comprehensive, integrated approach to addressing key elements of the nation's homeland security mission to prevent terrorist attacks, reduce vulnerabilities, and respond to incidents in an "all-hazards" context. Starting with fiscal year 2006, grant applicants' strategic plans for protecting critical infrastructure and other key resources based on the National Infrastructure Protection Plan will be one of the criteria for evaluating their strategies.

Hurricane Katrina has prompted a reassessment of the National Response Plan and the National Preparedness Goal, including the roles and responsibilities of the federal government during a catastrophic event that immediately overwhelms and cripples the response capabilities of state and local governments. In July 2005, before Katrina hit, Secretary Chertoff announced his plans for a reorganization of the DHS. Included in his six-point agenda was a goal to "increase preparedness, with particular focus on catastrophic events." The reorganization proposed creating a new undersecretary for protection and preparedness (recently confirmed), who would be responsible for consolidating the department's existing critical infrastructure for protection, preparedness, and state–local–private coordination efforts, including planning, training, exercises, and funding. In this plan, FEMA would be outside the new directorate, reporting directly to the secretary of homeland security so that it could "focus on its historic and vital mission of response and recovery." The new undersecretary of preparedness would have responsibility for all state and local grants for emergency preparedness. Many of the operational details of the reorganization are still to be worked out, and its effect on enhancing emergency preparedness and response in the nation will not be known for several years.

As Professor Wise discusses, emergency preparedness, particularly in an age of terrorism, must take place in an uncertain environment. Particularly with regard

to deliberate acts of destruction and injury, the risk evolves and changes over time, as do the capabilities needed to respond to those risks. The risks for which we need to be prepared vary across the country. For example, hurricanes and tsunamis are not a particular cause for concern in Nebraska, but river flooding is, as are attacks on food production in the state. However, it is easier to assess the potential risk of flooding (historical data are available) than it is to assess the risk of a terrorist attack on crop production (for which there is no historical experience). Any change in the method of assessing and prioritizing risks across the nation creates winners and losers in the distribution of federal funds to address those risks—hence the difficulty of reaching agreement on how to identify and assess risks.

Professor Wise notes that in this uncertain environment with many players, adaptive planning and response is likely to be most effective. Organizational structures and processes can encourage or facilitate specific desired behaviors, but in large, complex organizations, they are rarely successful in compelling changes in behavior. The DHS's challenge is particularly notable because the department has control over only a portion of the resources needed to be successful. Thus, the DHS must develop structures and processes that provide incentives and rewards for collaboration, consultation, and support for implementing key goals. This is particularly necessary in an environment in which the DHS has few sanctions to impose on those who do not collaborate. Collaboration and consultation are most likely when the participants perceive that the potential gains are at least as valuable as the potential costs (e.g., authority, resources). But an adaptive approach also entails a degree of uncertainty. In such an environment, personal relationships are very important, and they can either facilitate or hinder adaptive approaches. Constantly changing personalities in key positions can make an adaptive approach very difficult to implement and maintain.

This is not a new problem, and it manifests itself in a variety of areas within the DHS. One example is interoperable communications for emergency responders. As the Government Accountability Office (GAO) has reported, the principal challenge in developing effective interoperable communications for emergency responders is not technical, but cultural and organizational (GAO 2004). The three principal challenges we identified are as applicable to the DHS as a whole as they were and are to interoperable communications: (1) clearly identifying and defining the problem; (2) establishing national interoperability performance goals and standards that balance nationwide standards with the flexibility to address differences in state, regional, and local needs and conditions; and (3) defining the roles of federal, state, and local governments and other entities in addressing interoperable needs.

We noted that the single greatest barrier to addressing the decades-old problems in interoperable communications is the lack of effective, collaborative, interdisciplinary, and intergovernmental planning. No single first-responder group or governmental agency can successfully "fix" the interoperability problems that face the nation. Similarly, the DHS alone cannot "secure" the homeland—it must necessarily rely on and work with a wide variety of other entities. Their cooperation, collaboration, and support are essential. As a former colleague once said, the GAO's prescription for achieving interoperable communications is political and organizational "castor oil"—necessary medicine, but not one readily taken. The challenge is convincing the patient that the cure is not worse than the disease. With regard to both interoperable communications and the DHS generally, I would expect the patient to take a sip or two of the medicine but continue to ponder whether the entire dose is worthwhile.

Reference

U.S. Government Accountability Office (GAO). 2004. *Homeland Security: Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications.* Washington, DC: U.S. Government Printing Office. GAO-04-470.