

**PART TWO:
WORKING
GROUP ANALYSES**

REPORT OF THE WORKING GROUP ON ANALYTIC METHODS

This Working Group was chaired by James B. Steinberg, who drafted this report on behalf of the group. Participants in this group were John Arquilla, Bruce Berkowitz, Anne-Marie Bruen, Ashton Carter, William Crowell, Sidney Drell, Stanley Feder, Andrew Frank, John Gage, Lauren Hall, Margaret Hamburg, Tara Lemmey, Michael Mazarr, Douglas McDonald, James Morris, Alan Schwartz, Jeffrey Smith, Stefaan Verhulst, and Philip Zelikow, with assistance from Mary McKinley and Laura Rozen.

Working Group I was tasked with examining the information requirements and analytic methods needed to meet the challenge of new security threats, particularly threats to the homeland.

THE NATURE OF THE CHALLENGE

The information/intelligence challenge of today's new security threats is dramatically different from the Cold War security problem. During the Cold War, the United States had an information collection method that was highly focused; a known target; rich detail on the adversary's capabilities; collection technology designed specifically for well defined objectives (*e.g.* satellites to access denied areas); highly trained analysts with long experience and high degree of specialization in each aspect of the adversary's capabilities and methods; and a well-defined set of indicators and warnings. In short, we had a reasonably high degree of confidence of what to look for, and why it was important (at least on the military threat side). By contrast, today in the context of terrorism and unconventional threats, the adversary is poorly known and understood, potentially diffuse in geography, and small in numbers. What's more, our collection tools are limited (difficulty of human intelligence access, successful denial strategies against signals and imagery intelligence, etc.); we have few well trained and experienced analysts; and generally, we lack well recognizable indicators and warnings.

The Working Group therefore focused on how to develop an information strategy to address these challenges/deficiencies. Four core concepts emerged from our discussions.

1. We need to better understand our adversary—its membership, methods, capabilities, intentions—what we call the threat-based, or “focused,” dimension of strategic analysis.
2. Because our knowledge of even known adversaries is likely to be limited, and because some threats will emerge from previously unidentified sources, we also need an information collection and analysis strategy that will allow us to detect and prevent dangers from these unanticipated sources (vulnerability analysis, which includes both targets and means of attack).
3. Given the diffuse and dynamic nature of the threat, a broad range of information may be relevant to identifying the threat, and an equally broad range of sources may have relevant information. It will be difficult to specify *a priori* who may have relevant information. Therefore, there is an especially critical need to break down the compartmentalization of collection and analysis to allow the formation of constantly reforming virtual communities of analysis and connect them to users in at the international, federal, state, and local levels, as well as to the private sector. At the same time, the information and analysis system must remain sensitive to security of information concerns.

4. Because this form of analysis is heavily dependent on large volumes of data (to detect patterns and to make correlations) assuring the quality of data is critical.

STRATEGIC ANALYSIS: “WHAT” WE WANT TO KNOW—THREAT AND VULNERABILITY ANALYSES

Threat-based analysis: “Know thy enemy”

This dimension of strategic analysis centers on a focused, in-depth concentration on known threats. It is similar in kind to the analysis used against traditional state adversaries, but is adapted to take into account some of the peculiar characteristics of the non-state, non-hierarchical (or network) threat posed by terrorism. As in the traditional analysis, we are interested in knowing about the adversary’s goals/motivation, strategy, and capabilities (order of battle/membership, technical capabilities). But we must adapt how we learn these things. Considerable stress has been placed on improving HUMINT as the best (and in many cases only) way of learning these kinds of facts directly. But given the nature of these groups, there will be practical limits to the development of human sources, irrespective of the level of resources devoted to them. Therefore, other tools must be developed, including the following:

network analysis—drawing on the literature and tools of mathematics and physics, as well as social sciences, including group dynamics of like-minded individuals, and the properties of horizontal networks with many nodes; and

contextual analysis—drawing on history, culture, etc.; and allows in-depth knowledge to help reveal key indicators (the example of the “Afghan” connection of many al Qaeda members) that can be linked to pattern analysis (travel, financial flows).

The threat-based analysis should pay particular attention to the life cycle of attack planning and execution, because the information to be acquired will change dramatically in each phase. The life cycle is as follows:

1. target selection and planning
2. recruitment
3. intelligence and reconnaissance
4. logistics
5. strike

Gaining information on early stages is particularly important for the disruption and denial function.

Vulnerability analysis: “Discover thy enemy”

The danger of an in-depth, or threat, focus is that we will lose peripheral vision, and thus be highly vulnerable to surprise. This is particularly worrisome in the context of terrorism, because the adversary is highly adaptable, and because the means of causing serious harm are more widely available at relatively low cost and are employable by small groups or even individuals. No intelligence system will be perfect, but we have an especially high priority not to miss potential attacks

that will have large-scale impact. Thus we need to complement our threat-based analysis of known threats with crosscutting strategies that will reduce our vulnerability to “big” surprises.¹

This dimension of strategic analysis focuses on “vulnerabilities,” in two aspects—the vulnerability of targets and the vulnerability of means (that is, the ability of adversaries to acquire and use dangerous materials—biological, chemical, radiological, nuclear or conventional). Since there is an almost infinite number of targets and a broad array of materials that could be used as weapons, this dimension of analysis will require prioritization.² There are a number of ways to approach the problem of prioritization, including ordinal ranking of potential targets based on the magnitude of the consequences of a successful attack; focusing³ on “priority check points and portals;”⁴ and the development of templates that provide illustrative schema of attacks for planning both information collection and preventive measures.⁵ Tools for this form of analysis include:

Scenario analysis—including modeling terrorist plans through tools such as Hierarchical Holographic Modeling and other risk management techniques,⁶ Project Planning Paradigm⁷ and techniques such as red-teaming. Templates and scenarios should be the product of both “top down” approaches (experts from relevant agencies developing scenarios based on their own expertise and experience) and “bottom up”—the acquisition of new data prompting the development of scenarios or templates to “explain” the data. Large scale computer generated scenarios could prove particularly useful in connection with bottom up analysis triggered by data mining, as correlations derived from *data mining* could be cross-checked against computer generated scenarios which in turn could suggest additional data gathering priorities which in turn could either validate or refute the scenario.⁸

Means analysis, of what is necessary—in terms of personnel, expertise, material, access—to carry out an attack and how might each be acquired and deployed.

Counter-surveillance—what kind of information is the adversary trying to acquire.

Vulnerability surveys of key sites and networks—with particular attention to second and third order effects, such as the impact of a port attack on shipping commerce.

Technologies

Both threat and vulnerability analysis may lead to different technological requirements, such as transferable “expert” systems to allow additional analysts to read in quickly for threat-based analysis, and advanced search and data mining for vulnerability analysis. For the most part, technologies can be adapted from civilian use, although in some cases, the unique needs and lack of a civilian market may require direct government support for R&D.

Considerable information that will be valuable to analysis now resides in the private sector. It will be important for government to gain access to needed data, but in a way that is sensitive to civil liberties concerns and the business interests of private sector holders. By developing guidelines governing access, acquisition, and use of private sector data for analysis, the twin goals of enhancing

security and preserving core liberties are best assured. And greater government access to private databases should be accompanied by greater private sector protections on information not related to legitimate government security related requirements. This will give citizens greater confidence that providing accurate information will not lead to broad intrusions on privacy.

ARCHITECTURE OF ANALYSIS

How Do We Use the Information We Collect?

1. Building virtual analytic communities

Under the traditional threat paradigm, the intelligence/analytic community was a highly formal organization, with a fixed set of collection assets, analytic specialists, and a well-defined user community (largely the military and foreign policy/diplomatic community). Information was highly compartmentalized with fixed channels through which it flowed (largely vertically up through the intelligence channels until “finished” then laterally to users).

Because of the diverse, constantly adapting, and furtive nature of the new security threats, “hard-wiring” the analytic and user communities is not only difficult, but also counterproductive. Relevant information comes from a much wider range of sources (dedicated intelligence collectors, users themselves, state and local officials and the private sector), and it is difficult to know *a priori* what information will prove relevant to analysts or useful to users. For this reason, it is necessary to create a more horizontal, cooperative, and fluid process for intelligence collection, sharing and analysis. A good example is the virtual chat room used by the U.S military in the Afghanistan war, when the full range of actors and information (from sensor data, to imagery analysts, to experts on Afghanistan to fighter pilots) could interact in real time with access to the same data. New teleconferencing technologies may make it possible to engage in even more sophisticated community creation.

Key required features of this virtual community include the following:

- relatively open access (reduction or elimination of pre-clearance, need-to-know barriers) to the information base assuming basic levels of security clearance for trustworthiness;
- accessible platform/portals available to all potential users (modeled, perhaps, on DoD’s SIPRNET)⁹; and
- common cross-community technical standards drawn, if at all possible, from existing technologies and protocols. These should include the following:
 1. communication standards including TCP/IP;
 2. compatible databases (or alternatively, meta indexing or directory systems that can draw on existing but noncompatible technologies) that allow for sharing and integrated analysis; and
 3. data protocols that facilitate sharing while protecting especially sensitive information, such as sources and methods.

An important virtue of such an arrangement is that it avoids “turf” problems, since no single agency would own the process. But it would create a new opportunity for the standard-setting agency to leverage the ways that individual agencies operate to facilitate synergies among agencies.

2. Accountability

Although the virtual community has the advantage of empowering a broader community to contribute information, expertise, and perspective, by itself—given the horizontal nature of the network—there is a risk that no actor will be responsible for harnessing the power of the framework. Therefore, the network structure must be augmented by arrangements that ensure the following: 1.) that information in fact flows to all who need it; and 2.) that information is provided to decisionmakers and policymakers with responsibility and authority to act, who are ultimately accountable to the public for the performance of the system.

3. Linking Information Collection, Analysis, and Users

As noted above, in the new security threat environment, the line between collectors, analysts, and users is increasingly blurred. In addition, the relevant community of collectors, analysts and users extends beyond the federal government to include state and local governments and the private sector. This means strategies will be necessary to facilitate connectivity of information flows across inter-governmental and public/private lines in both directions. These strategies include the following:

- providing appropriate technology to state and local governments and the private sector to allow them both to provide and to receive information in a timely manner;
- eliminating barriers to information flows across the public/private boundary (including, where appropriate, liability rules, FOIA, Privacy Act, and antitrust limitations);
- facilitating coordination at the local level (integrated task forces), connected in a two-way flow to federal authorities, and convened by a representative of the DHS; and
- increasing ongoing interaction with users/policymakers to sensitize them to the analytic challenges and to provide the analytic community with a more operational sense of how information/analysis will be used.

4. Attracting Expertise

A common critique of existing efforts is the lack of expertise in the government’s analytic community—be it language, regional/cultural experience or scientific and technological expertise. While it is possible to increase the capabilities of the federal government through greater resources and incentives, the virtual community model provides a way of tapping into expertise beyond the federal work force, and a way to continuously adapt the mix of skills as the environment evolves. For the federal intelligence/analytic work force, particular emphasis needs to be placed on developing the analytic and data skills that can take advantage of new information-based technologies.

5. Data Quality

Both the threat and vulnerability analytic frameworks depend heavily on data collection and management tools. But these are only as useful as the quality of the data collected in the first place. Thus special emphasis needs to be placed on the quality of the “first tier”—data input. This means well designed protocols that are both useful and realistic given the nature of the collector (for example, not expecting highly detailed syndrome data to be collected and reported by emergency room physicians).

Data quality also has significant civil liberties implications, so procedures need to be devised to assure high degrees of accuracy without compromising security (*e.g.*, giving potential terrorists access to their records in the name of assuring accuracy). There is also the related privacy concern with respect to mega-databases. There is a clear tradeoff between protecting privacy through limits on who can access databases and maintaining the open nature of the virtual community as described above.

RECOMMENDATIONS

The imminent creation of a new Department of Homeland Security provides a unique opportunity to implement the concepts identified in this Report. Under the administration’s proposal, the new Department is charged with both threat and vulnerability assessment. In addition, the Department will have broad-ranging responsibilities for key parts of the user community, including border and transportation security, emergency response (with ties to state and local governments), and infrastructure protection (thus with important ties to the private sector).

An urgent task of this new Department should be to take the lead in setting in motion both the substantive strategic analyses and the creation of the virtual analytic community described above. Although the Department will “own” key elements of this community, it is critical that the Department itself not “own” the process, since fundamental elements of collection, analysis, and use (such as the CIA, FBI, Treasury, HHS/CDC, etc., not to mention state and local governments and the private sector) will remain outside the Department, no matter what form it finally takes.

The creation of this virtual community and the implementation of new forms of strategic analysis will not happen overnight. We need a sense of time scale—what can and must be done immediately, and what can be phased in over time.

In the short term, the new all-source analytic unit at the DHS could immediately implement the strategic analysis strategies identified above in Section A since both provide a framework for the Departments assigned mission.

With respect to creating the virtual community, this could be phased in over time. As an interim measure the Department could do the following:

- establish an inventory of all relevant collectors, analysts and users;
- establish an inventory of databases and data repositories;
- identify technical and operational (“work around”) bridges between key elements to facilitate communication during the period in which individual users continue to use non-compatible systems;
- establish local task forces that would include all key actors from the federal, state and local governments and the private sector to facilitate local real and virtual communities;
- review barriers to information flow between the public and private sector, and either act through Executive Order or propose legislation to make necessary modification; and
- convene an ongoing private sector advisory group to facilitate adoption of advanced IT technologies and strategies into the Department’s analytic work.

Meanwhile, on a more long-term time scale, the Department should begin to establish the infrastructure that would make possible an integrated virtual community. This would include the following:

- identifying a common information platform for the virtual community with procedures that provide for basic security of access while assuring that all classes of potential participants will have access;
- establishing database and information-sharing standards to be used by all would-be participants in the virtual community;
- providing technical standards and funding that would support connectivity for state and local users; and
- identifying personnel and skill needs, and developing recruiting and training strategies to enhance analytic capabilities at all levels.

ENDNOTES

¹ This approach thus helps break the straitjacket imposed by the concept of limiting planning to “validated” threats (an approach which drives much military planning) since by definition, surprises are unlikely to present the kind of evidentiary predicate that would “validate” a threat. In this sense, the approach here bears some similarity to Secretary Rumsfeld’s suggestion of a “capabilities” based approach to military planning.

² The Working Group identified, but did not try to resolve, the difficult question of the impact of large numbers of small attacks (e.g. individual suicide bombers using crude conventional explosives), and the difficulty of using horizontal analysis of this kind to detect and thwart such attacks.

³ This approach is developed in O’Hanlon et al. *Protecting the American Homeland*, Brookings 2002.

⁴ The idea is to focus information collection on individuals who seek access to key sites or materials, for the purpose of pattern and anomaly recognition, and also for use against reference database(s), either compiled from information previously collected at the priority checkpoints (e.g. individuals repeatedly trying to access a sensitive computer site), or from other sources (such as a watch list developed by threat-based analysis of a terrorist organization).

⁵ An illustrative example of such a template would be an attack on the U.S. electrical grid. The development of such a template would guide various aspects of intelligence collection (e.g. surveillance of critical transformers and cyber-infrastructure such as control devices associated with the operation of grids, counter-surveillance on websites that

provide information on the electrical grid) and point to remedial measures (e.g. elimination of single node failure points, enhanced security at key nodes, etc.).

⁶ See Horowitz, Barry M. and Yacov Haimes, “*Risk Based Methodology for Scenario Tracking for Terrorism: A Possible New Approach for Intelligence Collection and Analysis*,” unpublished paper from the Center for Risk Management of Engineering Systems, University of Virginia, July 22, 2002.

⁷ See, e.g. *Defense Science Board Task Force on Intelligence Needs for Homeland Defense*, Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., January 2002, pp. 21-22.

⁸ For example, data mining across two databases (workers in pharmaceutical research laboratories and airline ticket purchasers) might reveal that an individual who worked in a sensitive lab also bought a round-trip ticket to Kabul. This correlation would match with a scenario (man- or computer-made) of creating a manmade pathogen for a bioterror attack.) This might lead to a further database search of previous work histories of researchers in the lab—which might reveal that the individual in question graduated from Jihad U (thus reinforcing the probability of the scenario), or alternatively, that she was on secondment from WHO doing research on diseases of the Afghan highlands (and therefore tending to discount the probability of the scenario). The advantage of computer-generated scenarios is that very large numbers could be created without the unintended constraints of human definitions of “likely” or “plausible”, thus decreasing the chances of surprise through novelty.

⁹ SIPRNET (SECRET Internet Protocol Router Network) is a dedicated DoD wide data transmission network at the “secret” level, which provides for a degree of security since clearances and authentication are required, but without the constraints of higher level, compartmented information. An alternative might be the creation of a secure virtual private network that rides on the open internet.

REPORT OF THE WORKING GROUP ON ACQUIRING INFORMATION-RELATED TECHNOLOGY

This Working Group was chaired by Abraham D. Sofaer, who drafted this report on behalf of the group. Participants in this group were Robert Atkinson, James Barksdale, Jennifer Barrett, Eric Benhamou, Bruce Berkowitz, Wayne Clough, Esther Dyson, Dave Farber, Slade Gorton, Tara Lemmey, Gilman Louie, Judith Miller, Harvey Nathan, Michael Turner, Michael Vatis, Gayle von Eckartsberg, Rick White, and Philip Zelikow, with assistance from Mary McKinley.

ACQUIRING INFORMATION-RELATED TECHNOLOGY TO COMBAT TERRORISM

I. The Need for Advanced Technologies

The U.S. effort to prevent and respond effectively to terrorist acts depends on using advanced technologies. President Bush's call for a Department of Homeland Security (DHS), and the National Strategy for Homeland Security, issued on July 16, 2002, are designed in part to enable the nation to take full advantage of its technological edge. The National Strategy recognizes that "the nation's advantage in science and technology is a key to securing the homeland," and it calls for a "systematic national effort" to deploy "new technologies for analysis, information sharing, detection of attacks, and countering chemical, biological, radiological, and nuclear weapons."

Advanced technologies can help attain many potential improvements in the nation's capacity to prevent and respond to terrorism. Some commonly cited information-related areas in need of improvement are as follows:

- data collection, integration, and mining
- data analysis for management and risk control (reference databases)
- sharing of information across multiple databases (watch lists)
- secure communications networking for real-time crisis management
- systems for identifying and responding to conventional, chemical, biological, and nuclear threats
- systems for enhancing personal security controls through identity recognition and access management
- systems for enhancing physical security controls of vehicles and cargo
- enhanced, secure, wireless point-to-point communications

Almost all of these requirements have been recognized for years, by Congress, presidents, OMB, GAO, national laboratories, and private entities. Yet, repeated calls for enhanced use by federal agencies of advanced technologies have largely been ineffective, and the United States remains remarkably ill equipped to handle the challenges that homeland security presents.¹ The National

Strategy recognizes this, and rests on the premise that the U.S. government’s widespread failure to adopt necessary and even mandated technological innovations would be overcome once most homeland security functions are consolidated into one department. It states the following:

To date, research and development activities in support of homeland security have been underfunded, evolutionary, short-term in nature, fragmented across too many departments, and heavily reliant on spin-offs from the national security and medical sectors. Many of the involved agencies have little frontline knowledge of homeland security and little or no experience in technology acquisition and supporting research. The new Department would be responsible for overcoming these shortfalls by ensuring the pursuit of research and development activities where none existed previously.

Merely stating that the new Department would be “responsible for overcoming these shortfalls” will not enable it to do any better than its preexisting, component agencies have done. Consolidating agencies involved in homeland security will not ensure the development of new capabilities, functions, and techniques.² What Task Force member Ashton B. Carter has said about consolidating agencies into the DHS applies equally to the proposed consolidation of technology acquisition programs: “DHS should not just bring order to existing functions, but should accomplish new functions, especially development and practice of new types of ‘intelligence’ and new technology and techniques for homeland security.”³ To make a difference, the new agency formed to regulate homeland security must actually deploy those technologies best suited to make the nation secure. That will be achieved, not by consolidation alone, but by overcoming the barriers that have thus far interfered with or prevented achieving this goal.

II. BARRIERS TO UTILIZING NECESSARY TECHNOLOGIES

What are the barriers that have prevented the U.S. government from utilizing the best possible information-related technologies? Among the difficulties and inefficiencies in the government procurement process that have long been recognized are the following:

- inadequate acquisition planning
- complexity and rigidity of procurement processes
- security classification issues
- existence of legacy systems
- unresponsive regulatory environment
- liability and intellectual property issues for the private sector

This formidable set of problems is exacerbated in connection with cutting-edge information-related technologies. Government agencies have talented scientists and managers, and some exceptionally capable technology centers.⁴ But government agencies typically lack personnel with the expertise to understand, conceptualize, and formulate solutions for their information needs.⁵ They are also often unaware of potential solutions that exist in the private sector for their information management problems. Knowledgeable private sector contractors widely view government officials as incapable of even understanding their technological needs, and as unwilling to risk taking positions

when difficult choices need to be made. Those agencies that have acted have often attempted to adopt comprehensive solutions that take years to implement and tend to be outdated before they are fully in place. Agencies have failed to plan their information strategies based on their missions, and they lack the ability to develop information infrastructure plans,⁶ without which no amount of effort can produce acceptable results.⁷

Understandably, agencies have reached out to information experts for assistance in overcoming these difficulties. Private companies are currently doing a very substantial portion of the IT work of federal, state, and local governments,⁸ and federally funded research and development centers (FFRDCs) are doing much of the research and development.⁹ Delegating complex, mechanical tasks has proved helpful, and the FFRDCs are more productive than government centers would be. But hiring outsiders to come into agencies and craft solutions for the fundamental problems that cause inadequate utilization of information and other technology has proved ineffective. Outsiders, no matter how expert, and even if given broad authority as chief information officers (CIOs), are often unaware of the operational details of the working levels of their agencies. Affected workers, who are seldom included in developing these solutions, often view such efforts with suspicion and skepticism. Experience has demonstrated that the “top-down” solutions outside experts have typically provided are unsuited for identifying and satisfying information needs in an operationally effective manner. Outsiders, frustrated by the problems their reform efforts generate, frequently leave their posts well before completing the programs for which they have been retained.

Problems in the private sector also help explain the failure of government to satisfy its information-related technology needs. First, many of the technological capacities needed by government agencies to deal with terrorist threats have not been developed. In general, moreover, the ability to develop these technologies exists largely in the private sector, where funding has recently become difficult to secure from private sources. A real need currently exists for “seed” capital from government. The smaller companies most likely to produce elements of necessary advances are, in addition, poorly equipped to deal with the government’s conventional procurement rules and procedures. These companies are also in general unable to develop usable systems for deployment; their contributions must be coordinated and consolidated with other technologies into products or solutions by groups able to work with both private sector contributors and government customers.

The need for reforms in government procurement to overcome these barriers is widely recognized. Studies routinely call for legal reforms and the removal of bureaucratic obstacles.¹⁰ Some legal and regulatory adjustments are, in fact, necessary for effective reform. But the need for formal changes in procurement rules is overstated. Established devices already being utilized in existing agencies have greatly alleviated difficulties traditionally associated with procurement. The most significant of these are included in the Administration’s proposed legislation to create the DHS, and Congress seems prepared to adopt those provisions (and perhaps others) on at least a trial basis.

Ad hoc reform of existing procurement rules will not suffice, however, to ensure that any new homeland security agency is structured and empowered to achieve government-wide, mission-oriented planning, development, and deployment of the best information technologies. Actual deployment of advanced technologies can only be achieved by building into the new DHS capacities and mandates designed to provide needed expertise and to overcome practices and “cultural”

realities that currently prevent effective technology utilization. This will require, as both the President and Congress recognize, new entities within and outside the new Department that are assigned new activities, and that involve and exploit private sector resources in new and more productive ways. The public/private mix must be changed far more radically than is presently planned. The analytic, planning, research, testing, and development processes must be opened up to a far broader spectrum of non-governmental players than is currently the case, and the standard for adequate performance must be raised dramatically. In addition, when it becomes clear that the deployment of certain technologies is essential to homeland security, Congress and the Administration should demand more than business as usual from the DHS and other responsible agencies. They should require the DHS to institute special projects to focus on and achieve the rapid and effective development and deployment of exceptionally necessary technologies and capacities, and should provide the institutional arrangements and funds required for such projects.

III. ENSURING GOVERNMENT DEPLOYMENT OF NECESSARY TECHNOLOGIES

A. Improving Procurement Procedures

Commissions and Congress have repeatedly examined government procurement activities, and numerous reforms have been implemented to enhance efficiency and provide flexibility.¹¹ The draft Homeland Security Act of 2002 incorporates powers developed in response to the need for flexible procurement laws. Thus, Section 732(a) of the proposed law would authorize the Secretary of the new Department to utilize the authority granted to the Secretary of Defense under 10 USC, Section 2371 to engage in “transactions other than contracts, grants, and cooperative agreements” when carrying out “basic, applied, and advanced research and development projects.”¹² This power to engage in “Other Transactions” (OT) would add considerably to the new Department’s potential effectiveness in fulfilling its purposes.¹³ In particular it would enable the DHS to form joint ventures with private companies, and to accommodate the strong desire of companies with valuable intellectual property assets (or aspirations) to retain the power to exploit their discoveries while licensing to the government. These devices will, in turn, enhance the government’s capacity to raise private sector funds for projects intended to serve public sector needs and to help in encouraging high-tech companies, entrepreneurs, and technicians to work for or with government under conventional employment or procurement strictures.¹⁴ This authority should not be limited to five years, as bills adopted by the House and Senate provide.

The proposed legislation includes two other significant authorities. Section 732(b) would allow the Secretary to procure “personal services, including the services of experts and consultants (or organizations thereof)” without regard to the limitations in 5 USC Section 3109 that such services be obtained by direct hire under competitive appointment or other procedures under civil service laws. This provision will enable the Secretary to create employer-employee relationships with experts whose services could not readily be secured under civil service requirements. It should not be limited to periods of employment of one year, as Congress presently seems willing to allow.¹⁵ Specific efforts should be required to train individuals to become experts in the application of the Federal Acquisition Regulations, which control procurement. The regulations have significant flexibility, but they are extremely complicated, and only individuals who know and can apply them competently are able to take advantage of the flexibility provided.

Section 732(c) would add the DHS to the list of agencies in Section 602 of the Act of June 30, 1949 (40 USC 474) that are empowered to avoid the application of any procurement statute or regulation that would impair accomplishment of the Department's mission by limiting authority for necessary purchases or disposal. These provisions should be examined to determine whether the exemptions are themselves too limited to satisfy the DHS Secretary's likely requirements.

Congress should also ensure that special legal authorities now available to some agencies in acquiring information technologies are made available to the DHS.¹⁶ These provisions are useful, but Congress has heretofore failed adequately to support multi-agency technology improvements and projects. Experts agree that such projects are essential to enable the government to learn to share information across agencies and engage in other cooperative efforts. One underlying problem is that Congress' appropriations process does not support multi-agency activities, because the committee structure is divided largely along agency lines. Congress must address this deficiency in the DHS legislation. Bills passed by the Senate and House would allow the DHS to engage in joint projects with other agencies. One bill, for example, would allow DHS to spend certain categories of funds through the Department of Energy pursuant to agreements to develop certain technologies.

B. Creating New Capacities for Homeland Security Technology

A successful homeland security plan, in addition to including the necessary resources, personnel, and legal authority to achieve the plan's objectives, must call for organizational capabilities for providing the expertise, focus, and continuity needed to ensure that technology-related requirements are satisfied. Experience has demonstrated that conventional government mechanisms will fail to deliver technological improvements in a timely manner, if ever. Technological progress depends, not only on a centralized, empowered and well-funded government leadership,¹⁷ but also on creativity, skilled planning, knowledge, experience, and effective implementation. Government can "marshal and direct" these resources,¹⁸ but the resources themselves must necessarily be drawn from private sector experts, who, in fact, create and use most advanced technologies.¹⁹ This point is made clear by the fact that 80% of the nation's infrastructure is owned and operated privately. It is this fact that caused President Bush to mandate government officials to establish concrete mechanisms for public/private cooperation.²⁰

The range of issues the proposed DHS will face, moreover, is certain to be vast, and to include highly complex scientific and engineering problems at the cutting edges of many areas of expertise. The sheer complexity and array of tasks facing the new DHS Secretary makes it unreasonable to expect that acquisition issues will receive the depth and intensity of attention they require unless new mechanisms are created—mechanisms that are designed to encourage innovation and success. These mechanisms must require government to consult with and rely upon individuals who are capable of conducting mission-oriented planning and are aware of the best available technologies to accomplish those missions. The planning and acquisition of information technology, in particular, should be structured to avoid the top-down, inflexible, and ineffective initiatives that have done much to undermine Congress' confidence in the government's capacity to spend money constructively on information initiatives. Congress should consider using as a source for ideas the Internet Engineering Task Force (IETF), the principal body through which Internet technology has been shaped and regulated.²¹ While the Internet is a product of government-sponsored research, it

has been built up to its present virtually universal acceptance by a group of private sector experts, who have collaborated as volunteers in a structured yet open format. Government agencies cannot be expected to function in precisely the same manner as the IETF, but they would benefit from the disciplined, creative, and diverse input of private sector experts.

As discussed below, the changes proposed by the Administration and included in bills passed by the two houses of Congress are inadequate. They permit, but fail to require, the new agency and its officials to break with past practices and include innovative and open planning and technology development. Rather than the many offices and centers that would be created by pending legislation, Congress should create essentially two, new entities with built-in private sector participation and authority: (1) a government department, or Center for Technology, under the direction of the DHS Under Secretary for Science and Technology; and (2) a non-government entity, or Institute for Technology, created to serve DHS, that is assigned meaningful roles in setting and implementing the technology agenda, as well as given the task of developing and deploying on an expedited basis particular technologies considered essential to homeland security.

1. DHS Center for Technology and IT Support

The Bush Administration has recognized in proposed legislation to create a new DHS, as well as in its National Strategy, the importance of deploying the best possible technologies in homeland security. The Administration also recognizes that, in order to harness science and technology in the war on terrorism, the DHS must rely on the private sector. “The private sector has the expertise to develop and produce many of the technologies, devices, and systems needed for homeland security. The federal government needs to find better ways to harness the energy, ingenuity, and investments of private entities for these purposes.”²² The DHS is to take the lead in overcoming the obstacles to using private capacities that the Administration recognizes exist: lack of experience and/or desire to work with the federal government due to rules and restrictions; lack of programs that solicit research and development proposals related to homeland security; lack of experience within agencies in acquiring technology; and lack of adequate funding and planning for security technology. With regard to information technology, the Administration would assign to DHS the task of securing better systems, once again with private sector advice, as well as the task of securing more cooperation among federal agencies and others in sharing information by overcoming both technological as well as “cultural” barriers.

The Administration proposes a general plan and several specific programs to achieve its objectives. The general plan is to create within the DHS “a management structure to oversee the agency’s research and development activities and to guide its interagency coordination activities.” To this end, the DHS is to engage in “constant examination” of vulnerabilities, “continual testing” of security systems, and “updated evaluations” of risks; it is to establish a “national laboratory” for developing and demonstrating new technologies; to solicit independent and private analysis; to set standards for equipment; to establish mechanisms for rapidly producing prototypes and for “high-risk, high-payoff” research; and to conduct demonstration and pilot deployments. The DHS would, with regard to information, coordinate the sharing of information, the government’s acquisition of information systems, and the overcoming of legal and cultural barriers; adopt common “meta-data” standards for electronic information related to homeland security; and improve public-safe-

ty emergency communications.²³ At no point, and on no issue, does the Administration propose any definitive or authoritative role for private sector experts or institutions; and virtually every proposed use of non-governmental resources deals with institutions, entities, or ideas that already exist, such as use of the national laboratories.

It is essentially this plan that both houses of Congress have adopted in two bills that at the time this paper was written were being considered in conference committee. Both bills establish a management system within the DHS to determine technology needs and ensure production, testing, acquisition, and deployment. The Secretary of the DHS is assigned these tasks in general terms, and an Under Secretary for Science and Technology is given direct responsibility for most of the anticipated activities.²⁴ In addition, the bills create several other offices that are given significant responsibilities for evaluating and acquiring technology; among these is an Under Secretary for Information and Infrastructure, who would be assigned the task of determining technological needs for information systems and their protection.²⁵ To coordinate the technology-related activities of the many offices and programs that would be created, the bills would also establish bodies assigned that task, such as the Homeland Security Science and Technology Council, described in the House legislation,²⁶ or the somewhat different Council described in the Senate bill.²⁷ Both bills also contain provisions authorizing the use of national laboratories and private sector experts and resources for various purposes, suggesting recognition that such advice is needed.²⁸ Some provisions require the agency to supply some information to the private sector, or to establish methods for private entities to obtain information from the agency.²⁹ The Senate bill does, moreover, signal a clear intent to support private sector research and development, particularly of critically important technologies.³⁰ But neither bill requires any use of private sector advice, and neither mandates any specific role to any private person or entity.³¹ Both bills give DHS officials or entities exclusive responsibility for planning, research, development, and deployment of technology, including information technology.³²

The Administration and the bills passed by the two houses of Congress have the correct objectives. The DHS must have ultimate responsibility for the government's technology programs, and given the many functions to be assigned to the DHS, it is essential that an entity be created under the projected USST to coordinate technology activities for all DHS agencies and departments. That entity should, however, be given clear authority over all technology-related proposals and functions, regardless of the number of issues assigned to officials other than the Under Secretary for Science and Technology. Further, an individual with technical and private sector experience, appointed by the DHS Secretary, who works as a full-time Director under the Under Secretary for Science and Technology, should run it. The entity should have within its structure, and subject to its coordination, all the government laboratories and specialized bodies that have technology-related missions and are included in the DHS.³³ It should be provided with multi-year budgetary support, including funds to be used for interagency IT activities, and for monetary awards to individuals (and departments) at the DHS who perform exceptionally well in implementing IT initiatives. Among other things, the DHS Technology Center should be required to review all major IT infrastructure proposals made by, or on behalf of, any DHS entity, and to evaluate and, where appropriate, to certify such proposals to Congress as warranting legislative support.³⁴

The Center should be designed with specific roles for private sector experts. Its membership should include not only leading DHS and other agency officials, but also the heads of national laboratories and one or more businesspeople, academics, and scientists. These skilled outsiders should rotate over time to ensure fresh perspectives. While they serve, however, they should be full participants in the work of the Center, with the right to convey their individual opinions to the Secretary. The Center would be far more likely to call upon and give credence to private sector analysis and standards if it has some distinguished private sector participants. The Center will also be more effective at assigning work to, and evaluating the work of, a non-governmental entity established to enhance technology utilization.

2. Non-Governmental Technology Institute

The idea of having an expert entity guide the federal government on technological issues has been endorsed in principle in the National Strategy. The Administration supports creating “a laboratory—actually a network of laboratories—modeled on the National Nuclear Security Administration laboratories that provided expertise in nuclear weapon design throughout the Cold War.” But the national laboratories already exist, and their mere availability has proved insufficient. While the National Strategy anticipates that a “central management and research facility” may be created, even *that* is not mandated, and the plan gives no special authority or role to the facility. Instead, it reads as continuing and perhaps expanding the use of scientific resources available at existing laboratories. Repeated references are made in the National Strategy to non-governmental expertise, and “centers of excellence,” but once again nothing is proposed in that document or in the draft legislation that would vest any particular role in any private entity or individuals.

The bills passed by Congress also support making available additional non-governmental resources and expertise to enable the DHS to enhance its utilization of technology, as described above. The provisions for technology acquisition contained in these proposals would provide enhanced organizational elements, but no new capacities to overcome recognized and crippling deficiencies. These provisions would essentially continue, or, at best, marginally expand existing opportunities to utilize non-governmental resources. More is needed. It is inadequate, for example, merely to enable the DHS to “solicit independent and private analysis for science and technology research” on an ad hoc basis; Congress should ensure in the legislation establishing the DHS that independent, private expertise is a permanent feature of the agency’s structure, and a resource that must be used. The Administration and Congress should create a non-governmental entity—a technology institute—that has a clearly defined structure and fulfills specific roles needed to improve government performance.

The concept of creating an independent institute with significant functions in defining and achieving federal technology objectives has important support. A panel of distinguished scientists and engineers on the National Research Council Committee on Science and Technology for Countering Terrorism recently proposed that the challenges associated with deploying advanced technologies can best be achieved by creating a Homeland Security Institute empowered and funded to enable government to fulfill the mandate of using the best available technologies to protect the American people.³⁵ The panel studied prior reports and evaluations concerning the use of technology by government agencies in the national security arena. They concluded that “America’s historical strength

in science and engineering is perhaps its most critical asset in countering terrorism without degrading our quality of life,” and that the nation had to take advantage of its “immense capacity for performing creative basic research, at universities, government laboratories, industrial research facilities, and non-governmental organizations.”³⁶ The panel agreed that a central office should be created that would be responsible for strategy and coordination,³⁷ but it frankly stated its belief that the federal government lacked the capability to perform these roles: “The committee believes that the technical capabilities to prove the analysis necessary to support this organization do not currently exist in the government in a unified and comprehensive form. Thus the committee recommends the creation of a Homeland Security Institute to serve the organization setting priorities for homeland security.”³⁸ In its report concerning information systems, the Committee makes clear the special importance of acquiring the technology needed for effective protection, and the special need to rely in this area on private sector expertise:

All phases of counterterrorism efforts require that large amounts of information from many sources be acquired, integrated, and interpreted. ...Thus, information fusion and management techniques promise to play a central role in the future prevention, detection, and remediation of terrorist acts. Unlike some other sectors of national importance, information technology is a sector in which the federal government has little leverage. Thus, constructively engaging the private sector by emphasizing market solutions seems a desirable and practical way for the government to stimulate advances that can strengthen the nation’s information technology infrastructure.³⁹

The concept of an institute to provide expert support for all aspects of the DHS’ technology work is strongly supported by the distinguished members of the President’s Council of Advisors on Science and Technology, as well as by Dr. John J. Hamre, former Deputy Secretary of Defense, and a member of this Task Force.⁴¹ The DHS is far more likely to succeed in exploiting the technological potential of the United States if the agency has, and is required to use, the advice and assistance of an institute of the sort so strongly supported by the nation’s scientific elite. The legislation creating the DHS should therefore also create an institute whose authority and procedures are structured to enable it to succeed in accomplishing the technological objectives the Administration and Congress properly seek. Here are some ideas on the key issues.

Structure. The institute should be, as the NRC Committee recommends, “located in a dedicated, not-for-profit, contractor-operated organization” that is committed to serve, but outside the DHS.⁴² Its executive director should be an expert in some relevant technology, appointed by a non-partisan board of directors chosen by the President and Congress, and including public sector (federal, state, and local) CIOs and private sector experts as members. In addition, the institute should have a relatively large body—a scientific assembly—composed of agency CIOs and experts, private sector participants, and state and local officials. The scientific assembly, or some similar body, should be empowered to propose and regularly review and comment on institute activities. It should operate through committees, whose members should be selected on the basis of experience and expertise. The committees should perform the initial research and study on technology-related tasks assigned to the Institute by Congress or the DHS Secretary, or spontaneously undertaken on the basis of assembly resolution. These committees should develop proposals for assembly and board consideration, including protocols and certification standards, and should conduct pro-

grams to satisfy other institute responsibilities. Committees should welcome, to the extent possible, the participation of qualified experts on a voluntary basis, in order to inculcate an atmosphere of creative interaction, analogous to that of the IETF.

Tasks. The Institute should perform, or monitor the DHS performance of, the most demanding tasks assigned to the DHS, such as developing and implementing the DHS IT architecture; preparing and implementing necessary protocols for information-related activities, including those necessary to assure meta-data capacities that enable systems to be interoperable, for reliable security and storage of data, and for access by state, local, and foreign participants;⁴³ developing standards for information-related technological products such as identification cards; certifying private sector products that meet government requirements, and providing guidance concerning such products to federal, state, and local officials; monitoring and reporting to the DHS Secretary, the President, and Congress, on all government-funded information-related technological research at government labs or in the private sector; providing accessibility and responsiveness to private sector developers and vendors by screening their products and proposals, thereby lowering barriers to market entry, aiding R&D, and enhancing competition; searching throughout the world for technologies that could prove useful to agencies; generating ideas to enhance security through technology; developing standards for achieving security-related objectives with minimal intrusion on privacy and other recognized civil liberties; deploying funds through private entities such as the government-owned venture capital fund, In-Q-Tel, to provide “seed” or other capital needs for promising technological innovations; and recruiting and placing talented high-tech people in DHS agencies.⁴⁴ To perform these roles, the Institute should possess the expertise required to deal with scientific issues and technological objectives in the full range of relevant disciplines.

Powers. Congress should empower the institute to perform at least some of the functions listed above, such as the tasks of evaluating major IT proposals and of screening technologies proposed for use by private companies. In addition, Congress should authorize the DHS Secretary, GAO, or the President to assign to the Institute any relevant task, and should itself assign the institute the task of developing and deploying particularly important technologies.

The institute should rely upon persuasion rather than compulsion. Information specialists widely believe that mandated changes, imposed without consideration of the needs of users, are likely to fail. Protocols, rather than inflexible standards, should set operational requirements, leaving room for innovation and experimentation consistent with operational necessities. The institute should, however, be empowered to advise the DHS Secretary, or Congress, if it concludes that any DHS entity is failing to adopt appropriate methods or technologies.

Budget. The institute should not be wholly reliant on annual appropriations. It should be required to engage in many, long-term efforts, including special development and deployment projects of the sort described below. Congress should therefore provide funds for the institute in multi-year tranches, where appropriate, subject to annual review.

Conflict of Interest Limitations. Institute personnel, including board, assembly, and committee members, and consultants, should be required to comply with strict, open standards regarding disclosure and participation. No person should be allowed to decide or vote on any matter in which

he/she has a financial interest. It will be necessary to rely on experts and consultants, however, at all levels of the institute, who have various levels of involvement in particular fields. The participation and opinions of such individuals should be allowed, subject to full disclosure of their interests.

Special Projects. The DHS Secretary and/or the institute should be authorized by Congress—and where appropriate even required—to establish special projects to expedite development or deployment of technologies needed to satisfy specific requirements critically important to homeland security. Experience in government acquisition has demonstrated that, in the face of urgent needs, the United States has been successful in developing and deploying technologies by establishing special projects for those purposes. The Manhattan Project is the most famous of such initiatives; others include the Fleet Ballistic Missile Program; the original work in creating the National Reconnaissance Office acquisition system; the Y2K Project; and the Army's Force 21 initiative. These programs are characterized by the following: (1) a recognized, time-driven need of the highest priority; (2) funding stability sufficient to overcome the uncertainties of the normal, annual approval cycle; (3) funding levels sufficient to meet project deadlines; (4) a cooperative relationship between government and contracting entities based on teamwork rather than the adversarial relationship that normally exists with contractors; (5) continuity of personnel within both the private and government entities involved; and (6) small government/contractor program office teams empowered with complete end-to-end contracting and execution responsibility, including technical development, production, installation, and operational support. Projects may, but need not, be located at specific, secure locations.⁴⁵

Among the specific technological requirements widely recognized as necessary for homeland defense are sensors capable of identifying the full range of threats in a timely and reliable manner;⁴⁶ bridging the information gap that exists between agencies for the purpose of permitting access to information that may lead to identifying dangerous individuals (i.e., a watch list);⁴⁷ and developing a system to track all aliens in the United States.⁴⁸ Congress has indicated it is prepared to order specific projects aimed at producing security results based on technology. In creating the TSA, Congress ordered the installation of explosive detection systems, or the use of alternative methods, to screen luggage on passenger planes by the end of 2002. The deadline is unachievable, and Congress seems prepared to extend it for a year. But the decision to force such screening has expedited development of the necessary technology. Coupled with a plan and resources, such efforts would have an even greater impact on security.

IV. CONCLUSION

The call for enhanced use of technology to prevent and respond to terrorism is valid and deserves a credible and effective plan for action. Government must set the nation's objectives and the policies needed to procure the best possible technologies. Government possesses neither the capacities nor the culture, however, to create and deploy new technologies in an efficient manner. To assign this task to government agencies that have repeatedly failed to deliver will be no more fruitful merely because the same agencies have been consolidated into one DHS. Nor will it suffice to create new government entities with new, catchy names to perform this work. None of this ensures sufficient new capacities.

The President and Congress should require the DHS to involve those people and companies actually responsible for America's extraordinary technological achievements. The legislation will be far more effective at achieving its aims concerning technology if the legislation is narrowed and simplified, and if it mandates roles for companies, individuals, and universities at every stage of planning, development, and implementation.

ENDNOTES

¹To illustrate, the testimony of the GAO's Director of Information Security Issues, Robert F. Dacey, before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, released on July 9, 2002, contains detailed evaluations of the failures of agencies to adopt mandated measures concerning the most important of all homeland targets, critical infrastructure, as well as seriously inadequate development of information sharing technologies and practices, and egregiously insufficient measures related to cyber security. The GAO concluded that the nation continues to lack a national critical infrastructure protection strategy, despite many public statements and the creation of several specialized entities on the subject. It also concluded that the new DHS would have to address "pervasive weaknesses in federal information security." On the latter issue, GAO stated:

Our November 2001 analyses of audit results for twenty-four of the largest federal agencies showed that weaknesses continued to be reported in each of the twenty-four agencies. These analyses considered GAO and Inspector General (IG) reports published from July 2000 through September 2001, which included the first annual independent IG evaluations of agencies' information security programs required by government information security reform legislation (commonly referred to as GISRA).

The weaknesses GAO identified covered "all six major areas of general controls, including security program management; access controls; software development; segregation of duties; operating systems controls; and service continuity." GAO-02-918T, p. 29.

²This point is concretely made by Jim Puzzanghera in commenting on the prospective absorption of INS into the new DHS: "But the new agencies would be saddled with the same outdated technology that has left the INS unable to effectively guard the nation's borders or cope with growing immigration." San Jose Mercury News, April 29, 2002, p.1A.

³Testimony to the Comm. on Gov't Affairs, U.S. Senate, June 26, 2002, p.1, at http://www.senate.gov/~gov_affairs/062602carter.htm

⁴For example, the National Institute of Standards and Technology, currently part of the Department of Commerce but likely to be included in the DHS, has provided measurements, standards, and technical advice related among other things to terrorist threats. See generally, "Technologies for Improved Homeland Security," describing its functions, at https://axess2.Stanford.edu/a2kprd76ha/user/campnet/cn_frameset.asp

⁵The GAO testimony, supra, calls for a "human capital strategy" to overcome the problem of properly protecting the nation's critical infrastructure. The GAO clearly recognizes that "few federal departments and agencies" have either the personnel or the management practices necessary to develop and implement technologically sophisticated initiatives, such as enterprise architecture.

⁶The GAO reports that "a March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in federal agencies' implementation of PDD 63 requirements to (1) establish plans for protecting their own critical infrastructure that were to be implemented within two years, or by May 2000, and (2) to develop procedures and conduct vulnerability assessments." GAO-02-918T, "Critical Infrastructure Protection," p. 9 (July 9, 2002).

⁷The FBI, which is not going to be made part of the DHS, has been widely criticized for its failures in information technology, despite the importance of the tasks it is assigned. Among other things, it has failed to develop an adequate strategic plan, has no comprehensive strategic human capital plan, has personnel with inadequate language skills, antiquated computer hardware and software, no enterprise architecture, and several disabling cultural traditions. See generally, "FBI Reorganization," GAO-02-865T, pp. 8-11, 15 (June 21, 2002); "How Outdated Files Hamper FBI Effort to Fight Terrorism," *Wall Street Journal*, p.1 (July 9, 2002); "War on Terrorism Highlights FBI's Computer Woes," *Los Angeles Times*, July 28 & 29, 2002. The INS has also been severely criticized for its information shortcomings. See "Homeland Security," GAO-02-886T, p.23 (June 25, 2002).

⁸ An Intellibrige Analysis reports an estimate that federal agencies will spend \$13.2 billion on private workers to manage and run their technology systems by 2006. It also quotes Norman Lorentz, CTO of OMB, predicting that outsourcing will increase far beyond current levels (August 20, 2002).

⁹ Several specific instances now exist of efforts to force agencies to use the private sector, or to adopt technologies already being used in the private sector. The Government Information Security Reform Act of 2000 (GISRA) requires agencies to integrate security programs into their computer networks and capital plans, or face budget cuts. Many agencies are reported to have begun “doing things they should have been doing long before.” “Taking Security Concerns Private: U.S. Appeals to IT Firms,” *Washington Post*, p. EO5 (June 20, 2002).

¹⁰ A CFR study calls for a “Red Team” project to create a Counter-Terror Information Technology system (CTIT) that combines data from a wide variety of border administration and security agencies, private sector firms in transportation and finance, educational institutions, and foreign sources; in a common format that can be swept by a variety of data-mining technologies; and return useful information on suspicious patterns and behavior in a timely fashion to line agents and law enforcement agencies. It states, however, that “the business-as-usual federal IT contracting approach will not create what the Terrorist Tracking Task Force needs in any reasonable time frame,” and calls for “throwing out the rulebook.” Jan M. Lodal & James J. Shinn, “Red-Teaming The Data Gap,” pp. 2-4, <http://www.cfr.org>. The Markle Task Force agrees with the need for and feasibility of bridging technologies for sharing data, though it advocates a more discriminating collection of data, and regards the procurement obstacles as far more manageable than the CFR study assumes.

¹¹ See “Reinventing Federal Procurement,” describing the many initiatives underway to modernize, streamline, and simplify procurement, available at <http://govinfo.library.unt.edu/npr/library/nprprt/annrpt/vp-rpt96/appendiz/federal.html>

¹² The DHS Secretary would be required to comply with limitations and conditions applicable to the Secretary of Defense, in using this authority, including the requirement that he/she determine “that the use of a contract, grant, or cooperative agreement for such project is not feasible or appropriate.” This limitation may prove too restrictive in dealing with smaller companies far less able to deal with government than large, defense contractors.

¹³ See generally the discussion in David S. Bloch & James G. McEwen, “Other Transactions’ with Uncle Sam: A Solution to the High-Tech Government Contracting Crisis,” *10 Tex. Intell. Pro. L.J.* 195 (Winter 2002).

¹⁴ A somewhat revised form of the same OT authority, given to the Defense Advance Research Projects Agency (DARPA) in Section 845 of the 1994 NDAA, to “carry out prototype projects that are directly relevant to weapons or weapon systems,” is also proposed to be given to the new Department in Section 732(a)(2). This, too, is a sound proposal, though the statute should be revised to make clear that the authority extends beyond “weapons” to any prototype project that the DHS Secretary finds would enhance homeland defense.

¹⁵ The Task Force supports flexible rules for key personnel needed to enhance homeland security. It has not considered the need for broader reform of personnel rules.

¹⁶ For example, federal information policy provides authority for coordination (44 USC 3504), for capital planning and investment control, and for pilot programs to “test alternative approaches for acquisition of information technology by executive agencies,” including on a multi-agency basis, and to use pilot programs to test “solutions-based contracting” for information technology acquisition (40 USC 1422, 1471 & 1492). See generally the FAR, Part 39: Acquisition of Information Technology, Vol. 1, Parts 1-51 (Sept. 2000).

¹⁷ The emphasis on internal government reform was signaled in the instructive and otherwise sound analysis in William B. Bonvillian & Kendra V. Sharp, , which at one point speculates that “the overwhelming public support for the fight against terrorism suggests that first-rate scientists and engineers would be willing to work for this entity [DHS’ DARPA] in this time of crisis.” “Homeland Security Technology,” *Issues in Science & Technology*, Winter 2001, p. 6.

¹⁸ *Id.* at 1. Mr. Bonvillian is legislative director and chief counsel to Sen. Joseph I. Lieberman of Connecticut; Ms. Sharp is an assistant professor of mechanical engineering at Pennsylvania State University.

¹⁹ The GAO explained this in commenting on the FBI reorganization: “There is also a growing understanding that all meaningful results that agencies hope to achieve are accomplished through networks of governmental and non-governmental organizations working together towards a common purpose.” GAO-02-865T, p.17 (June 21, 2002).

²⁰ Executive Order 13231, entitled “Critical Infrastructure Protection in the Information Age,” and issued on October 18, 2001, requires the Critical Infrastructure Assurance Office to establish a broad-based partnership with the private sector, to encourage the exchange of assistance on information security practices.

²¹The IETF is a purely voluntary organization that nonetheless has been able to develop and approve the standards under which the Internet operates. It taps the talents of private (and public) sector experts who are eager and able to participate in fulfilling ambitious technological missions, such as identifying and proposing solutions to operational and technical problems of the Internet; specifying the development or usage of protocols and near-term architecture to solve such problems; making recommendations regarding the standardization and usage of protocols to the Internet Engineering Steering Group (IESG); facilitating technology transfers from the Internet Research Task Force (IRTF) to the wider Internet community; and providing a forum for information exchange among Internet vendors, users, researchers, agency contractors, and network managers. See generally, *The Tao of IETF: A Novice's Guide*, RFC 3160, (August 2001). https://axess2.stanford.edu/a2kprd76ha/user/campnet/cn_frameset.asp

²² National Strategy, p.51.

²³ See *id.* at 53-58.

²⁴ E.g., H.R. 5005, Sec. 301. The Senate bill (and Lieberman amendment) describes the DHS Secretary's duties in some detail, including the duty "to identify and promote key scientific and technological advances that will enhance homeland security," and "to oversee and ensure the development and implementation of an enterprise architecture for Department-wide information technology, with timetable for implementation." S. 5005, Sec. 102(8), (16), & (17).

²⁵ H.R. 5005, Secs. 201, 204, 206. In addition, an Under Secretary for Management would be responsible for "information technology and communications systems, and a Chief Information Officer would separately report directly to the Secretary on all information-related issues. Id. 601(4); 603. The Senate bill also would create several offices with overlapping technology-related responsibilities, including: an Under Secretary for Critical Infrastructure Protection with wide authority over key U.S. industries and cyber security; an Under Secretary for Science and Technology to run a Directorate of Science & Technology with comprehensive responsibilities for homeland security technology; an Under Secretary for Emergency Preparedness; and a Chief Information Officer. It would also create an additional layer of authority over information technology by assigning to the Director of the Office of Management and Budget the task "in consultation with" the DHS Secretary, "of creating a comprehensive architecture for information systems," as well as the task of developing a "plan to achieve interoperability between and among information systems...of all agencies with homeland security responsibilities."

²⁶ The House version of the Council would be composed of all the DHS Under Secretaries, and chaired by the Under Secretary of Science and Technology, who would decide when to call meetings. The Council would "establish priorities for research, development, demonstration, testing, and evaluation activities conducted or supported by the Department," and to "ensure that the priorities established" reflect the Department's acquisition needs. Sec. 306(a) & (b).

²⁷ The identically named Council in the Senate bill would have senior DHS officials as members, but would also include the Director of the Office of Science and Technology Policy, the Director of a new organization, the Security Advanced Research Projects Agency (SARP), and officials of the Executive Office of the President. This Council would coordinate homeland security research and development among all agencies "and entities in the private sector and academia..." recommend specific areas to fund for rapid deployment, and assist the Under Secretary of Science and Technology in developing the technology roadmap assigned to the Directorate for Science and Technology for preparation. Beyond even this, the bill would create an Office for Technology Evaluation and Transition, which would serve "as the principal, national point of contact and clearinghouse for receiving and processing proposals or inquiries regarding such technologies;" would identify and evaluate promising new technologies; test and assist in deploying them; and coordinate with SARPA to accelerate the transition of technologies it develops. If the DHS Secretary finds even this insufficient, the Secretary could assign any aspect of the Science and Technology Directorate to be carried out through or in coordination with a Technical Support Working Group or similar entity.

²⁸ H.R. 5005, Sec. 304. The House bill says the Under Secretary of Science and Technology "may establish a headquarters laboratory" for the DHS, after following certain procedures, "at any national laboratory and may establish additional laboratory units at other laboratories" p. 46. This provision adds nothing to existing resources, other than the designation of a lead lab. The bill also provides that the Under Secretary of Science and Technology "shall operate extramural research, development, demonstration, testing, and evaluation programs . . ." "involving entities from as many geographic areas as practicable and on the basis of competitions as open as possible. Within one year or enactment, the Secretary, through the USST, "shall establish" a university-based center or centers for homeland security, taking into account a number of technology and terrorism-related capacities. The next section, however, gives the Secretary "discretion to establish such centers," and requires a report to Congress on implementation. This may mean that a center will be designated, but the bill nowhere provides any particular role for such a center, or assigns it any particular responsibility, p. 44. The House bill goes through the trouble of providing for a "Special Assistant" to the DHS Secretary, who would be required to interact and foster communications with the "private sector," other agencies, national labs, FFRDCs, and academia, including creating "advisory councils" from which to

obtain advice on various issues. The Under Secretary of Science and Technology would, in addition, be required to create a “centralized Federal repository of information related to technologies” regarding possible use of unconventional weapons, and to disseminate that information to federal agencies, state and local governments, and the private sector. The Under Secretary of Science and Technology would also create a repository of information “for persons seeking guidance on how to pursue proposals to develop or deploy technologies that could contribute to homeland security,” or to assist in evaluating and implementing technologies and research and development. Sec. 301(8), (9), & (10).

²⁹ For example, the Under Secretary of Science and Technology is instructed in the Senate bill to share and disseminate research and development discoveries and opportunities with other entities, including the private sector, and to contract with or establish FFRDCs “determined useful by the Secretary” to provide independent analysis and support.

³⁰ The bill would create an “Acceleration Fund” to support technology research and development, to be used for projects selected by the newly created SARPA (in contrast to DoD’s existing DARPA), with recipients to include private sector entities or individuals, universities, or FFRDCs. SARPA would support especially “high-risk, high-pay-off” technologies that “may lie outside the purview or capabilities of the existing Federal agencies,” and emphasize “revolutionary rather than evolutionary or incremental advances.”

³¹ The Senate bill would require the DHS to prepare a “Strategy for Countermeasure Research,” or “plan for engaging non-Federal entities, particularly including private, for-profit entities, in the research, development, and production of homeland security countermeasures for biological, chemical, and radiological weapons,” and to submit the plan within 270 days of enactment for Congress’ consideration. Regrettably, this plan would not explicitly extend to information systems.

³² The House bill would create a Federal Information System Security Team, consisting of agents and scientists, to provide technical expertise to agencies (when requested). This team would assist them in securing critical information systems by conducting security audits, vulnerability assessments, and testing the effectiveness of information security control techniques. No non-government participants are provided for, despite the obvious superiority of private companies in this work.

³³ The technology-focused entities the President has asked to be included within the DHS include the three research laboratories at Los Alamos, Sandia, and Livermore, as well as the National Infrastructure Protection Center, the Critical Infrastructure Assurance Office, the Computer Security Division, the National Infrastructure Simulation & Analysis Center, the Federal Computer Incident Response Center, and the Special Adviser of Cyberspace Security. Other technology-related entities exist, within the White House and in other agencies. Congress should give serious consideration to including all these within the overall control of the Institute, in addition to the President’s personal advisor on science and technology.

³⁴ If, as one bill provides, the DHS is required to put together an overall plan for information security, or any other comprehensive plan, the Center should review it.

³⁵ *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Nat’l Academy Press 2002). The Committee is composed of 118 of the nation’s top scientists, engineers, and doctors, drawn from the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine, all independent research organizations chartered to advise the government on technical issues. In addition to an Executive Summary, the report contains chapters detailing recommendations concerning nuclear threats, threats to humans and agriculture, toxic chemicals and explosives, information technology, energy systems, transportation systems, cities and fixed infrastructure, human response to attacks, complex and interdependent systems, and various aspects of technology.

³⁶ Pages ES-19 & 17.

³⁷ The Committee recommended establishing the office of Under Secretary for Technology in the DHS to provide a focal point for guiding key research and technology programs across the department, but added “**and most importantly, engaging commitments from the major science, engineering, and medical science agencies that will remain outside the proposed new department.**” Chap. 12-6 (emphasis in original).

³⁸ Page ES-17 (emphasis in original).

³⁹ ES-9.

⁴⁰ The Council’s report to the President of July 23, 2002, spells out the case for an independent institute, and a variety of other measures. With regard to the importance of involving the private sector in the DHS’ work, it states: “Just as most of America’s critical infrastructure is private owned (85 percent), the majority of research and technology capacity resides in the private sector, i.e., in business, academia or not-for-profits. Capturing this capacity for homeland security R&D presents challenges. We believe that homeland security R&D should focus on setting require-

ments, establishing budgets, determining priorities, awarding and managing grants and contracts, testing and evaluating products, and other related functions. Most 'hands-on' R&D work can best be done in academia, industry, and national laboratories, with a very few important exceptions. ..." Draft Report, pp. 5-6.

⁴¹ Dr. Hamre, who is President and CEO of the Center for Strategic and International Studies, testified in detail on DHS issues to the Senate Committee on Government Affairs on June 28, 2002. Among other things, he called for establishment of an FFRDC dedicated to the technological support of several critical homeland security functions, essentially identical to many of those recommended in this study. Testimony, pp. 17-18.

⁴² ES-17. This form was settled upon in creating the Institute for Information Infrastructure Protection. The Institute for Defense Analyses considered the four structural alternatives, and settled on a national research and development institute for much the same reasons applicable to the present situation. See *A National R&D Institute for Information Infrastructure Protection (I3P)*, Chap. 10 (IDA Paper, P-3511) (April 2000).

⁴³ It seems dubious to assume that regular government personnel will in fact develop the meta-data standards that would enable agencies to establish interoperable information systems, as Congress still seems to assume. They lack the capacity to bring about that result.

⁴⁴ The NRC Committee proposes a similar set of functions: "The institute would perform systems analysis, risk analysis, and simulation and modeling to determine vulnerabilities and the effectiveness of the systems deployed to reduce them; perform sophisticated economic and policy analysis; manage red-teaming activities; facilitate the development of common standards and protocols; provide assistance to agencies in establishing testbeds; design and use metrics to evaluate the effectiveness of homeland security programs; and design and support the conduct of exercises and simulations." Report of the NRC, p. ES-17.

⁴⁵ The Department of Transportation's Security Agency resorted to such an approach in connection with its role in improving airport security. It invited proposals by airports to find, test, and deploy technologies needed to accomplish certain recognized requirements, including the capacity to prevent explosives from being taken onto aircraft, and to identify persons likely to pose a risk sufficient to warrant preventing them from boarding passenger aircraft. The 2002 Silicon Valley Blue Ribbon Task Force for Airport Security and Technology submitted such a proposal to the Agency, in a report that specifies the security aims of San Jose's airport and how it intends to go about achieving them. This approach will expedite identification of useful technologies and trigger intense and focused efforts to secure their effective utilization.

⁴⁶ Research is currently underway to develop sensor technologies in several government laboratories and private sector institutions. This research needs to be better coordinated, and to be made more focused on producing devices that are deployable in the near future. PR events are no substitute for actual deployment. The task is formidable. Materials that must be sensed to provide security include, in addition to metal, the nuclear, chemical, and biological substances likely to be used in bombs and weapons of mass destruction. Sensors are needed, moreover, that have the capacity to detect these materials in differing physical contexts, and at much greater distances than is now possible. Shipping containers, cars, ships, and other moving objects, are among the most likely vehicles terrorists will use in future attacks, and sensors capable of detecting the full range of suspect substances within these vehicles would greatly enhance security. Advanced sensing capabilities are also desirable at bridges, tunnels, and other critical physical infrastructure. We are far from having the capability to detect suspect substances on a timely basis in these contexts.

⁴⁷ There is widespread recognition of the need for a system that provides more than simple information sharing, "information awareness." Comprehensive databases are unnecessary impingements on privacy and other protected interests. Consolidated watch lists are needed, however, to overcome the failures associated with the September 11, 2001 attacks and other failures based on a lack of sufficient information coordination. Fashioning and deploying watch lists is well within the technological capacities of IT experts. Respected and experienced individuals uniformly claim to have created, or to be able to create, in relatively short time periods (less than six months), the technological equivalent of government watch lists far larger and more complicated than any that might be required for most government functions, such as airport and border security. Access control for such lists is readily managed through available programs that can be incorporated. A database can be designed to permit partial or complete disclosure of information to particular groups or individuals, and can be limited whenever desired to providing notice of the existence of information to which the user is invited to seek access on a need-to-know basis, or upon which the user is instructed to act in a specific manner, such as to refuse access to, or to arrest, a particular individual. IT experts suggest that an entity with authority to insist that a needed database be established, even with partial coverage and incomplete data, could provide the breakthrough necessary to put these capacities to the service of the nation.

⁴⁸ The pending bill, H.R. 5005, Sec. 435 would establish a Technology Advisory Committee on the feasibility of a system to track all aliens in the United States. This is the type of task that the Institute would be ideally suited to perform.

REPORT OF THE WORKING GROUP ON ORGANIZATIONAL CHALLENGES

This Working Group was chaired by John Hamre. This report was drafted on behalf of the group by John Hamre and Mary DeRosa. Participants in this group were Alexander Aleinikoff, Robert Atkinson, Zoë Baird, James E. Baker, Stewart Baker, Jerry Berman, Robert Bryant, James Dempsey, Amitai Etzioni, Eric Holder, Arnold Kanter, Michael Leavitt, James Lewis, Mary McCarthy, Dave McCurdy, Beth Nolan, Joseph Onek, Daniel Ortiz, Larry R. Parkinson, Harvey Rishikof, Jeffrey Smith, Paul Schott Stevens, Michael Vatis, and Philip Zelikow, with assistance from Ryan Coonerty.

Working Group III was asked to examine two issues about government organization. First, how must government structures adjust to accommodate new information needs? Second, as our approach to information collection, analysis, and sharing changes, how do we oversee these new practices and structures effectively to protect the liberties and values that define our society?

ORGANIZING FOR EFFECTIVE COLLECTION, ANALYSIS, AND USE OF INFORMATION

New security threats require new approaches to information collection, analysis, and dissemination. We no longer face only known enemies who operate almost entirely overseas. Although the terrorist threat is foreign, they operate all over the globe including, as we know so well since September 11, in this country. We know relatively little about their methods and many traditional intelligence techniques are of limited use in providing warning of their plans. The traditional compartmentalized approach to collection, analysis, and use of information about vulnerabilities and adversaries will not work with this new, dynamic threat.

To keep ahead of this threat, vastly more information must flow to and from elements within the federal government, state and local governments, and the private sector. Working Group III examined whether the dramatic changes we need to make in our approach to collection and use of information will require revisions to current governmental structures and agency roles.

The working group discussed three ways in which our institutions must adjust to satisfy these new information needs.

Remove barriers to information sharing between and within federal government organizations. The federal government must develop an integrated information system that allows sharing of all sources of information related to homeland security. This would involve not only members of the intelligence community and the FBI, but organizations such as the INS, Customs, other border agencies, consular offices, health agencies, and many other entities that come across information in carrying out their responsibilities that could be critical to uncovering terrorists' plans. Information must flow not only up chains of command, but out to the agents in the field. There has been a good deal of attention to "breaking stovepipes" since September 11 because of the many stories of important information that did not make it to people within the government who could have used it.

There already have been some improvements, largely resulting from increased use of mechanisms that were in place, but underused, before September 11. What is needed most is coordinated and sustained attention to improvement of information systems so that they are interoperable and, to the maximum extent possible consistent with security, eliminate barriers to information flow.

Develop an effective, coordinated mechanism for exchange of information between the federal government and state and local entities. State and local law enforcement, health, and other government agencies are the source of the vast bulk of domestic information that is relevant to the fight against terrorism at home. After all, the FBI has only 11,400 agents across the country; there are many hundreds of thousands of local police, sheriffs' office employees, and other government personnel collecting information every day. 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.

There are several promising information-sharing initiatives among states and in local jurisdictions. For example, Pennsylvania's Justice Network, known as JNET, links databases from various state law enforcement agencies. JNET participants have access to approximately 60,000 images of criminal suspects, driver's license photos, and other information useful for identification. There are other new projects in Dallas, Houston, and California, to name a few. What is missing is a federal effort to promote and coordinate these initiatives and ensure they are effective and interoperable.

Improve domestic collection of foreign intelligence and its analysis and use for prevention, warning, vulnerability analysis, and policy decisions. The United States has never had a separate agency devoted to domestic intelligence. In countries such as Canada, France, Germany, Israel, and the United Kingdom, internal security agencies are charged with providing the government the domestic intelligence it needs for terrorism prevention and policy decisions related to terrorism. These agencies collect intelligence within the country using surveillance and other techniques, analyze it, and provide it to those within the government who need it for prevention of terrorist attacks and policy decisions. These agencies are separate from the countries' law enforcement organizations.

In the United States government we have a different structure. A law enforcement agency, the FBI, is also the primary agency responsible for domestic collection of foreign intelligence, including intelligence on terrorist threats, and analysis of that intelligence. Approximately one-quarter of the FBI's almost 28,000 employees are devoted to collecting and analyzing intelligence pursuant to the Attorney General's Foreign Intelligence Collection Guidelines. Their priorities are counterintelligence and counterterrorism. The FBI has a long history of effectiveness in the area of counterintelligence. With its newer counterterrorism role, the FBI's effectiveness is undercut by its cultural and organizational bias in favor of its law enforcement mission.

Unlike an intelligence agency, the orientation of a law enforcement agency is primarily reactive. Its purpose is to capture and prosecute criminals. Law enforcement agencies often will prevent acts of

terrorism or other crimes by catching a criminal before a crime is committed, but they collect information to catch criminals, not to provide warnings, assess vulnerabilities, or inform policymakers. The customer for law enforcement information is the prosecutor and a significant concern in its collection is the suitability of the information for use in court. Law enforcement and foreign intelligence information are collected using many of the same tools and techniques, but different legal authorities and guidelines.

The FBI's culture is that of a law enforcement agency. There is little representation, particularly in the senior levels of the agency, from people with experience in national security. Although senior personnel interact regularly with national security policymakers, there is a resistance ingrained in the FBI ranks to sharing counterterrorism information with the national security community or others outside of law enforcement channels. Unlike our foreign intelligence agencies, the FBI has no effective process for providing intelligence on terrorism to policymakers and others outside of the law enforcement community who need it. Moreover, the FBI has not prioritized intelligence analysis in the area of counterterrorism. The role of analysts is not valued at the FBI the way it is in other intelligence agencies. There is insufficient funding and staffing to conduct the kind of intelligence analysis that is needed for domestic intelligence in the counterterrorism area.

A NEW STRUCTURE

The first significant step in government reorganization to accommodate new information needs is creation of a new Department of Homeland Security. But the legislation creating the department raises many more questions than it answers about the roles of the players—within the federal government and outside—in information collection and analysis. It is critical that these roles be clarified in the new department's first days. We provide here our views on the most sensible roles for the key players.

The Department of Homeland Security. The Department of Homeland Security will be a significant consumer of domestic intelligence and a significant producer as well. The new department will bring together the border authorities and other entities that collect significant domestic information. Its Secretary will be among the principal policymakers responsible for domestic security.

The legislation establishing the Department's new intelligence directorate envisions a center to receive, collate, and analyze intelligence from all sources, including domestic intelligence. This is a significant step toward an internal security function—although it would not combine all domestic collection and analysis in the U.S., as the internal security agencies in other countries do. If done well, this directorate could be enormously useful as a nerve center for intelligence related to domestic security. If mismanaged, it will be toothless, ignored by CIA and FBI, and useless to policymakers.

To be sure that the new intelligence directorate lives up to its promise, it must have authority to receive the information it needs from other federal government sources. The question whether the Department of Homeland Security may “task” the FBI and CIA for intelligence collection and analysis has generated significant controversy and concerns that the new department would become a “super agency” with too much power. Similarly, there is enormous resistance to giving the new department the authority to receive intelligence in its “raw” form from other entities. But with-

out these authorities the new directorate will be hampered significantly. An intelligence directorate with no collection powers of its own will not be able to set its own priorities or pursue avenues it considers important if it cannot influence directly the intelligence it receives. One of the Administration's first priorities once the Department of Homeland Security is established must be to coordinate a set of understandings among the relevant entities that will give the Department of Homeland Security real authority—without bureaucratic hurdles—to receive the information and analysis that it needs.

The new directorate is also the most sensible place to assign some newer domestic intelligence responsibilities that are not traditionally “investigative” and for which the FBI has no special expertise. The best example of such a function is the use of government and private databases to identify terrorist planning and activities before attacks occur. There is growing understanding that access to information in government and private hands is an essential tool in the fight against terrorism. Obtaining and analyzing this information is a natural role for the new intelligence directorate.

The FBI. The FBI is the federal government's chief law enforcement agency and law enforcement will always be a critical part of anti-terrorism policy. In addition, information collected during criminal investigations often will have value outside of the law enforcement context, for prevention, warning, and policy. The FBI must improve its ability to analyze and retain law enforcement information and to share it within its own agency and with others. The FBI is taking a number of steps to improve its ability to share this information internally, including development of Trilogy and other more advanced information systems.

The FBI's role in the separate discipline of intelligence collection and analysis for counterterrorism is more difficult. The FBI culture's strong bias in favor of the law enforcement mission has interfered with its ability to be effective at collecting, analyzing, and sharing domestic intelligence related to counterterrorism. There are sound reasons why many countries have chosen to separate their law enforcement and intelligence functions.

There are advantages, though, to keeping certain domestic intelligence functions and law enforcement in the same organization. First, there are synergies between the two disciplines. An agency with both foreign intelligence and criminal investigative authorities can use the criminal authorities when the intelligence authorities are not available to gather information on suspected terrorists. Sometimes an investigation of, for example, a computer attack, will begin as a criminal investigation because the source of the attack is unknown, and therefore there is no way to make the connection to international terrorism or a foreign actor. Once more is learned through criminal investigation about the source of the attack, a determination might be made to pursue an intelligence investigation. An agency with both disciplines also may have less difficulty with a transfer if a decision is made to end an intelligence investigation and instead pursue prosecution of a suspected terrorist.

Second, many of the tools and techniques used in intelligence collection and law enforcement are similar. The FBI has significant experience with use of the tools and techniques in intelligence collection—electronic surveillance, physical searches, and interrogation, for example. Because of this familiarity, FBI personnel are accustomed to paying attention to the constitutional issues that the

domestic use of surveillance tools raise. In addition, the Attorney General has historically played an important role in approving and overseeing use of these methods.

We believe the FBI should continue to be the entity responsible for domestic intelligence collection for counterterrorism using electronic surveillance and other investigative tools and techniques, and the Attorney General should continue to supervise that collection. The FBI also must be responsible for providing its products to policymakers at the Department of Homeland Security and elsewhere in the national security community.

To perform its counterterrorism intelligence mission effectively, the FBI will have to reorient significantly. The reforms that Director Mueller has instituted will not be enough to overcome the FBI's overwhelming cultural and organizational pull toward its law enforcement mission. Additional reforms are necessary, both to elevate the importance of analysis in the FBI culture and to increase FBI's familiarity and communication with the national security policy community. These reforms should include:

- Bringing people with national security experience into the senior FBI leadership.
- Making it a requirement for promotion that FBI analysts rotate through the Department of Homeland Security or the CIA. In much the same way that the Goldwater-Nichols Act's requirement of "purple" tours transformed the military's attitude toward jointness, this requirement will elevate the value of intelligence analysis among FBI personnel, increase analyst competence, and improve working relationships between FBI personnel and other members of the intelligence community.
- Creating a more attractive professional track for intelligence analysts.
- Revamping training at Quantico to increase focus on terrorism analysis and the uses of intelligence outside of the criminal justice system.
- Hiring more agents and analysts from disciplines other than law enforcement, including some with foreign affairs or national security backgrounds.
- Continue to improve information systems and procedures for sharing information so that information travels not only up to headquarters from local offices, but throughout the FBI system and—just as important—can be accessed by those who need it outside of the FBI.

Foreign Intelligence Agencies. CIA and other foreign intelligence agencies are currently prohibited from collecting intelligence on the domestic activities of U.S. persons. Although relaxing this restriction could allow the government more effectively to take advantage of CIA expertise for homeland security, the restriction should be maintained. The CIA and other foreign intelligence agencies are accustomed to collecting intelligence on foreign nationals, but collection on U.S. persons and in the United States involves a range of constitutional protections with which CIA personnel are not familiar. A change that permitted CIA collection on U.S. persons would require changes to culture, procedures, training, and oversight. This could hamper the agency's effective-

ness in collecting foreign intelligence. A decision to give CIA a significant role in collection on U.S. persons would cause discomfort in a public suspicious of this very secretive agency and aware of past abuses by the Agency when it last took on a domestic collection role.

Current law and regulations do permit the CIA to receive, retain and analyze domestic intelligence with a foreign “nexus” that has been collected by the FBI or others. That the CIA does not regularly receive this intelligence is a result of poor procedures and communication, not a legal restriction. This authority should be clarified and procedures developed for effective and timely sharing of that information. Other uses of foreign intelligence agencies for domestic intelligence, such as use of NSA information on U.S. persons collected as part of its foreign intelligence mission, should be examined.

The President/National Security Council. Coordination is one of the great challenges for our executive branch. Now more than ever, agencies must work together as a team, rather than act as separate fiefdoms fighting over limited turf, money, and power. There have always been a number of players in the intelligence community; creating a Department of Homeland Security adds a new, very large player. Its presence will do nothing to calm the interagency battles and the jockeying for position in the early days is likely to be intense. Unless there is a strong hand coordinating and leading these departments little that is productive will be accomplished.

Responsibility for this coordination must rest with the President. The President is the only one with clear authority to direct agency action. Since the National Security Act of 1947, the President and the National Security Council have driven the foreign intelligence process and operations—setting priorities and, in the area of covert action, making operational decisions. The President and National Security Council must play a similar role with intelligence collected domestically.

Particularly once the Department of Homeland Security is up and running, a continuing bifurcation in the White House structure between “national security” and “homeland security” makes no sense and would be counterproductive. In the case of terrorism, the homeland threat and the foreign threat are inseparable. To create a coordinating mechanism that institutionalizes this false distinction would not only cause practical and bureaucratic problems, but could result in seams in coverage and coordination that would allow important issues to be missed.

Within the National Security Council interagency process, a reconstituted Executive Committee should be responsible for coordination of the intelligence mission. This group should include the National Security Advisor, the Director of Central Intelligence, the Secretary of Defense, the Secretary of Homeland Security, and the Attorney General. The Director of the FBI should be involved in all the group’s meetings. Having this group meet regularly to sort through what inevitably will be myriad management and substantive issues that involve all members of the intelligence community will be critical to effective coordination.

State and Local Governments. One fundamental shortcoming with most discussion of organizing for homeland security has been a tendency to focus only on the federal government’s role. This is understandable. Difficult as it is to sort through the federal government’s structure, the task pales by comparison to the challenge of coordinating more than 50,000 state and local jurisdictions. But an effective national strategy to combat terrorism will have to address this challenge.

Over the next five years, there must be creative thinking about how our federal system will work in an age when coordination and information networks are so important to our security. Without new ideas, the current trend of increasing central control inevitably will continue. The first step should be to focus on how information from states and localities, which is so crucial to the homeland security effort, can reach those in the federal government who need to act on it, and how the federal government's information can reach those on the front line. To be effective at collecting and using all relevant information, the entire national system must work like a network, coordinated at the federal level but controlled locally. Two concrete steps can help start this process. 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.

To do their part, states should form task forces or use other methods of coordinating important local information. The state task force formed in Utah in advance of the Salt Lake City Olympics is illustrative of a structure that encouraged input from all relevant entities in the state and established a direct line of communication with interested federal government entities. State and local health, police, and emergency officials worked together with representatives of the INS, FBI, DoD, FEMA, the National Guard and key members of the private sector to coordinate activities and share information. Although this task force was created for a specific event, it was so effective that it is being maintained indefinitely and will be chaired by the state's Director of Public Safety on behalf of the Governor. Other states may choose somewhat different models, but some coordination mechanism that involves all relevant parties in each state—or perhaps involving groups of states—will be essential.

There currently is no coordinated strategy in the federal government for interaction with state and local entities. Although many federal agencies, including the FBI, DoD, and HHS will always have relationships with state and local entities, one agency—the Department of Homeland Security—should take on the responsibility for promoting and coordinating these relationships. The federal government has a responsibility to support state, local, and regional information sharing efforts with funding. With this support must come requirements for interoperable systems and coordinated information-sharing mechanisms. The Department of Homeland Security must establish minimum guidelines and procedures for sharing and impose some order on a system that currently is almost entirely ad hoc.

OVERSIGHT: PROTECTING CIVIL LIBERTIES AND SUSTAINING AN EFFECTIVE HOMELAND SECURITY MISSION

The events of September 11 exposed the need for changes to the structures and methods we have used to protect national security. To keep ahead of the new threats requires the government to collect information from a much wider range of sources and share it more broadly. Many of the changes to information collection that have been implemented or proposed—such as collection and mining of data from private sector databases, linking of federal databases, and compilation and use of watch lists—would require lifting traditional protections for civil liberties. Creating a more robust domestic intelligence structure—although clearly necessary—will present increased civil liberties challenges that our current system of oversight is not adequately equipped to address.

The American way of life is a critical part of what our government is protecting when it provides for America's security. An open society and civil liberties are essential components of that way of life. In the past, we have avoided certain structures and practices because they make the potential for government abuse greater. If these restrictions must be relaxed because they interfere with our ability to counter the terrorist threat, we can still be vigilant about protecting liberties. The government must institute a system that sets clear standards, keeps tabs on government action, and holds it accountable for abuses. Moreover, in this new environment, the government must be creative and energetic in pursuing new models for protection of civil liberties.

Too often, civil liberties protections and security are seen as in conflict; more attention to one means the other is shortchanged. In fact, the right guidelines, the right measure of review, and the right process are essential to effective national security decision-making. They allow decision-makers to allocate finite resources and redirect them from ineffective operations or away from activities that sap resources for very little gain.

An Effective System of Oversight

A system of oversight has three levels of protections: environmental, structural, and transactional protections. To ensure our system is healthy and effective, we must strengthen each level.

Environmental. The first category of oversight involves the environment in which the activities exist: the statute or other authorization that establishes the scope of permissible activities and the congressional and executive branch entities that keep tabs on activities.

Congress. In the case of homeland security, Congress is taking steps to create a new intelligence agency and there is discussion of new authorities and techniques for collecting and using intelligence. What is missing from this debate so far is how Congress intends to provide oversight for this new intelligence capacity. As it stands, the new Department of Homeland Security will have seven or eight committees in each of the House and Senate looking over its shoulder. It is not clear what this means for oversight of the intelligence/information function. Will the judiciary committees—the committees that oversee law enforcement activities—have jurisdiction over the government's new, more robust collection and analysis function, or will the task go to the two intelligence committees? Will all of these committees claim responsibility for oversight?

Congress has a responsibility to clarify its own process. When too many congressional committees have oversight responsibility, we end up with both too little and too much. There is insufficient institutional expertise in any committee to review and assess the effectiveness of a system on an ongoing basis, but when something goes wrong every committee wants to be involved in investigating and assessing blame.

Congress should simplify its oversight of homeland security. The ideal approach would be to form standing committees on homeland security. Difficult and disruptive as this would be for Congress, it is no more than is being asked of the Executive Branch and it is the only way to assure sensible, effective congressional oversight and responsibility. If Congress does not elect to form standing committees, at the very least it should create select leadership committees with the responsibility to

oversee all agencies and activities involved in intelligence/information collection and analysis for homeland security. These committees would include the chairpersons and ranking members from the committees and subcommittees that now exercise oversight over the various agencies involved in homeland security.

The Executive Branch. Even if Congress acts to improve its oversight, there are limits to what it can accomplish. It is necessarily removed from management of the programs it oversees. In addition, in the area of oversight, the culture of the legislative branch is, more often than not, reactive. This argues for some environmental oversight mechanism within the Executive Branch. The President can provide this by instructing his Foreign Intelligence Advisory Board's Intelligence Oversight Board (PFIAB/IOB) to conduct periodic reviews of the newly strengthened domestic intelligence apparatus to ensure standards are consistent, training and compliance are adequate, and guidelines are performing their intended function. This kind of periodic review can identify problems before they result in serious abuse. The PFIAB/IOB is particularly suited to this mission. It reports directly to the President, has long experience with overseeing intelligence operations on the President's behalf, and would have access to intelligence operations and products that other bodies, even within the Executive Branch, would be denied.

Structural. Structural oversight involves the internal mechanisms and ground rules for guiding the conduct of activities. The most important elements of structural oversight are standards or guidelines and training.

Guidelines. An effective system to protect against abuse requires clear, uniform standards for behavior. If they are clear and consistent, guidelines empower more than they constrain. Fear of crossing the line into prohibited behavior causes timidity. If workers are comfortable that they know what is permitted and what is not, they will be more likely to take action. Development of guidelines should be an immediate priority for the Administration and the Department of Homeland Security. The kind of direction and structure that guidelines provide are particularly important now, given the range of new or increased intelligence activity that is being contemplated. In particular, the Administration must act quickly to establish guidelines for activities such as acquisition of private sector data, use of government databases, analysis of personal data, and development and use of watch lists.

These guidelines should be developed in close consultation with Congress and, to the maximum extent possible, with public involvement. Acting alone is quicker, but legitimacy and acceptance of the resulting product is strengthened when guidelines are developed in a transparent, consultative fashion. Changes to guidelines should be handled in the same way. It is essential that the domestic intelligence system have the confidence of the American people. That will not happen if guidelines are developed and changed under a cloud of secrecy.

Training. Standards and guidelines will serve little purpose if employees do not understand them or never learn to apply them to their duties. The Department of Homeland Security should develop and implement quickly training programs in uses of personal and private sector data and other domestic analysis activities. The FBI should also revamp and improve its training on domestic intelligence collection and analysis. Training on standards and guidelines should be an integral part of training for the intelligence mission and should be updated regularly.

Other Structural Protections. An important task for the Department of Homeland Security will be to seek out new, creative ways to build structural protections for civil liberties. Technology has the potential to advance privacy in a number of ways. For example, authentication procedures, including use of biometric identifiers for authentication, and methods of tracking access to information systems can increase accountability by recording who sees personal information. Automated information processing techniques can keep information out of the hands of government personnel or others unless it is absolutely necessary. Information can be aggregated or anonymized where appropriate to protect confidentiality. The Department of Homeland Security should review these measures and others like them and employ them in handling private and confidential information.

Transactional. Transactional oversight is the way the system deals with individual cases. This includes how permission is obtained to take action and investigation of errors.

Investigation of failures and abuses. This is the most familiar element of a system of oversight. It is important that when abuses are discovered they be investigated impartially and that responsible officials be held accountable. But a system is weak if it places too much emphasis on investigation of problems as they occur, rather than routine and periodic review of effectiveness. Investigations are prone to politicization and tend to focus on finding individual culprits. Excessive attention to individual wrongdoing causes timidity in those carrying out their duties because the consequences of errors are so professionally devastating. Scandal-driven solutions are often narrow and ultimately ineffective solutions aimed at only one piece of the problem. It can be a failing of congressional oversight that it focuses more on politicized investigation of errors than periodic review of the effectiveness and strength of a system. Similarly, inspectors general who are not integrated into an agency's decision making or structure often have little voice or stake in maintaining a healthy system and can focus excessively on exposing individual wrongdoing.

A healthy system of transactional oversight will include officers, such as Inspectors General, who can conduct impartial investigations and audits when necessary. But it should also include people integrated into the line offices who can guide and review the way decisions are made on an ongoing basis to prevent failures, not punish them.

The Department of Homeland Security will have an Inspector General and a Privacy Office. It may also have a Civil Rights and Civil Liberties office. The roles of these offices should be spelled out and deconflicted. Only one—the Inspector General—should be charged with investigation of failures or abuses. The others should focus on developing guidelines and training programs and should be integrated as much as possible into the day-to-day work of the intelligence directorate and other offices to promote practices consistent with guidelines, not to punish errors.