United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives

For Release
on Delivery
Expected at
10:00 a.m. EDT
Friday
June 7, 2002

NATIONAL PREPAREDNESS

Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy

Statement of Randall A. Yim
Managing Director, National Preparedness

GAO-02-811T

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing on homeland security. In the wake of the terrorism attacks of September 11, the Office of Homeland Security is preparing a strategy to address these threats to our nation. In addition, federal, state, and local governments, and the private sector, are taking steps to strengthen the safety and security of the American people, including actions to strengthen border and port security, airport security, and health and food security and to protect critical infrastructure. You asked me to discuss what challenges exist in facilitating these security initiatives--particularly in terms of technology and information sharing—and how addressing these challenges fits in with developing and implementing a national preparedness strategy.

In brief, there are specific data, information-sharing, and technology challenges facing the country in developing and implementing a national preparedness strategy.

- The nature of the terrorist threat makes it difficult to identify and differentiate information that can provide an early indication of a terrorist threat from the mass of data available to those in positions of authority responsible for homeland security.
- We face considerable barriers—cultural, legal, and technical--in effectively collecting and sharing information.
- Many technologies key to addressing threats are not yet available, and many existing technologies have not been effectively adapted for the threats the country now faces.

The real challenge, however, is not just to find the right solutions to each of these problems but to weave solutions together in an integrated and intelligent fashion so that they are collectively more than the sum of their parts. At the national level, this will require developing a blueprint, or architectural construct, that defines both the homeland security mission and the information, technologies, and approaches necessary to perform the mission in a way that is divorced from organizational parochialism and cultural differences. Local, state, and federal agencies responsible for homeland

security will need to carry out their respective roles under this construct with a great deal of assistance from the private sector. Fortunately, there are starting points for addressing each challenge and actions are being taken to strengthen security in a broad range of areas. But there will still be a need for mechanisms to make sure that things happen as they should.

In preparing for this testimony, we relied on our prior reports and testimonies on national preparedness, critical infrastructure protection, enterprise architectures, intellectual property, and information technology. We reviewed and analyzed studies on homeland security and a variety of proposals for developing a comprehensive strategy. We also analyzed government and industry reports on the use of remote sensing technologies, media reports of information-sharing difficulties, governmentwide guidance on the development of architectures, as well as statements from the Office of Homeland Security on the actions taken to address homeland-specific challenges. In addition, we recently discussed with industry officials the specific barriers to sharing information on vulnerabilities and attacks.

THE THREAT THAT THE COUNTRY IS FACING AND HOW IT NEEDS TO BE POSITIONED TO RESPOND

Our country cannot be 100-percent secure from terrorist attack, particularly when these threats are asymmetric to our strengths, and when terrorists intend to sustain their efforts for as long as need be but view success in terms of single, isolated events causing loss of life or disruption of normal daily routines. What makes it particularly difficult to gauge and respond to this kind of threat?

- Terrorist groups are typically loosely structured, fluid and flexible units, operating in the background seeking targets of opportunity--what futurist Edith Weiner terms "hiborgs" or hybrid organizations. By contrast, our government is highly structured and less able to change rapidly.
- Terrorists groups take advantage of targets becoming complacent, or simply being

unable to recognize threats that "blend" into the background of normal life. Countering this complacency and sustaining a high alert status on our part is very difficult.

- The primary job of the terrorist is to find the soft spots, or vulnerabilities, such as lax airport security, unprotected borders, or weak controls over critical computer assets--and to attack these targets in asymmetric ways. Our job—to limit the soft spots--is much more difficult and costly. As the aftermath of the September 11 attacks has shown, providing airports with adequate security alone is a massive challenge--requiring the hiring of thousands of security personnel, acquiring advanced security technology, placing undercover law enforcement officials on flights, developing new passenger boarding procedures, training pilots and flight crews on hijacking scenarios, limiting access points, deploying national guardsmen, and instituting second screening procedures. While significant steps have been taken to improve passenger security, concerns remain, such as the safety of charter airlines.
- Moreover, our government agencies are still required to perform missions or provide essential public services that extend their responsibilities well beyond countering terrorists--with finite fiscal and human capital resources.

It is extremely difficult to defend against a suicide bomber or other asymmetric threats. Yet we are not helpless. Asymmetry can also be made to work to our advantage particularly if we recognize that government institutions are highly structured and less fluid, and deliberately take advantage of innovative and readily adaptable tools that enable us to better counter terrorists and employ our positive asymmetrical advantages against such groups. Moreover, this country has tremendous resources at its disposal, leading edge technologies, a superior research and development base, and extensive expertise and experience of human capital resources. However, there are substantial challenges to leveraging these tools, including getting the right information at the right time and sharing it and getting the right technologies, and developing a construct that makes sure not only that the right information goes to the right people, but that we can prevent, detect, and respond to attacks in a concerted, effective manner.

DATA CHALLENGES

What Needs to Be Done?

- Develop an understanding of the homeland security mission and who does what, for what reason, and how/where/when they do it. From that knowledge, decide on the types of data to be collected and reported as well as on the level of detail.
- Collect needed information from a broad range of entities—from federal, state, and local agencies, the private sector, and the research and development community--not just once, but consistently over time so that trends may be established.
- Determine the right format and standards for collecting data so that disparate agencies can aggregate and integrate data and communicate those standards to reporting entities.
- Prioritize data, boil it down to the pieces that can be used to build baselines of normal activity and mechanisms that can effectively detect deviations or anomalies that would indicate vulnerabilities or threats and how serious they may be.

Getting the right information needed for effective and sustainable homeland security will be a daunting challenge, considering the myriad of possible targets, types of attack, and variables that need to be considered in any one aspect of homeland security. Nevertheless it is important to begin deciding what needs to be collected, how it should be collected, and what form it should take so that we can begin to collect data that we will need over time to detect terrorist activity before an actual attack.

The first challenge in doing this is to develop an understanding of the homeland security mission, goals, and objectives, and the key activities and players involved.[1] This includes learning specifically (1) who does what for what reason; (2) how, where, and when they do it; (3) what do they use in order to do it; and (4) in what form. It also includes developing risk and threat analyses. Building this knowledge will be considerably difficult, considering the number of individuals and organizations involved in national preparedness and the asymmetrical nature of the threat, but it is essential to identify gaps in data, technology, and approaches.

[1] We plan to issue a report on the need to define the homeland security mission within the next month.

Other data-related challenges include the following:

- ***Deciding what types of data need to be collected for certain activities as well as the level of detail.*** This can be extremely complex for any one aspect of national preparedness. Take transportation mobility, for example, which is critical in the event of a chemical, biological, or nuclear attack. Road network information, when combined with digital elevation models and terrain analysis would help analysts identify transportation or other infrastructure open to threats and to plan mitigating strategies. The same information would also help to identify alternate routing to evacuate or avoid affected areas. Census data and current weather patterns (winds, temperature, and humidity) would allow emergency management officials to determine which areas are most at risk and plan appropriate evacuation routes under multiple scenarios. Finally, any large-scale evacuation will stress emergency facilities and other transportation network elements. As immediate post-attack work done at the World Trade Center illustrates, real-time aerial data can also assist clean-up and recovery efforts.[2]

- ***Balancing varying interests and expectations.*** For example, as we have testified in the past,[3] when it comes to protecting cyberspace, the private sector may want specific threat or vulnerability information so that immediate actions can be taken to avert an intrusion. Law enforcement agencies may want specific information on perpetrators and particular aspects of the attack, as well as the intent of the attack and the consequences of or damages due to the attack. At the same time, many computer security professionals may want the technical details that enable a user to compromise a computer system in order to determine how to detect such actions.

---

[2] See Ray A. Williamson, "Information as Security: Remote Sensing, Transportation Lifelines and Homeland Security," *Space Imaging*, (May/June 2002).

[3] See U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination*, GAO/T-AIMD-00-268, (Washington, D.C.: July 26, 2000).

- ***Deciding how much is enough.*** It is important to recognize that it is not possible to build an overall, comprehensive picture of activity on a national scale or even certain confines of activity. For example, it would not be possible to develop a complete picture of the nation's information infrastructure. Networks themselves are too big, they are growing too quickly, and they are continually being reconfigured and reengineered.

- ***Determining the right format and standards for collecting data so that disparate agencies can aggregate and integrate data sets.*** For example, Extensible Markup Language (XML) standards could be considered as one option to exchange information among disparate systems.[4] Further, guidelines and procedures need to be specified to establish effective data-collection processes, and mechanisms need to be put in place to make sure that this happens—again, a difficult task, given the large number of government, private, and nonprofit organizations that will be involved in data collection. Finally, mechanisms will be needed to disseminate data, making sure that it gets into the hands of the right people at the right time.

More importantly, to make sure the homeland strategy is sustainable, we eventually need to boil data down to the pieces that will allow us to build baselines of normal activity and mechanisms that will enable us to effectively detect deviations or anomalies that would indicate vulnerabilities or threats and how serious they may be. This is already done on a much smaller scale for such things as self-diagnostic systems in automobiles, aircraft, and even electric appliances that alert the owner or manufacturer after sensing slight temperature changes or other small deviations that could indicate a mechanical problem even before it occurs. Moreover, it is done for protecting computer networks.[5] But

[4] XML is a flexible, nonproprietary set of standards for annotating or "tagging" information so that it can be transmitted over a network and readily interpreted by disparate systems. For more information on its potential use for electronic government initiatives, see U.S. General Accounting Office, *Electronic Government: Challenges to Effective Adoption of the Extensible Markup Language*, GAO-02-327, (Washington, D.C.: April 2002).

[5] Intrusion detection systems used to protect computer networks 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.

doing this promises to be an extremely complicated endeavor for homeland security. For starters, determining what is normal and abnormal activity relative to terrorists 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.

Fortunately, there are good places to start data gathering and modeling. Organizations known as Information Sharing and Analysis Centers (ISACs) are already collecting information on critical aspects of our infrastructure; government agencies at all levels have databases that may be adapted and become useful for such activities as tracking potential terrorists or detecting biological attacks; and extensive information is already being collected through the use of satellites and remote sensing technology that should be useful in building models to detect, analyze, and respond to threats.

Starting Points

- Information Sharing and Analysis Centers are being established to develop information on the nation's critical infrastructure, specifically, information to identify vulnerabilities and prevent and respond to attacks. These include the National Coordinating Center for Telecommunications and the Financial Services Information Sharing and Analysis Center. In September 2001, we reported that six ISACs within five infrastructures had been established and that at least three more were being formed.
- Federal agencies, such as the Federal Bureau of Investigation (FBI), the Immigration and Naturalization Service (INS), Customs, Health and Human Services, already have databases containing information critical to homeland security. State and local governments also have databases that, if adapted, will be useful, such as those belonging to highway and transportation departments, county health departments, and school systems.
- Models and statistical techniques have already been developed by the military to analyze threats and provide "gaming" simulation of multiple-threat scenarios. In addition, agencies are already collecting information that could feed into these models, such as census and weather data; aerial mapping of cities and farmlands; detailed images of shipping and transportation routes; and maps detailing critical infrastructure and their capacities, such as telecommunications and utility lines.

INFORMATION-SHARING CHALLENGES

What Needs to Be Done?

- Establish effective information-sharing between private-sector, nonprofit, and government organizations to facilitate research and development efforts, data collection efforts, law enforcement efforts, and efforts to respond to attacks.
- Ensure that security measures exist to protect sensitive information.

Events preceding and following the attacks of September 11 spotlighted one of our most serious vulnerabilities. We do not share information effectively, particularly when it comes to intelligence, law enforcement, and response activities. If we cannot do a better job of sharing information, we will not be able to effectively identify vulnerabilities, develop needed technology, and coordinate efforts to detect and respond to attacks.

Federal agencies and the Congress are still looking into the specifics of information sharing-difficulties related to the September 11 attacks, but recent reports of information-sharing failures within the FBI and CIA highlight some of the primary barriers we face: stovepiped organizational structures, inadequate database sharing, and simple "turf" issues. Legal and regulatory impediments may have made information-sharing even more difficult.

This problem is not new. Two years ago, for example, we testified that the ILOVEYOU computer virus, which affected governments, corporations, media outlets, and other institutions worldwide, highlighted the need for greater information sharing and coordination to respond to attacks on our critical infrastructure. Because information-sharing mechanisms were not able to provide timely enough warnings against the impending attack, many entities were caught off guard and forced to take their networks off-line for hours. Getting the word out within some federal agencies themselves also proved difficult. At the Department of Defense, for example, the lack of teleconferencing capability slowed the response effort because Defense components had to be called

individually. The National Aeronautics and Space Administration had difficulty communicating warnings when E-mail services disappeared. Some departments that received warnings did not share that information with their bureaus.

As illustrated below, however, the problem of information sharing is much more extensive than just sharing information about an impending attack—it extends from the early stages of research and development, to collecting data, preventing and detecting attacks, and responding to attacks. Barriers themselves extend well beyond poor mechanisms for issuing attack warnings or communicating calls for "heightened alert." For example, in recent discussions with us, industry officials said that their chief concern in sharing information about vulnerabilities and attacks is disclosure of proprietary data. Our past reviews have also highlighted concerns about roles and responsibilities, antitrust violations, and national security as barriers to sharing information.

In short, there are formidable challenges that need to be overcome to build a more comprehensive and effective information-sharing relationships.[6] Trust needs to be established among a broad range of stakeholders, important questions on the mechanics of information sharing and coordination need to be resolved, and roles and responsibilities need to be clarified among all levels of government.

Where Information Sharing Can Potentially Break Down	***Why***
Government efforts to sponsor research and development efforts to develop new homeland security technologies	• Intellectual property concerns may affect the willingness to contract with the government, including poor definitions of what technical data are needed by the government and unwillingness on the part of government officials to exercise the flexibilities available to them concerning intellectual property rights. • Concerns that inadvertent release of confidential business material, such as attempted or successful attacks, gaps in security, or trade secrets or proprietary information, could damage reputations, lower consumer confidence, hurt competitiveness, and decrease market shares of firms.

[6] For more information about barriers to information sharing, see GAO/T-AIMD-00-268 and U.S. General Accounting Office, *Intellectual Property: Industry and Agency Concerns Over Intellectual Property Rights*, GAO-02-723T, (Washington, D.C.: May 10, 2002).

Where Information Sharing Can Potentially Break Down	***Why***
Government efforts to facilitate data sharing on critical infrastructures	• Concerns about potential antitrust violations may keep companies from sharing information with other industry partners. • Concerns that sharing information with the government could subject data to Freedom of Information Act disclosures or expose companies to potential liability may also prevent companies from sharing data with government agencies.
Private sector efforts to get data from the government on potential vulnerabilities and threats	• National security concerns may prevent agencies from sharing data with the private sector. • The process of declassifying and sanitizing data takes time—possibly too long to be of use to private-sector time-critical operations. • Security clearances may not be available for the "right people" who need to know.
Coordinating law enforcement and intelligence activities	• Law enforcement and intelligence agencies operate in "distinct universes" separated by jurisdictional, organizational, and cultural boundaries. At the same time, however, roles and responsibilities at different levels of government are not always clear and distinct. • Information may be considered too sensitive to release to law enforcement colleagues because it could compromise source and collection techniques. • Certain laws and regulations as well as privacy concerns may prevent information sharing between federal agencies, state, and local law enforcement agencies. • Insufficient direction about what specific steps should be taken when security alert status is increased. • Lack of access to databases and problems with interconnectivity may impede information sharing between agencies.
Issuing attack warnings and responding to attacks	• Information-sharing mechanisms and procedures for warning against attacks, especially between different levels of government, may be inadequate. • Roles and responsibilities between emergency, rescue, relief, and recovery organizations may not always be clear, especially at different levels of government.

Because information sharing was a critical problem in other crises facing the government, there are some very good models to learn from and build on. The ISACs mentioned earlier are a good example of government and private-sector relationships for

information sharing. The Centers for Disease Control and Prevention (CDC) also uses several information-sharing computer systems to help accomplish its mission to monitor health, detect and investigate health problems, and conduct research to enhance the prevention of disease.[7] In addition, actions have already been taken by the Congress and the administration to strengthen information sharing. The USA Patriot Act, for example, enhances or promotes information sharing between federal agencies, and numerous terrorism task forces have been established to coordinate the investigations and improve communications between federal and local law enforcement agencies. Also, very recently, leading financial services firms in New York formed a private database company that will compile information about criminals, terrorists, and other suspicious people for use in screening new customers and weeding out those who may pose a risk. The company will specifically focus on helping financial companies comply with anti-money-laundering regulations, including requirements in legislative approved after the September 11 attacks. Additional private-sector solutions also need to be considered, such as current research efforts to link airline reservation systems.

Starting Points

- The Agora is a Seattle-based regional network of over 600 professionals representing various fields, including information systems security; law enforcement; local, state, and federal governments; engineering; information technology; academics; and other specialties. Members work to establish confidential ways for organizations to share sensitive information about common problems and best practices for dealing with security threats. They develop and share knowledge about how to protect electronic infrastructures, and they prompt more research specific to electronic information systems security.
- Carnegie Mellon University's CERT Coordination Center (CERT/CC) is charged with establishing a capability to quickly and effectively coordinate communication between experts in order to limit damage, respond to incidents, and build awareness of security issues across the Internet community. In this role, CERT/CC receives Internet security-related information from system and network administrators, technology managers, and policymakers and provides them with this information along with guidance and coordination to major security events.

[7] We reported in September 2001 that the usefulness of several of these systems is impaired both by CDC's untimely release of data and by gaps in the data collected.

TECHNOLOGY CHALLENGES

What Needs to Be Done?

- Research and develop new technologies integral to the fight against terrorism, such as bioweapon- or low-level-radioactive-weapons-detection systems and biometric devices.
- Refine emerging technologies so that they are more user friendly and less cost prohibitive.
- Adapt existing technologies to the homeland security mission.
- Connect and make interoperable databases integral to information sharing, such as those belonging to the FBI and INS.

This is one area where we certainly have an edge over terrorists. Newly developed unmanned aerial vehicles are providing intelligence vital to military efforts in Afghanistan. Satellite networks and remote sensing technologies are facilitating assessments of threats overseas as well as military operations and guidance systems for weapons systems. However, though we have vast technological resources available on the homefront, there are substantial challenges confronting us.

- Certain technologies important to homeland security have not been developed. These include bioweapons- and low-level-radioactive-weapons-detection systems and disease surveillance systems.

- Some technologies already in existence have not been effectively adapted to homeland security. Space-based satellites and sensors, for example, are being used to guide weapon systems, map cities, and study the weather and environment. But they also may be adapted to the homeland security mission. Moreover, some experts believe that making this transition may require modifications to current technology, such as the addition of video features so that we can observe ground activity as it is changing.[8]

[8] See Joseph A. Engelbrecht Jr., "Global Security Will Drive Real-Time Surveillance," *Space Imaging*, *(*May/June 2002).

- There is a lack of connectivity and interoperability between databases and technologies important to the homeland security effort. Databases belonging to federal law enforcement agencies and INS, for example, are not connected, and databases between state, local, and federal governments are not always connected. In fact, we have reported for years on federal information systems that are duplicative and not well integrated.[9] A related problem is that there are not common standards for data exchange and application programming interfaces for technologies that provide physical security. As a result, much of the equipment needed to protect buildings is not interoperable. We recently testified, for example that deploying an access control system that uses a smart card containing a fingerprint biometric would require at least three pieces of equipment: the card reader device, the fingerprint scan device, and the hardware device used to house and operate the biometric software.[10] If these devices are made by different manufacturers, they cannot function as an integrated environment without costly additional software to connect the disparate components.

- Some existing technologies important to homeland security are not user-friendly. We recently testified that some biometric technologies are inconvenient to use.[11] Retina scanning, for example, feels physically intrusive to some users because it requires close proximity with the retinal reading device. Moreover, fingerprinting feels socially intrusive to some users because of its association with the processing of criminals. There is also an assortment of health concerns among a segment of the population regarding certain security technologies. For instance, there is evidence that pacemakers and hearing aids can be adversely affected by some detection technologies.

---

[9] See U.S. General Accounting Office, *Information Technology: Enterprise Architecture Use across the Federal Government Can Be Improved*, GAO-02-6, (Washington, D.C.: February 2002).

[10]See U.S. General Accounting Office. *National Preparedness: Technologies to Secure Federal Buildings*, GAO-02-687T, (Washington, D.C.: April 25, 2002).

[11]See GAO-02-687T.

- The capabilities of security technologies can be overestimated, potentially luring security officials into a false sense of security and relaxed vigilance. During our recent review of federal building security technologies, we found instances in which the performance of biometric technologies was overestimated.[12]

Because of our nation's substantial investment in technology and research and development, there are numerous good starting points for developing and harnessing technology needed for the homeland security mission. Significant advances, for example, have already been made in technologies needed to protect buildings, airports, and other facilities. We also have a good technological foundation, including space-based satellites, imagery, and remote sensing systems, to begin developing systems for effectively monitoring and gauging terrorist activities.

Additionally, the administration is promoting a host of new initiatives to acquire the technologies needed for homeland security. For example, projects already under way include the following:

- Taking stock of what technologies are already available and what gaps exist.
- Assessing what changes are needed to federal databases to facilitate information sharing.
- Efforts to develop protocols to permit the access of databases and information owned by federal agencies as well as state and local authorities.
- Developing an optimized entry-exit system for border security.
- Assessing biometric technology options.

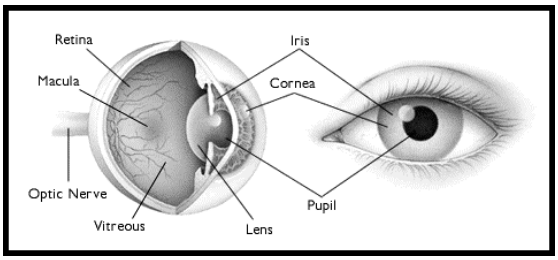
---

[12] See GAO-02-687T.

Starting Points

Continue to Develop and Refine Emerging Technology

- Some of the emerging biometric devices, such as iris scans and facial recognition systems, theoretically represent a very effective security approach because biometric characteristics are distinct to each individual and, unlike identification cards and pin numbers or passwords, they cannot be easily lost, stolen, or guessed. Until recently, in addition to being very expensive, the performance of most biometric technologies had unreliable accuracy. However, prices have significantly decreased and, after years of research, the technology has recently been improved considerably.



Iris scan technology is based on the unique visible characteristics of the eye's iris, the colored ring that surrounds the pupil. A high-resolution digital image of the iris is taken to collect data. The system then defines the boundaries of the iris, establishes a coordinate system over the iris, and defines the zones for analysis within the coordinate system. The visible characteristics within the zone are then converted into a 512-byte template.

Adapt potentially useful existing technology

- Combining geospatial digital information tools, including remote sensing and satellite imagery technology, can assist efforts to model threat prevention and response scenarios and build baselines of normal activities and detect deviations from the norm. The same information can also be used to respond to a successful attack and assist in crime scene investigation. This technology is already being used to plan and execute military operations and analyze threats overseas, as well as to map cities, study the environment and weather, monitor transportation and shipping routes, monitor compliance with laws, regulations and treaties, and model differing scenarios to assist in planning and prevention.

Satellite photo with geospatial digitized overlay.

Make Good Use of Low Tech Alternatives

- New ionization radiation technologies that the United States Postal Service (USPS) is implementing may be a promising way to sanitize mail contaminated by anthrax, but there are proven low-tech solutions that should still be considered, such as manual mail-handling procedures to presort nonanonymous mail to reduce the volume that would require higher tech irradiation techniques.
- New high-tech explosive detection systems can be used to detect bulk or trace explosives concealed in, on, or under vehicles, containers, packages, and persons. However, dogs are also an effective and time-proven tool for detecting concealed explosives. The dogs currently used by Defense, for example, can detect nine different types of explosive materials. And since dogs have the advantage of being mobile and able to follow a scent to its source, they have the significant advantage over mechanical explosive detection systems in any application that involves a search.

Security dogs may be more cost effective and easier to deploy than new high tech explosive detection systems

MECHANISMS NEEDED TO EFFECTIVELY RESPOND TO CHALLENGES

What Needs to Be Done?

- Apply risk management principles to identify assets that need to be protected to maintain continuity of operations, as well as threats, vulnerabilities, risks, priorities, and countermeasures.
- Use this understanding to develop a blueprint, or architectural construct, that defines the information, technologies, and approaches necessary to perform the homeland mission.
- Assign responsibilities among the stakeholders so that everyone is not doing the same thing, but instead all are doing something slightly different that together forms a more effective shield.
- Establish analytical and warning capabilities.
- Create performance goals and metrics, and feedback and accountability mechanisms, so that efficacy of investments and efforts may be measured and programs continually improved.

The overriding challenge for homeland security, of course, is how to prevent, detect, and respond to attacks. Technology and information are critical enablers, but they are not the sole answer. Significant issues involving people and approaches also need to be dealt with. For example, people—the majority of whom will never witness a terrorist event--will be required to be able to sense relevant minute changes from normal activity that could alert them to the possibility of a threat. They will also be required to work together to implement policies, processes, and procedures that serve as countermeasures to identified risks. To do so effectively, they will need information about what additional concrete things they must do when new threat information becomes available. In addition, because there are thousands of individuals and organizations involved in detecting, preventing, and responding to attacks and numerous projects being initiated, measures need to be taken to prevent redundancy and inefficiency in homeland security efforts.

To be truly effective, however, the homeland security strategy needs to go beyond promoting redundancy and efficiency to finding innovative approaches to homeland security activities—ones that fully optimize skills, capabilities, and available resources. The asymmetrical threat we face demands that we act in accordance with the Marines' operation motto: "Improvise, Adapt, Overcome." In fact, expeditionary forces within the military provide a good example of how we can find new approaches 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 considerable infrastructure in their deployments. In the Navy and the Marine Corps, for instance, expeditionary forces have the ability to go rapidly and easily to places where there is no infrastructure to operate on their arrival because they carry their infrastructure in the holds of ships and on their back. The forces are trained to be self-reliant, self-sustaining, highly adaptable, and adept in the most austere environments. Because they are uniquely positioned and organized to accomplish a wide range of missions, including long-range strike operations and early forcible entry to

facilitate or enable the arrival of follow-on forces, they have been used in a wide range of missions for decades.

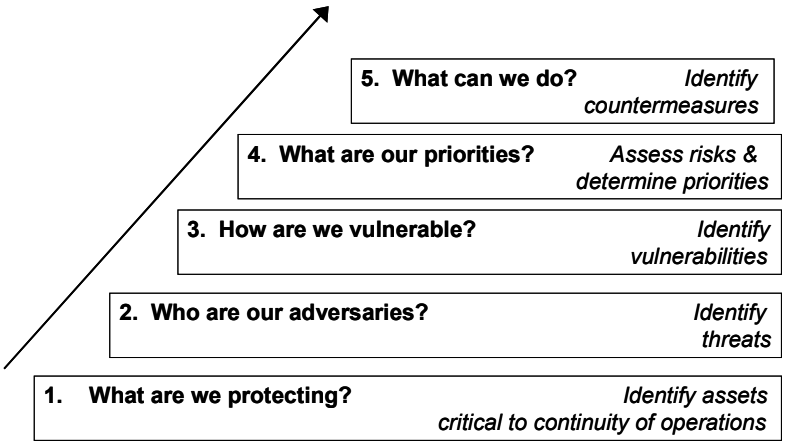
Starting Points

There are some very good starting points for addressing all of these challenges as well as the need to integrate solutions to information-sharing and technology problems. These include applying risk management principles to identifying security priorities and implementing appropriate solutions; developing an architecture for homeland security; developing analytical and warning capabilities; and establishing goals and performance measures and accountability mechanisms.

Risk Management Principles

Risk management principles should be applied to analyze and identify assets that need to be protected to maintain the continuity of critical operations, as well as threats, vulnerabilities, risks, priorities, and countermeasures. It may seem ideal to employ extreme security measures that cover every risk imaginable. But the reality is that this cannot be done, either because doing so could disrupt operations and adversely affect the safety of citizens or the economics of our businesses, or merely be impractical from a resources standpoint. Our previous reports on homeland security and information systems security, have shown that risk management principles can provide a sound foundation in identifying security priorities and implementing appropriate solutions.[13] These principles, which have been followed by members of the intelligence and defense community for many years, can be reduced to five basic steps that help to determine responses to five essential questions:

[13] See U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Oct. 31, 2001) and *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68 (May 1998).



The first step in risk management is to identify assets that must be protected to maintain continuity of critical operations and the impact of their potential loss. The second step is to identify and characterize the threat to these assets. Is the threat, for example, that unauthorized individuals can gain access to the building to commit some crime, or more menacing, that a terrorist will introduce a chemical/biological agent or even a nuclear device into the building. Step three involves identifying and characterizing vulnerabilities that would allow identified threats to be realized. In other words, what weaknesses can allow a security breach? In the fourth step, risk must be assessed and priorities determined for protecting assets. Risk assessment examines the potential for the loss or damage to an asset. Risk levels are established by assessing the impact of the loss or damage, threats to the asset, and vulnerabilities. The final step is to identify countermeasures to reduce or eliminate risks. In doing so, the advantages and benefits of these countermeasures must also be weighed against their disadvantages and costs.

In prior reports, we have recommended that the federal government conduct multidisciplinary and analytically sound threat and risk assessments to define and prioritize requirements and properly focus programs and investments in combating terrorism.[14] Without the benefits that these assessments provide, many agencies have

[14] See U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822, (Washington, D.C.: Sept. 20, 2001); *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T, (Washington, D.C.: Oct. 12, 2001); *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, GAO/NSIAD-98-74,

been relying on worst-case chemical, biological, radiological, or nuclear scenarios to generate countermeasures or establish their programs. By using these worst-case scenarios, the federal government is focusing on vulnerabilities (which are unlimited) rather than credible threats (which are limited).

Homeland Security Architecture

The federal government should develop a blueprint, or architecture, that defines both the homeland security mission and the information, technologies, and approaches necessary to perform the mission in a way that is divorced from organizational parochialism and cultural differences. This would need to be based on the outcome of a risk assessment along with a good understanding of the roles and responsibilities of individuals involved in the homeland security mission. The Office of Homeland Security has acknowledged that an architecture is an important next step because it can help identify shortcomings and opportunities in current homeland-security-related operations and systems, such as duplicative, inconsistent, or missing information. Of course, while the federal government can develop the construct for homeland security, it will be up to state and local governments to carry it out, with a great deal of assistance from the private sector.

Specifically, the architecture should describe homeland security operations in both (1) logical terms, such as interrelated processes and activities, information needs and flows, and work locations and users, and (2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards. It should provide these perspectives both for the current or "as is" environment and for the target or "to be" environment as well as a transition plan for moving from the "as is" to the "to be" environment. A particularly critical function of an architecture for homeland security would be to establish protocols and standards for data collection to ensure that data being collected are usable and interoperable--and to tell people what they need to collect

---

(Washington, D.C.: Apr. 9, 1998) and *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attack*, GAO/NSIAD-99-163, (Washington, D.C.: Sept. 7, 1999).

and monitor.

Many organizations have successfully developed enterprise architectures, though on a much smaller scale, and have found that doing so promotes better planning and decisionmaking; prevents the building of redundant systems; facilitates the management of extensive, complex environments; improves communication and information sharing; focuses on the strategic use of emerging technologies; and achieves economies of scale by providing mechanisms for sharing services. Our experience with federal agencies has shown that managed properly, architectures can clarify and help optimize interdependencies and interrelationships between related enterprise operations and the underlying technology infrastructure and applications that support them.

Readily available frameworks could be used in developing an architecture for homeland security. These include Defense's C4ISR Architecture Framework, the Department of Treasury's Enterprise Architecture Framework, and the Federal Enterprise Architecture Framework, published by the Federal Chief Information Officers (CIO) Council. In addition, the CIO Council, Office of Management and Budget, and GAO have collaborated in producing guidance on the content, development, maintenance, and implementation of architectures.[15]

Analytical and Warning Capabilities

Analytical and warning capabilities should be developed to detect precursors to terrorist attacks so that advanced warnings can be issued and protective measures implemented. Since the 1990s, the national security community and the Congress have identified the need to establish analytical and warning capabilities to protect against strategic computer attacks against the nation's critical computer-dependent infrastructures. Such capabilities involve (1) gathering and analyzing information for the purpose of detecting and reporting hostile or otherwise potentially damaging actions or intentions and (2)

[15]See Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0, (Washington, D.C.: Feb. 2001).

implementing a process for warning policymakers and allowing them time to determine the magnitude of the related risks. In April 2001, we reported on the National Infrastructure Protection Center's progress in developing such mechanisms for computer-based attacks and impediments, which include a lack of a generally accepted methodology for strategic analysis of cyber threats to infrastructures, inadequate data on infrastructure vulnerabilities, and a lack of needed staff and expertise.[16] Similar approaches should be developed for other homeland security priorities.

Goals and Performance Measures and Accountability Mechanisms

Goals and performance measures and accountability mechanisms should be established not only to guide the nation's preparedness efforts but to assess how well they are really working. The Congress has long recognized the need to objectively assess the results of federal programs. For the nation's preparedness programs, however, the outcomes of where the nation should be in terms of domestic preparedness have yet to be defined. Given the recent and proposed increases in preparedness funding as well as the need for real and meaningful improvements in preparedness, establishing clear goals and performance measures are critical to ensuring both a successful and fiscally responsible effort. As we testified earlier this year, without measurable objectives, policymakers would be deprived of the information they need to make rational resource allocations, and program managers would be prevented from measuring progress.[17] In our earlier testimony, we highlighted the recommendation of one expert with the Office of Homeland Security that the government should develop a new statistical index of preparedness, incorporating a range of different variables, such as quantitative measures for special equipment, training programs, and medicines, as well as professional subjective assessments of the quality of local response capabilities, infrastructure, plans, readiness, and performance in exercises. The index could go well beyond current

---

[16]See U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323, (Washington, D.C.: Apr. 25, 2001).

[17]See U.S. General Accounting Office, *Combating Terrorism: Critical Components of a National Strategy to Enhance State and Local Preparedness*, GAO-02-548T (Washington, D.C.: Mar. 25, 2002).

rudimentary milestones of program implementation to capture indicators of how well a particular city or region could actually respond to a serious terrorist event.

-- -- -- -- --

In conclusion, developing a comprehensive and sustainable homeland security strategy is a formidable, even unprecedented task. Because of the nature of the threat, the scope of the things that need to be done are seemingly endless. There are significant challenges on a variety of fronts, particularly in making sure that the right information gets to the right people at the right time and in making good use of technology. Moreover, any solution must be national in nature, not just a federal strategy, since over 80 percent of nation's infrastructure is privately owned, and state and local government are the front line defenders and responders in the fight against terrorism. While there are no quick fixes or "silver bullet" single solutions, there are good starting points for addressing specific areas of challenges as well as for weaving solutions together to develop an integrated framework for preventing, detecting, and responding to attacks.

Even with these mechanisms in place, however, there will still be a need for strong leadership on the part of the federal government and the Congress not just to provide the resources, expertise, and training needed carry out the strategy, but to work through concerns and barriers, develop trust relationships, make sure things are working as they should, and most importantly, sustain national attention to the problem.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have.

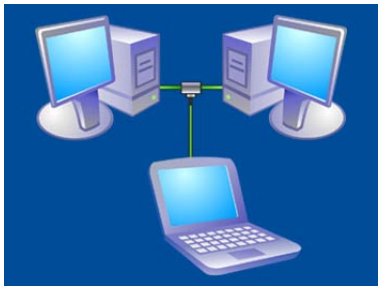
CONTACT AND ACKNOWLEDGEMENT

For further information, please contact Randall A.Yim at (202) 512-6787. Individuals making key contributions to this testimony include Cristina Chaplain and Dave Powner.

Building Tools to Detect and Assess Terrorist Threats

Getting information to the right people at the right time is critical, but we also need an intelligent strategy to integrate the information. One way is to build baselines of normal activity and mechanisms that will enable us to effectively detect deviations or anomalies that would indicate threats and how serious they may be.

First step: Use Existing Technology



Intrusion detections systems are already being used to protect critical computer networks. 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.

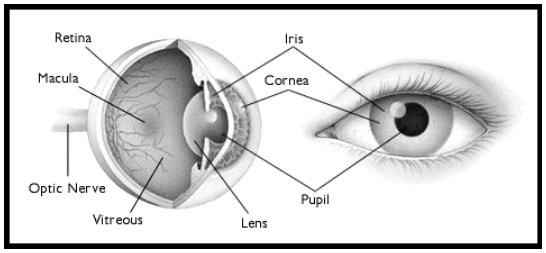
Next step: Apply the Same Know-How to Protect Other Infrastructures

For example, security information systems can be built to assess threats to air travel. Data could be drawn from government watch lists and airline reservations systems. Deviations could be identified by matching names from reservation systems to government watch lists or by detecting unusual patterns in travel or reservations.

The Challenge Ahead

Building systems to predict and detect deviations on larger scale, for example, to protect major cities. This will be an extremely complex and difficult endeavor. 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.

Technologies that can be used in this regard include geospatial digital information tools, including remote sensing and satellite imagery technology.



Iris scan technology is based on the unique characteristics of the eye's iris, the colored ring that surrounds the pupil.
(976301)

Developing other new technologies needed to detect and protect people, buildings, and critical infrastructures from attack. This includes

- Bioweapons- and low-level-radioactive-weapons-detection systems
- Disease surveillance systems
- Biometric devices, such as iris scans and facial recognition systems, facial recognition systems, and speaker verification systems.