G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

August 30, 2002

The Honorable Tom Davis
Chairman, Subcommittee on Technology
and Procurement Policy
Committee on Government Reform
House of Representatives

Subject: *National Preparedness: Technology and Information Sharing Challenges*

Dear Mr. Chairman:

On June 7, 2002, we testified before your Subcommittee on technology and information sharing challenges confronting our nation's approach to homeland security.[1] Addressing the challenges—particularly making sure that the right information gets to the right people at the right time and making good use of technology—is essential to making sure the nation's strategy is sustainable and effective. Effective information sharing will also be critical to success for the proposed Department of Homeland Security, both to assist in the integration of the agencies and programs being consolidated within the new Department, and to ensure the sharing of relevant information with state and local governments and the private sector. This letter responds to specific questions you had related to our testimony. Our answers are based largely on the research and analysis supporting our testimony and past GAO findings. Our work was conducted in accordance with generally accepted government auditing standards from June through August 2002. Your questions, along with our responses, follow.

1. **One of the barriers identified by various witnesses to effective homeland security is interagency cooperation, which was largely attributed to "turf" issues. What incentives have been provided to or could be used by agency managers to encourage more effective cooperation and coordination of information pertaining to homeland security?**

[1] U.S. General Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing Into an Effective Homeland Security Strategy*, GAO-02-811T (Washington, D.C.: June 7, 2002).

Response: Clearly, the best incentive is strong and sustained commitment by agency leaders to break down cultural resistance to cooperating and push their managers and staff towards embracing new ways of doing business. No effort to do things differently can succeed without such commitment. Moreover, agency leaders have a wide range of tools at their disposal for enforcing and rewarding change, including performance bonuses for senior executives, incentive award programs for staff, and the ability to reorganize programs so that they are focused more on cross-cutting goals instead of in-house goals and outcomes instead of process.

We have also studied other cross-cutting federal services with similar "turf" problems, such as housing and food and nutrition services, and found that the agency performance plans, which are required by the Government Performance and Results Act (GPRA), offer a good avenue for developing incentives to cooperate. Specifically, agencies can set up goals in their performance plans for participation in cross-cutting programs and report on their progress in meeting these goals to Congress.[2] Congress could also build in similar incentives into budget resolutions.

Shared programmatic goals and metrics also encourage cooperation and coordination. Affected agencies should all participate in the development of goals, milestones and metrics to measure progress and success, and such indicators should be clearly articulated and endorsed by senior management. Such goals and metrics must be carefully chosen, since how performance is measured greatly influences the nature of the performance itself; poorly chosen metrics may lead to unintended or counter-productive results. However, visible, clearly articulated and carefully chosen shared goals and metrics can effectively overcome "turf" issues. One of the first tasks for the new Department of Homeland Security should be the articulation of such shared goals, milestones, and metrics.

Finally, organizing around and through information sharing can help overcome turf issues. New technologies for data integration and interoperability can enable agencies to share data and work cooperatively along informational lines, without the need for radical structural changes. Simply put, enhanced IT technology can allow agencies to work together yet retain a measure of autonomy, thus removing some barriers hindering agencies from embracing change.[3]

2. **You mention in your testimony that there may be legal or regulatory barriers to better information sharing. What, if any, legal or regulatory barriers exist that hinder effective electronic communication among federal agencies, with state and local government organizations and the private sector?**

[2] U.S. General Accounting Office, *Managing for Results: Barriers to Interagency Coordination*, GAO/GGD-00-106 (Washington, D.C.: Mar. 29, 2000).

[3] Testimony of Anne K. Altman, IBM Corporation before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, U.S. House of Representatives, February 26, 2002.

Response: We have reported that the private sector has expressed concerns about voluntarily sharing information with the government concerning our nation's critical infrastructure.[4] For example, concerns have been raised that industry could potentially face antitrust violations for sharing information with other industry partners, have their information be subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith.

3. What steps could be taken to protect information in shared databases while allowing full use in a homeland security context?

Response: Various technologies can be used to protect information in shared databases. For example, data in shared databases can be protected through electronically secured entry technology (ESET). ESET allows users or separate databases to cross check or "mine" data securely without directly disclosing their information to others. This allows agencies to collaborate but also addresses their needs for secrecy or privacy. Such technology could allow an airline to cross check a passenger or employee against data held by government agencies in a single-step process without actually disclosing the base data to the airline. In checking an individual, the airline would not receive any data from the agencies' databases, rather they would receive a "yes or no" type response and/or a referral for further action. Additionally, appropriate authorities could automatically be notified.[5]

New technologies like ESET, however, will not be fully effective without sound information security controls over agency databases. For several years, we have reported[6] that federal computer systems are riddled with weaknesses, including poor access controls, that continue to put critical operations and assets at risk. Many agencies also lack a good framework for ensuring that risks are understood and that effective controls are selected and implemented.

4. In your testimony, you mention that even though America has a superior research and development base, great human capital resources, and leading-edge technologies for the fight against terrorism, there are nonetheless substantial challenges to leveraging these strengths. How can these challenges be met and are there models in the military or elsewhere that may be of assistance?

Response: The homeland security challenge we are now facing is unprecedented. The scope of things that need to be done are seemingly endless. The threat itself is fluid, elusive and extremely difficult to counter. And the solution requires massive planning and coordination not just by the federal government, but by all state and local governments, as well as the private sector. As a result, there is no one model

[4] U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed*, GAO-02-918T (Washington, D.C.: July 9, 2002).

[5] http://www.house.gov/reform/tapps/hearings/2-26-02/ibm226homelandsecurity.htm

[6] U.S. General Accounting Office, *Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk*, GAO-01-600T (Washington, D.C.: Apr. 5, 2001).

that we can draw on for a complete solution to the problem. But there are models that can help us address particular aspects of it. For example,

- Expeditionary forces within the military provide a good example of how we can find new approaches to preventing and responding to attacks by capitalizing on technology, skills and capabilities, and flexibility. These are forces that are designed, trained, and organized in a fashion very different from that of conventional forces, which previously relied on highly structured and standardized approaches to war-fighting and require a considerable infrastructure in their deployments.

- The President's Council on Year 2000 Conversion can provide a model for leadership and coordination. To address the Y2K problem, the Council used a sector-based approach and established effective public-private partnerships necessary to address the problem. The more than 25 sector-based working groups, which were led by one or more federal agencies that established partnerships with over 250 organizations, gathered information critical to the nation's Y2K efforts and addressed issues such as contingency planning. In addition, the Chair of the Council formed a Senior Advisors Group composed of representatives from private-sector firms across key economic sectors. Members shared perspectives on cross-cutting issues, information sharing, and appropriate federal responses to potential year 2000 failures.

- Intrusion detection systems provide a good model for building systems that can protect major cities and infrastructures. These systems are built based on data on normal use of system and network activity as well as known attack patterns. Deviations are discovered based on data from analyses of network packets, captured from network backbones or local area network segments, or data sources generated by the operating system or application software. The concept could be applied on a bigger scale using geospatial digital information tools, including remote sensing and satellite imagery technology. Doing so, however, will be challenging. For starters, determining what is normal and abnormal activity relative to terrorist activity would be difficult because it would require developing an extensive body of knowledge—beyond just intelligence information—to build a baseline for terrorist activity when the activity itself is elusive, fluid, and difficult to predict.

There are also models for integrating agencies into the new homeland security department, particularly private sector merger and acquisition efforts (both successful and unsuccessful), which we plan to study. Private sector models may be more instructive than past government reorganizations, due to the private sector imperative to maintaining customer focus and "profitability" during reorganization. The Department of Homeland Security should similarly focus upon reducing the extent and duration of decreased agency effectiveness due to major reorganization.

5. **In your testimony to the Subcommittee, you stated that there are three broad challenges to be faced in order for the country to develop and implement a national preparedness strategy for homeland security: the difficulty in identifying and differentiating key information; the cultural, legal and technical barriers to collecting and sharing information; and the**

gap between existing technologies and what is needed for the war on terror. What is your sense of the progress being made on these challenges by government?

Response: As we have recently testified, the creation of a Department of Homeland Security is an encouraging first step, but implementation and successful transition and transformation will be critical to success.[7] The new department will integrate programs currently spread across approximately 22 agencies. It is likely that few if any of those agencies would have listed "homeland security" as their primary mission prior to September 11th. It is also likely that few if any of such agencies would have predicted the variety of potential methods of attack considered by terrorists. Also, some of the agencies being proposed for merger into the new department faced significant program management and resourcing challenges, even before assuming the additional homeland security responsibilities.

Creation of a new department whose primary mission is homeland security is a major step forward in implementation of a national strategy. The Office of Management and Budget directive of July 19, 2002, to review redundant homeland security information technology (IT) infrastructure for consolidation and integration is also a strong indication of the desire to overcome such barriers.[8] Designing and intelligent IT architecture that meets the new homeland security mission, while supporting the dual or multiple missions of the agencies involved in homeland security, will be a critical enabler.

But once information sharing is enabled, then the right information must be shared. Great emphasis has been placed upon data mining and data integration, but the third and perhaps most crucial component may be data visualization. The vast amount of information potentially available to be mined and integrated must be intelligently analyzed, and the results effectively "visualized" or presented, so that the right people have the right information necessary to act effectively upon such information. This may involve differentiating the relevant anomalies or "needles in the haystack" from the mass of background data. An intelligent scheme to derive "background" must be employed, and the data collection necessary to create "trends" may take some time; but information that will be useful needs to be considered and identified now, and efforts to collect the information (preferably from existing sources) begun. Again, remote sensing technologies and techniques may provide useful analogies, particularly when combined with digitization of data, allowing advanced computer modeling, geospatial system interfaces, and area-wide data visualizations.

Both the House and Senate proposed legislation for the new department emphasize investments in new and emerging technologies to meet some of these challenges. Resourcing remains a major concern.

[7] U.S. General Accounting Office, *Homeland Security: Proposal for Cabinet Agency Has Merit But Implementation Will be Pivotal to Success*, GAO-02-886T (Washington, D.C.: June 25, 2002).

[8] Office of Management and Budget, *Reducing Redundant IT Infrastructure Related to Homeland Security, Memorandum for the Heads of Selected Departments and Agencies*, July 19, 2002, M-02-12.

Progress in identifying the issues, and re-structuring agencies and functions to meet these issues has been made, but as with most major programmatic challenges, implementation including follow-through will be the key.

6. Why is XML (Extensible Markup Language) useful for better information sharing?

Response: XML is a flexible, nonproprietary set of standards for tagging information so that it can be transmitted over a network such as the Internet and readily interpreted by disparate computer systems. If implemented broadly with consistent data definitions and structures, XML offers the promise of making it significantly easier for organizations and individuals to (1) identify, integrate, and process information that may initially be widely dispersed among systems and organizations, and (2) conduct transactions based on exchanging and processing such information.

7. In the Subcommittee's February hearing on information sharing for Homeland Defense, several witnesses discussed the applicability of customer relationship management (CRM) techniques and technology to help give us a "360 degree" view of terrorist suspects and to better share data. Are agencies implementing any CRM technologies at this time?

Response: We have not conducted a review of agencies using CRM technologies. However, we are aware of some agencies implementing CRM technologies at this time. For example, IRS is developing a Customer Relationship Management Core system that is designed around a universal case folder that will capture information from each taxpayer and track all transactions, such as notices, forms, publications, and letters, that the taxpayer receives until the case is closed. A telephone assistor would be able to pull up this historical information each time the taxpayer calls in. The system is also designed to capture feedback for management purposes. The project's completion is scheduled between 2005 and 2007. The U.S. Postal Service and the Transportation Security Administration are also using CRM software. There are potential cultural barriers to implementing CRM techniques and technologies to better study terrorists, particularly since successful use of CRM requires breakdowns in stovepiped organizational structures and data silos.

-- -- -- -- --

This letter is also available on GAO's home page at http://www.gao.gov. If you or your staff have any questions regarding this letter, you can contact Randall Yim (202) 512-6768 or by e-mail at yimr@gao.gov or Steve Backhus (202) 512-7111 or by e-mail at backhuss@gao.gov.

Sincerely yours,

Randall Yim
Managing Director
National Preparedness

(976302)