Customs and Border Protection officer checks documents for entry to the United States

CBP

The Department of Homeland Security
An Organization in Transition

By CHARLES B. KING III

On November 25, 2002, the Homeland Security Act of 2002 became law, and 60 days later, the Department of Homeland Security (DHS) became the newest Cabinet-level organization in the U.S. Government. Over the following 5 months, DHS merged elements of 22 agencies from 9 departments into its structure.[1] In the nearly 7 years since, the Department has undergone one major internal reorganization (the 2005 Second Stage Review), two externally driven reorganizations (prompted by the Intelligence Reform and Terrorism Prevention Act of 2004 and the Post-Katrina Emergency Management Reform Act of 2006), and several smaller, agency-specific reorganizations.

The transition from the George W. Bush administration to the Barack Obama administration provides an opportunity to review these changes and to examine the extent to which it would be advisable to make further modifications to DHS. In that spirit, this article represents a synthesis of a series of 19 interviews with current and former career and noncareer DHS officials, staff members of both the House and Senate Homeland Security Committees, academic observers of the Department, and staff members who supported the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission). The 19 interviewees made suggestions for the Department in four areas: changes to policy, modifications to oversight, management and integration improvements, and areas in need of additional focus.

Policy

Interviewees had few policy-related suggestions for the Obama administration. There

Charles B. King III is the Risk Analysis Branch Chief for the Transportation Security Administration of the Department of Homeland Security.

was, however, one policy issue that many interviewees felt warranted significant attention: immigration.

The key test of a successful immigration reform package is how well it addresses several interrelated issues:

- provision of temporary work visas
- path to citizenship for noncitizens currently illegally working in the United States
- means by which the United States will enhance border control
- expansion (numbers and eligibility) of the work visa program
- establishment of a reliable system for employers to validate the citizenship (or visa status) of prospective employees
- provision of work and training opportunities for current U.S. citizens.

This list is similar to those that underpinned President Bush's 2006 immigration reform proposal—unsurprisingly, perhaps, neither the numbers of migrants nor the Nation's interest in addressing their presence has changed significantly. The United States still has between 12 and 20 million illegal aliens in the country, far too many to have a "reasonable expectation [to] send . . . back home." The United States still has an interest in welcoming and retaining immigrants (particularly those who are smart, creative, and industrious). And the United States still has an interest in promoting the employment of citizens over noncitizens for both high- and low-skill jobs.

The consensus view of the interviewees is that a reform package would consist of three elements, each requiring positive and negative inducements to change both individual and corporate behavior. The first of those elements is enhancing penalties for employers who knowingly violate the provisions of the Immigration Reform and Control Act of 1986 as they apply to hiring illegal immigrants. Establishing a straightforward safe-haven process for validating worker credentials would complement those enhanced penalties.

The second element is facilitating a path to citizenship for illegal immigrants who have been in the United States for a period of years and have been net contributors to the Nation's well-being. Complementing this element would be some form of noncriminal penalty (a requirement for community service or a fee) in order for the program to avoid the "amnesty" label. The third element is enhancing border control efforts aimed at stopping illegal migration, a task that would be linked to easing temporary and permanent work visa requirements. By shifting the incentives of immigrants from attempting illegal crossings to making legal crossings at designated points, the Federal Government would facilitate its task of focusing screening efforts on people with suspect backgrounds.

DHS should have three roles in the development of this policy. First, it should conduct outreach efforts to state and local governments to gather input on how best to execute this policy. State and local governments bear the brunt of illegal immigration, and their buy-in would be vital to enacting meaningful legislation. Secretary Janet Napolitano's engagement is critical in this phase because of her credibility, by virtue of her experience as a border state governor, with these constituencies.[2]

establishing a straightforward safe-haven process for validating worker credentials would complement enhanced penalties

The second element should be providing the White House with input on the feasibility of implementing the policy. The final role should be publicly discussing DHS implementation requirements under the legislation. However, DHS should not have any public role in discussing the policy elements of reform legislation. After the Bush administration designated Michael Chertoff as its point-person for immigration reform, Secretary Chertoff's lobbying efforts hurt his credibility with the Federal legislative branch on a range of other issues because immigration reform became so politicized. When making comments on this subject, DHS should also take care not to overemphasize border control as either a counterterrorism issue or an antidote to illegal immigration. With a 1,969-mile southern border that runs through both cities and mountains, border control cannot be a 100-percent success story, and DHS should be careful to not imply that it could be.

Oversight

Interviewees made a number of comments touching on oversight. This article addresses only two of these recommendations: streamlining oversight of DHS, and merging the Homeland Security Council (HSC) with the National Security Council (NSC).

Congressional Oversight. The most important issue facing DHS is congressional oversight, but the Department has very little influence on it. Groups as diverse as the 9/11 Commission, Council for Excellence in Government, Homeland Security Advisory Council, National Academy of Public Administration, and Center for Strategic and International Studies have identified streamlining congressional oversight as one of the most difficult, and most important, issues for DHS, and many interviewees agreed.[3]

Streamlining oversight would enhance unity of effort for DHS; having between 79 and 86 committees and subcommittees (depending on which organization is counting) claiming jurisdiction has led to no committee providing effective supervision. This aspect is particularly important in that DHS spends over $35 billion and provides over $3 billion more in grants each year based on a risk assessment process that relies on intuition far more than on hard data. It is a situation that begs for better, not more, oversight. Streamlining oversight would also provide for more effective management of the organization; having senior management testify frequently to a wide variety of committees is a significant drain on management time and attention.

Congress partially implemented the oversight portion of the 9/11 Commission's recommendations in 2005, but has found the politics of implementing the balance of those recommendations daunting. DHS has a number of activities not related to homeland security—such as providing aids to navigation—embedded in it, and these activities are important to many Members of Congress who are on neither the House nor the Senate Homeland Security Committees.

One partial solution is to expand the jurisdiction and membership of the Homeland Security Committees at the expense of other committees. A useful model would be the Department of Defense oversight structure in which, despite having bases in almost every district and a budget 13 times that of DHS, only 36 committees and subcommittees provide oversight.[4] Such a change would reduce conflicts in guidance from appropriators and authorizers, provide for better defined requirements, enhance relations between branches of government,

and improve the effectiveness of acquisition programs.[5] This is one of the few areas where the important question is not, "What is best for the Nation?" Here, the important question is, "How do we make the politics work?"

Homeland Security Council. Established by Presidential directive on October 28, 2001, the HSC is a stepchild of the NSC, and its function is to "ensure coordination of all homeland security–related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies."[6] As one may expect from its origin, its membership has significant overlap with that of the NSC: 11 of the NSC's 15 members/statutory advisors/substantive invitees are also on the HSC.

There is a considerable degree of symmetry between its role and that of the NSC, which is charged to "coordinate executive Departments and agencies in the effective development and implementation of those national security policies,"[7] including the defense of the Nation. The very fact that the NSC jointly administers 3 of the HSC's 10 policy coordinating committees illustrates the degree of overlap between the two organizations' roles and membership.[8]

Interviewees who commented upon the HSC supported merging the organization into the NSC. They believe that the concept of national security includes homeland security and that addressing terrorist threats will never again be the second-tier issue it was before September 11, 2001. Accordingly, they recommend that the Obama administration return the functionality and personnel of the HSC to the NSC, add more departmental representatives as full NSC members, build a strategic planning capability at the NSC, and expand the NSC long-term issue integration staff. In addition to retaining its current capabilities, this staff should possess the capacity to manage integration issues, should be familiar with the capabilities of DHS, and must be capable of writing a strategy with state and local involvement.

interviewees believe that the concept of national security includes homeland security and that addressing terrorist threats will never again be the second-tier issue it was before September 11, 2001

Management and Integration

Interviewees suggested changes in four areas to enhance cross-component management and integration. These recommendations focused on meshing the needs of each of the components with those of the Department's senior leadership. All interviewees who commented in this area were aware that one impact of most of these changes would be to slow the decisionmaking process, but they believed that the same forces that would produce delays would also result in a better performing Department.

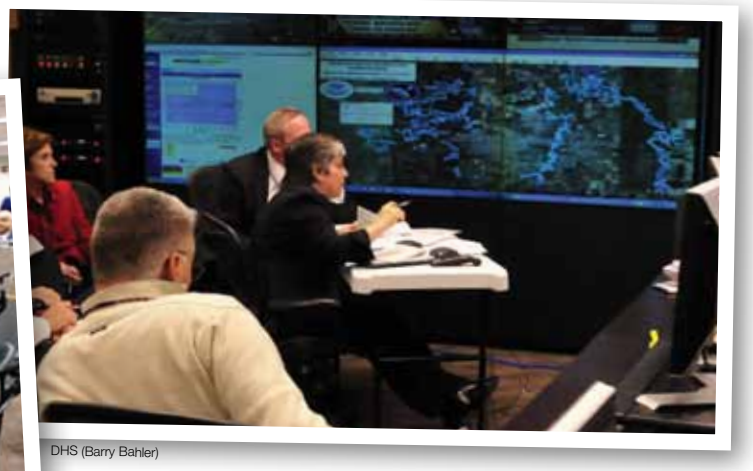
Under Secretary of Policy. Because DHS began as a merger of 22 agencies, with none of them dominating the integration process, it started without a common purpose to unite its components. That lack of a singular raison d'être has contributed to situations where components have been willing to "reinterpret" guidance from the Secretary. Having a headquarters that functioned more as an umbrella than a command element contributed to their ability to do so.

One approach to addressing this issue would be to increase the influence of the Office of Policy by elevating the Assistant Secretary for Policy to an Under Secretary position while also selecting an Under Secretary for Policy who has the confidence of, and chemistry with, both the White House and the Secretary. This officer would require the staff and the judgment to focus only on the most critical issues. The combination of these changes, each necessary but not sufficient on its own, would set the preconditions for the Office of Policy to monitor and enforce the Secretary's guidance to the components.

Risk Management Link to Budget. The next integration-related issue upon which interviewees commented was the absence of a link between risk management and budget development. A linkage between the two functions would have two major impacts: it would provide the Secretary with an additional vector for unifying the Department's efforts, and it would improve the connection between risk management and policy.

As one interviewee noted, risk management is at the heart of all the Department does. Inherent in every decision is a prioritization, implicit or explicit, of the risks DHS chooses to address. While some of the threats facing the Nation are knowable (for example, floods cause an average of $8 billion worth of damage every year), others—particularly terrorist threats—are inestimable. The two questions that then face DHS are what threats to focus on, and how to address them. The current approach

DHS



DHS (Barry Bahler)

Homeland Security Secretary visits Federal Emergency Management Agency headquarters (left) and receives briefing at DHS on flooding in North Dakota and Minnesota (above)

is for DHS to focus on the large-scale threats, while providing grants and technical support to state and local governments to address the small-scale ones. This approach is aligned with the foci of the various organizations involved in homeland security. The Federal Government feels a need to concentrate efforts on large-scale events, while local governments prefer to focus on the small-scale hazards they deal with on a regular basis.

That approach leaves DHS in a quandary as to how to prioritize the large-scale threats it needs to counter. The Secretary would be well advised to have a portfolio analysis performed to inform those choices. Without such an analysis, the Secretary is working on intuition. This all-hazards portfolio analysis should be based on a simple model and should be tailored to meet the Secretary's stated needs.

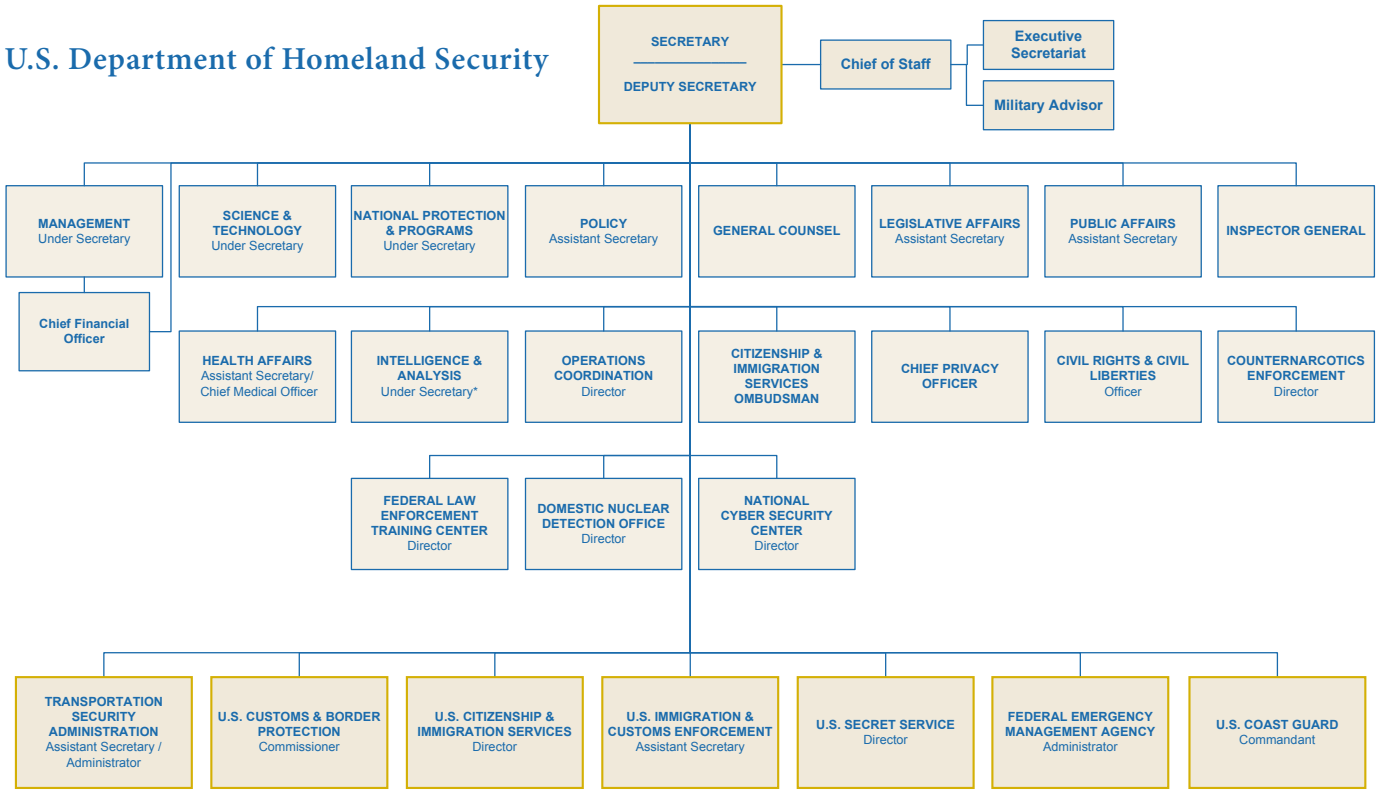
Moving primary sponsorship of the Homeland Security Institute[9] from the Science and Technology Directorate to the Office of Policy would give the Office of the Secretary direct control over the analytical capacity needed to develop a risk portfolio analysis.[10] Such an analysis would inform the Secretary's Interagency Planning Guidance, which the components use as a roadmap to set budgetary priorities, thereby expanding the connection between the Secretary's priorities and agency budgets.

Information Technology Acquisition/Integration. One of the most effective ways that the Secretary can ensure intradepartmental coordination is through the acquisition process, and the largest element of acquisitions (consuming about 10 percent of the DHS total budget) is information technology (IT). Because IT procurement is a technically complex and detail-driven subject, senior leadership tends not to focus on it, which is a significant error.[11] The devolution of responsibility to component procurement organizations results in projects that meet the needs of individual agencies but not those of the Department as a whole. In situations where a lead component has opened the development of project requirements to other components, it has occasionally begun too late in the acquisition process to avoid substantial cost and schedule overruns.

Over the past 2 years, DHS has made significant improvements to the IT acquisition process, particularly on the chief information officer (CIO) front. The DHS CIO now has increased authorities; DHS has an IT lifecycle management process; and the IT project review process, with levels of scrutiny dependent on project cost, has become effective.

With respect to improving IT acquisition staff capabilities, DHS has not been as successful. The components maintain their own procurement organizations that work with legacy systems, and the Department has not assigned enough people, dedicated enough leadership attention, or allowed for enough planning time to execute IT acquisitions well. One congressional staff member believes that, as a direct result of these factors, DHS has not had any unqualified successes in regard to major IT acquisitions. Others differ, citing the success DHS has had executing the U.S. Visitor and Immigrant Status Indicator Technology program as a gauge.

because information technology procurement is a technically complex and detail-driven subject, senior leadership tends not to focus on it, which is a significant error



*Under Secretary for Intelligence and Analysis title created by Public Law 110-53, August 3, 2007
Approved March 20, 2008

IT projects have a high impact on Department-wide performance because the Department as a whole has a requirement to know as much as possible about those whom it screens.[12] Without a CIO who enforces both the use of open standards and the execution of a detailed, time-consuming, cross-departmental requirements-development phase, DHS either builds multiple, similar, incompatible IT structures at an increased cost or changes requirements at a late date and pays for those changes through increased cost, lengthened program schedule, and decreased project performance.

Federal Emergency Management Agency. The Federal Emergency Management Agency's (FEMA's) proper location in the Federal bureaucracy has been a topic of considerable discussion for almost as long as it has been a part of DHS. Broadly speaking, there are two schools of thought regarding the proper structural place for FEMA. One school, led by former FEMA Administrator James Lee Witt, believes that the agency should return to its Clinton administration–era position of an independent agency reporting directly to the President. A direct reporting relationship between FEMA and the President would give the agency additional bureaucratic clout and restore some of the public confidence it lost after its response to Hurricane Katrina.

Moving FEMA out of DHS has disadvantages that President Barack Obama must weigh against these advantages. It would reduce the number of personnel the agency could immediately call upon during an emergency—as a stand-alone organization, it would have access to 2,600 full-time employees and 4,000 standby employees rather than the 162,000 members of DHS.[13] Similarly, a stand-alone FEMA would not have the bureaucratic heft that its present parent, a full-scale department, has when coordinating a response to an emergency.

Interviewee observations about a potential FEMA move took three forms: the impact on DHS, impact on the President, and impact on the Nation. From a DHS perspective, a FEMA move would reduce the conceptual viability of DHS, which is currently a full-spectrum homeland security organization; it addresses prevention, protection, response, recovery, and preparedness. Without the responsibility to execute FEMA's response/recovery functions, DHS would lose its ability to execute its integrative function, and that loss would invite the Departments of Defense and Justice to "encroach" on DHS prevention and protection functions.

From a Presidential perspective, it is useful to have someone, in this case a Secretary, act as political insulation in the event a response goes poorly. As one noncareer official framed the issue, "Does any politician really want to have the head of FEMA as a direct report?" Finally, at a national level, requiring yet another reorganization would jeopardize current reforms that appear to be paying dividends. Since early 2007, Governors have begun complementing FEMA's response to emergencies (for example, the wildfires in California and the hurricanes in Texas). They like FEMA's "forward leaning" posture and its eagerness to respond to emergencies—its desire to do more than write checks in an event's aftermath. While they still blame FEMA for communications breakdowns at the local level, they understand that those breakdowns are, for the most part, the Governors' issues to address.

Interviewees had some recommendations for FEMA. Two thought that FEMA authorities under the National Response Framework were insufficient and that the agency needed to be able to execute tactical control over other agencies when necessary. Another thought that FEMA needed to build a deliberate planning capacity to complement its response expertise. Finally, one mentioned that the Post-Katrina Emergency Management Reform Act of 2006 gave the FEMA administrator certain statutory responsibilities that used to be the Secretary's and that the change created friction between the two officials until they developed a shared view of the administrator's responsibilities.[14] That interviewee went on to note that the understanding was a matter of personalities, and that the next administrator and Secretary will have to reach a similar understanding. Of note, one interviewee thought that lessons identified in the *Federal Response to Hurricane Katrina Lessons Learned* report did not place enough emphasis on the role of leadership during a crisis.

CBP (James R. Tourtellotte)

Customs and Border Protection officer directs truck with seaport container to inspection area

from a Presidential perspective, it is useful to have someone, in this case a Secretary, act as political insulation in the event a response goes poorly

Focus Area Issues

In addition to these oversight and integration changes, interviewees suggested that the Department place additional focus on several areas, including the national cyber security strategy; liaison with state, local, and private sector authorities; infrastructure protection; and resiliency. The one theme that was consistent across all interviewee comments was that DHS should take account of, and incorporate into planning, the views of outside stakeholders while developing and executing policy.

Cyber Strategy. With the exception of congressional oversight, no other issue

received as much attention as cyber security. Interviewees noted three fundamental challenges when dealing with cyber issues: technology moves faster than regulation, even partial solutions require significant interagency cooperation, and the private sector does not trust the Federal Government.

To improve cyber security, DHS should focus on two missions: acting as a conduit to the private sector for enhancing critical infrastructure Supervisory Control and Data Acquisition (SCADA) systems; and serving as a coordinator for protecting the Federal Government's systems. The DHS lead element for improving SCADA security should be the National Cyber Security Division (NCSD), which should begin by gaining situational awareness of cyber attacks on both the private and the public sectors. NCSD should continue its work by providing public praise for companies that collaborate with DHS, working through the National Institute of Standards and Technology to develop standards for SCADA system security, and partnering with the Securities and Exchange Commission to require publicly traded companies to include a discussion of cyber-related risks in the Management's Discussion and Analysis section of their quarterly 10–Q filings.[15]

Addressing private sector security is the first half of the equation, and addressing Federal cyber security is the second half. DHS, through a significantly expanded National Cyber Security Center, should be the interdepartmental lead agency to protect the ".gov" domain on the Internet. This task will not be trivial for a number of reasons, not least of which is developing a consensus opinion of to whom (employees, contractors, vendors) authentication rules should apply.

In an effort to address the private sector's reluctance to share information with the government, DHS should develop proposed legislation establishing limited-access provisions (akin to, but more restrictive than, those for Protected Critical Infrastructure Information) for narrowly defined types of cyber-related information. This task, too, will not be a trivial effort since it will require DHS to hire cyber experts such as those found at Google or Microsoft, and those candidates have not traditionally been attracted to the Federal culture.

State and Local/Private Sector Information Sharing/Outreach. It is axiomatic that the people best positioned to protect infrastructure are those closest to it, since they are the ones most aware of its strengths and weaknesses. The most effective ways the Federal Government can support those leaders are by providing them with information on the threats to their facilities and serving as a platform upon which they share best practices within and across sectors. Unfortunately, there are stumbling blocks to doing so. As one interviewee noted, "If it has taken us 8 years to get to the information sharing point we are at, it is because it is hard to do, not because we are stupid."

DHS's fundamental issue with information-sharing lies in defining the primary customers of intelligence products. Interviewees suggested that DHS's primary intelligence customer should be state and local emergency preparedness employees, mostly—but not exclusively—police officers. This definition would represent a profound shift from the current practice that holds DHS leadership as the primary consumer of intelligence. Essentially, interviewees recommended that the Department deliberately decide to play a backup role to state and local governments. This recommendation dovetails with the Director of National Intelligence's recognition that the Federal Government must move from a "need-to-know" mindset to one that recognizes its responsibility to provide information to new partners.[16]

interviewees recommended that the Department deliberately decide to play a backup role to state and local governments

Coast Guard C–130 Hercules patrols with USS *Crommelin* and Micronesian–FSS *Independence* in western Pacific Ocean

U.S. Coast Guard (Michael De Nyse)

Such an approach would demand that DHS emphasis be on building trust on the part of state and local officials. There is still a popular misconception that DHS knows more than it does, that it is keeping the "good stuff" to itself. While the Department will never completely eliminate that perception, having liaison officers regularly ask what local officials need, and then delivering on those needs, would go far toward reducing it. DHS has taken a number of steps to address this issue:

- granting 1-day clearances
- developing Information Sharing and Analysis Councils
- funding Fusion Centers
- including local officials in the Interagency Threat Assessment and Coordination Group within the National Counterterrorism Center
- granting clearances to state officials and private sector leaders.

These steps address most of the process changes needed; now DHS needs to focus on the human element.

To help build those relationships, DHS should change its paradigm to one in which most intelligence products are unclassified and are geared for law enforcement use. These products should identify behaviors that local law enforcement and infrastructure operators should be suspicious of, and they should describe those behaviors in operational terms. DHS should support the development of these products by establishing a core of analysts who know both law enforcement needs and how to address those needs through Intelligence Community resources.

Infrastructure Protection. Few people would argue with the premise that one of DHS's core missions is ensuring the continuing function of critical infrastructure during a crisis. However, that consensus dissipates when people begin to discuss what constitutes "critical infrastructure," and it vanishes when people discuss how to execute that protection function. Congress defined *critical infrastructure* in section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." When the executive branch published the 2007 edition of the *National Strategy for Homeland Security*, it restated the definition to include whole sectors because of the possibility of significant downstream consequences stemming from an attack.

This expansion was an error. The Federal critical infrastructure protection mission should be ensuring that critical assets work in a crisis, and executing that mission would require limiting the direct Federal role to supporting security improvements at a defined set of possible targets. One interviewee took a restrictive view of what may be critical, suggesting that the Federal Government use the downstream, nationwide impacts of Hurricane Katrina as a test to determine which types of assets may be critical. In this more limited infrastructure protection model, the Federal Government, specifically the Office of Infrastructure Protection, would focus on enhancing the point-defense/survivability-assurance mission for those critical assets, while the Sector Specific Agencies (SSA) would focus on facilitating information-sharing and standards-setting across the 18 critical infrastructure sectors.

Such a layered approach would focus lead agency efforts on their areas of expertise. The Federal Government—through the SSAs—adds the most value on a sector-wide basis when providing refined intelligence to support local decisions (no other organization has the capability) and when identifying security standards that have applicability across sectors (no other organization has the scope of view). In those cases where the Federal Government determines that specific pieces of infrastructure have to remain operational regardless of circumstances, the Office of Infrastructure Protection is well positioned to provide direct assistance to the operators.

Resiliency. A vital element of homeland security is *resiliency*—ensuring that events, natural or man-made, are no more disruptive to the Nation than they have to be. A key element of resiliency is reassurance, and providing reassurance is the responsibility of DHS's senior leadership. In an emergency, the government's information dissemination strategy, primarily by means of officials' statements and answers to questions, will have a tremendous influence on the population's reaction. People want reassurance, and multiple conflicting messages will not provide it. Coordinating messages even within the executive branch is a challenging and time-consuming task, so senior officials should establish relationships with their counterparts in other departments and agencies before a crisis begins.[17] Building confidence with counterparts before an emergency will not guarantee success, but not earning their trust beforehand will guarantee failure.

Spreading a reassurance message (that "terrorists getting lucky is not the end of the world") has to start before an incident, and should be repeated until the public internalizes the concept that, provided the government has made reasonable attempts to prevent them, acts of terrorism are in the same category as plane crashes and traffic accidents. They are terrible tragedies for the families involved, but cannot be eliminated under any set of measures that are remotely reasonable to implement, and are certainly not a threat to society as a whole.

in an emergency, the government's information dissemination strategy will have a tremendous influence on the population's reaction

Conceptualizing Homeland Security

In addition to the policy, oversight, management and integration, and focus area issues discussed above, interviewees provided their thoughts on two broad questions, neither of which has firm answers: "What is homeland security, and where does DHS fit within that construct?" and "How does DHS structure itself within that model?"

Homeland Security Defined. Homeland security means many things to many people. The 2006 *National Strategy for Homeland Security* defines it as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." However, that definition, limited to countering terrorism, excludes many DHS activities, suggesting that it is too narrow. An alternative definition of homeland security, taken from several interviewees' comments, could be "a concerted national effort to prepare for and address the full range of physical and virtual domestic risks to the Nation's citizens and their well-being." This definition would encompass the protection, prevention, response, recovery, and preparedness activi-

ties inherent in an all-hazards view of DHS without requiring that all homeland security activities be part of the Department.

The Path Forward. Congress has provided guidance to DHS, which sometimes focused on the organization in its antiterrorist role, sometimes in its counterterrorist one, and sometimes in its all-hazards guise. The conflicts inherent in these three distinct views of DHS have created some confusion and inefficiencies within the organization, and DHS should use the Quadrennial Homeland Security Review as a vehicle to address those issues. By adopting a functional model to examine DHS operations, the Department may be able to identify synergies between components, particularly those that share similar core competencies: screening, patrolling, and incident management. This examination would provide a platform for the Department to address threats irrespective of how they originate (for example, trafficking is trafficking, regardless of whether it is of drugs or people). It would facilitate a convergence of how DHS screens for potential threats (for example, Customs and Border Protection and the Transportation Security Administration both look for suspicious people, yet the latter concentrates on passenger behavior while the former focuses on identity validation). It would also illustrate the utility of using open standards to enhance data-sharing between components. While no interviewee suggested that any component abandon its processes and adopt another's, several did suggest that this analysis would allow components to identify areas where the agencies would be able to work together more efficiently.

Analyzing interviewee comments, the two greatest stumbling blocks to the Department of Homeland Security's success are in the areas of congressional oversight and internal integration. The multiplicity of congressional oversight both guarantees that the Department receives conflicting guidance and limits the ability of its senior leaders to build relations with the members of its oversight committees. Divergent legislative guidance, in particular, is an enabler for components to interpret guidance from the Secretary as flexibly as they can, not the way the Secretary wants them to.

The nature of the Department's headquarters, more umbrella than command element, also facilitates the components' inclination to gravitate toward independent operations. A group on the Secretary's staff with the influence to require convergence among the Secretary's risk-informed priorities, component budgets, and agency information technology architecture would enhance the functioning of the Department as a whole. The Quadrennial Homeland Security Review presents the current Secretary with the opportunity to drive the organizational changes DHS needs. It is an open question as to whether the environment will allow her to do so.

The United States has come a long way in the nearly 7 years since the creation of DHS. After forming an entirely new agency with 50,000 employees, providing more than $20 billion in grants to state and local governments, and undergoing the largest reorganization of the Federal Government since the Goldwater-Nichols Department of Defense Reorganization Act of 1986, the Department of Homeland Security has undeniably increased the security of the Nation's citizens. After two major and countless minor reorganizations, it is also clear that DHS has more work to do. In a world where every solution both is partial and brings its own set of challenges, the issues to focus on and the means to address them will require significant thought on the part of Federal and state leaders. **JFQ**

NOTES

[1] The requirement was that almost all organizations transfer by March 1, 2003, with the Plum Island Animal Disease Center to transfer by June 1, 2003. The final personnel, assets, and liability transfers were to occur by September 30, 2003. See <www.dhs.gov/xlibrary/assets/reorganization_plan.pdf>.

[2] Admiral James M. Loy, USCG (Ret.), comments during interview with author, December 16, 2008.

[3] Combination of National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: National Commission on Terrorist Attacks Upon the United States, July 22, 2004), available at <www.9-11commission.gov/report/911Report.pdf>; Peter D. Hart Research and Public Opinion Strategies, *The Aftershock of Katrina and Rita: Public Not Moved to Prepare* (Washington, DC: Peter D. Hart Research and Public Opinion Strategies, December 2005), available at <http://ceg.files.cms-plus.com/EmergencyPreparedness/America%20Get%20Prepared%20report.pdf>; Homeland Security Advisory Council, *Top Ten Challenges Facing the Next Secretary of the Department of Homeland Security* (Washington, DC: Department of Homeland Security, September 11, 2008), available at <www.dhs.gov/xlibrary/assets/hsac_dhs_top_10_challenges_report.pdf>; National Academy of Public Administration, *Addressing the 2009 Presidential Transition at the Department of Homeland Security* (Washington, DC: National Academy of Public Administration, June 2008), available at <www.napawash.org/pc_management_studies/DHS/DHSExecutiveStaffingReport2008.pdf>; and Center for Strategic and International Studies (CSIS), *Untangling the Web: Congressional Oversight and the Department of Homeland Security* (Washington, DC: CSIS, December 10, 2004).

[4] CSIS.

[5] Combination of Andrew Morral's comments during interview with author, October 27, 2008, and Price Roe's comments during interview with author, October 27, 2008.

[6] Homeland Security Presidential Directive–1, "Organization and Operation of the Homeland Security Council," available at <www.fas.org/irp/offdocs/nspd/hspd-1.htm>.

[7] National Security Presidential Directive–1, "Organization of the National Security Council System," available at <www.fas.org/irp/offdocs/nspd/nspd-1.htm>.

[8] Alan G. Whittaker et al., *The National Security Policy Process: The National Security Council and Interagency System* (Washington, DC: Industrial College of the Armed Forces, November 15, 2008).

[9] The Department of Homeland Security Federally funded research and development center.

[10] Morral.

[11] Roe.

[12] Ibid.

[13] See <www.opm.gov/feddata/html/2008/january/table2.asp>.

[14] A career official commented during an interview with the author on January 9, 2009, that the perception that the act shifted responsibilities is not universally held. Whether it did so centers around the differences between emergency management and incident management.

[15] Form 10–Q "includes unaudited financial statements and provides a continuing view of the company's financial position during the year. The report must be filed for each of the first three fiscal quarters of the company's fiscal year." See <www.sec.gov/answers/form10q.htm>.

[16] Office of the Director of National Intelligence (ODNI), *U.S. Intelligence Community Information Sharing Strategy* (Washington, DC: ODNI, February 22, 2008), available at <www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf>.

[17] Loy.