

# **CYBERSECURITY FOR THE HOMELAND**

**December 2004**

**Report of the Activities and Findings**

**by the Chairman and Ranking Member**

**Subcommittee on Cybersecurity, Science, and Research & Development**

**of the**

**U. S. House of Representatives Select Committee on Homeland Security**

# **CYBERSECURITY FOR THE HOMELAND**

---

**EXECUTIVE SUMMARY ..... 3**

**INTRODUCTION .....6**

**CASE FOR ACTION ..... 8**

- Vulnerabilities
- Threats
- Economic Perspective
- Private Sector
- Emerging Technology and the Future

**ROLE OF THE DEPARTMENT OF HOMELAND SECURITY ...16**

- Information Analysis and Infrastructure Protection Directorate
- Cybersecurity Duties and Responsibilities
- National Cybersecurity Division Activities

**SUBCOMMITTEE OVERSIGHT ..... 22**

- Subcommittee Jurisdiction
- Subcommittee Membership
- Subcommittee Activities

**CYBERSECURITY ROADMAP FOR THE FUTURE ..... 34**

- Department of Homeland Security Activity for 2005
- Congressional Activity for 109<sup>th</sup> Congress
- Conclusion

## EXECUTIVE SUMMARY

---

September 11, 2001, changed the life of each and every American and brought to the forefront a compelling need to change how the federal government is organized to meet new and emerging challenges to our homeland and national security. Congress and the President worked together to create the Department of Homeland Security (DHS). The U.S. House of Representatives created a Select Committee to oversee the new Department and its activities.

A growing yet underestimated threat is that of a cyber attack on U.S. critical information infrastructures. Criminals, terrorists, and foreign governments are exploiting the anonymity and global reach of the Internet to attack the U.S. information infrastructure; perform reconnaissance for physical attack; conduct hostile information operations; steal money, identities, and secrets; and potentially undermine the U.S. economy. In many respects this threat is escalating due to the increased availability of automated tools for malicious actions, the complexity of the technical environment, and the increased dependence of our society on interconnected systems.

The information infrastructure is unique among the critical infrastructures because it is owned primarily by the private sector, it changes at the rapid pace of the information technology market, and it is the backbone for many other infrastructures. Therefore, protection of this infrastructure must be given the proper attention throughout government.

The Department of Homeland Security brought together for the first time under a single organization, elements of the federal government devoted to cybersecurity and protecting the critical information infrastructure. Similarly, the Subcommittee on Cybersecurity, Science, and Research & Development of the Select Committee on Homeland Security was established to oversee DHS's cybersecurity and science and technology efforts. The Subcommittee devoted considerable effort working with DHS, the private sector, and the academic community to ascertain the most important cybersecurity-related issues and identify possible actions to make cyberspace safer for all users.

The Subcommittee believes DHS has made some progress in improving cybersecurity but has much work to accomplish in the coming years. DHS created the National Cybersecurity Division (NCSA), the U.S. Computer Emergency Readiness Team, the technical National Control Systems Center, and several government coordination entities. Many of these elements existed in some form prior to the establishment of DHS, and now is the time to build toward more robust capabilities. DHS also conducted outreach sessions with the private sector, but more effort is needed in working across critical infrastructure sectors as well as with state and local governments.

In the coming year, the challenge will be to bring together resident expertise, programs, and budgets within DHS to develop a roadmap that fully implements the *National Strategy to Secure Cyberspace*. Based on the Subcommittee's work during the past year, there are six specific recommendations for the Department to consider:

1. Create an Assistant Secretary of Homeland Security within the Information Analysis and Infrastructure Protection Directorate to improve integration of the cybersecurity mission

- within the Department and coordination of cybersecurity best practices, risk assessments, and warnings across all levels of government and with the private sector;
2. Develop comprehensive and detailed program and budget information that delineates current and future plans and links expenditures to the goals of the *National Strategy to Secure Cyberspace*. Such a plan should include implementation guidance and personnel recruiting, retention, and assignment goals;
  3. Update the plan for outreach and coordination and improved information sharing with the private sector. Such a plan should consider the varying needs of different segments of the private sector, including owners and operators of the critical information infrastructure; companies that provide products and services that help secure the critical information infrastructure; and small and large business users and individual citizens. The plan should also include developing innovative mechanisms for information sharing on cybersecurity threats, vulnerabilities, best practices, emergency response, and solutions;
  4. Improve performance on cyber risk assessments and remediation activities to include a plan for Internet-related recovery in the event of a disaster or coordinated attack, and work closely with cyber first responders across federal, state, local, and private sectors.
  5. Identify specific initiatives for NCS and the National Communications System (NCS) to work together because of the increasing similarity of their respective missions and the convergence of voice and data technology; and
  6. Support research and development and educational activities to improve cybersecurity products and services that are user friendly and keep pace with risk and technology.

The Subcommittee Chairman and Ranking Member also introduced legislation, H.R.5068, “The Department of Homeland Security Cybersecurity Enhancement Act of 2004,” to improve the cybersecurity posture within the Department of Homeland Security and to provide a standard definition for cybersecurity within the federal government. A subsequent version of the legislation was included in the House passed version of the “9/11 Recommendations Implementation Act,” S.2845. Specifically, this legislation included a provision (Sec. 5028) to create an Assistant Secretary for Cybersecurity within DHS.

In the coming year, legislative initiatives that should be considered by Congress include creation of an Assistant Secretary for Cybersecurity (if not enacted by the 108<sup>th</sup> Congress) and working with the private sector and other committees of jurisdiction to develop insurance and incentive options for companies that implement cybersecurity programs. Congress should consider specific incentives that would encourage the private sector to raise cybersecurity standards for all users. Oversight topics include ensuring DHS is promoting improved cybersecurity science, technology, education, and training; assessing current and future DHS cybersecurity plans, programs, and budgets; gauging the success of cybersecurity mission execution; and encouraging the Department to develop metrics to show how its actions are improving cybersecurity and reducing cyber vulnerabilities throughout the nation.

The government is working to make the nation safer than it was in the days preceding and immediately following the terrorist attacks on our homeland. The men and women of the Department of Homeland Security, along with other elements of government, state and local first responders, businesses, and individual citizens have worked to achieve this end. Whether it is protecting borders, bolstering transportation security, or improving first responder capabilities, the cyber infrastructure often provides the basis for successful operations and communications. DHS

has a unique opportunity and mandate to bring together different government and non-government entities to improve cybersecurity. The nation still faces homeland security challenges on many fronts. But, with challenges come opportunities for improved cooperation, advances in technology, and more efficient and effective government. We are hopeful that with a renewed spirit among all Americans to do our part in homeland security, including cybersecurity, we will continue to become safer in the days and years ahead.

## INTRODUCTION

---

On a fateful day in September 2001, our lives changed forever as a handful of terrorists dramatically proved they had the means to destroy on a level equal to their hatred. Each and every American felt a loss of sanctuary and a loss of security. The government responded and took initial steps to reorganize the federal bureaucracy to better protect the homeland and its citizens. Congress and the Executive Branch worked together to create the Department of Homeland Security. Congress established homeland security appropriations subcommittees in the House and Senate.

In January 2003, the U.S. House of Representatives also created a Select Committee on Homeland Security to improve coordination efforts among federal agencies tasked with protecting our homeland from terrorist attacks and to oversee the newly created Department of Homeland Security. The Subcommittee on Cybersecurity, Science, and Research & Development was given responsibility for the authorization and oversight of the Department's activities related to security of computers, telecommunications, information technology, industrial control, electric infrastructure, and data systems, including science and research and development; protection of government and private networks and computer systems from domestic and foreign attack; and prevention of injury to civilian populations and physical infrastructure caused by cyber attack.

During the 108<sup>th</sup> Congress, the Subcommittee conducted numerous hearings and briefings for Members of Congress and staff on cybersecurity issues. The Subcommittee also reached out to diverse groups and individuals on ways to improve cybersecurity for the nation. Since May 2003, fifteen hearings and briefings were conducted, as well as several other informal sessions with Members and staff. The Committee heard from private sector experts who own and operate critical information infrastructure. Federal, state, and local government officials and academic experts testified on the need to fortify the nation's cybersecurity. A variety of witnesses also discussed the Department of Homeland Security's role and responsibilities in helping to improve cybersecurity.

One product of the Subcommittee's work was legislation to create an Assistant Secretary for Cybersecurity within DHS. The other major product is this report—a bipartisan effort that highlights key cybersecurity issues and recommends a course of action for improving the Department of Homeland Security's effectiveness in securing cyberspace.

When DHS was created at the beginning of 2003, it inherited the missions of several existing cyber-related organizations previously located in other agencies, including the Federal Bureau of Investigation (FBI), the General Services Administration, and the Departments of Commerce, Defense, and Energy. During these early months, the cybersecurity mission was neither well structured nor organized as DHS struggled with the overwhelming task of assimilating fragmented organizations from other agencies. In addition, some of these agencies, such as the FBI, did not transfer to DHS the personnel associated with its cyber-related activities.

Given these factors, the Subcommittee initially focused its oversight on the key management functions required for the success of any organization. Through hearings and oversight letters, the Subcommittee questioned DHS about its cybersecurity mission and functions. The Subcommittee was also interested in how DHS was developing working definitions related to cybersecurity and

what progress it was making to implement a viable organizational structure, as well as formal personnel, resource, and programmatic planning efforts. Success was measured in the Department's ability to provide its workforce and Congress the core planning documents required to function and grow. From these initial plans, progress was gauged by results, such as milestone completion, budget execution, hiring, space allocation, policy publications, and process controls.

Unfortunately, the level and detail of planning documents needed to manage the new cyber mission within DHS was not forthcoming. Budget paperwork throughout the fiscal year was vague. It is still unknown whether spending plans and detailed budget execution data exists.

Indeed, the organizational structure for national cybersecurity was not announced until June 2003 when DHS created the National Cybersecurity Division (NCSD) within the Information Analysis and Infrastructure Protection Directorate. Due to a variety of factors, including the perceived relatively low priority of the cybersecurity mission within DHS, the Department was unable to find a suitable director for the NCSD until September 2003. Once in place, the Director, a well-respected cybersecurity expert with experience in both the private and government sectors, left the Department after only a year and has not been permanently replaced as of this writing.

Throughout 2004, Subcommittee hearings and briefings reviewed DHS cybersecurity program planning, budget authorization, and organizational issues. During a series of closed briefings with critical infrastructure sector representatives, the Subcommittee focused on developing a dialogue for public-private partnerships and information sharing. Subcommittee staff also held numerous meetings and interviews with individuals at the federal, state, and local government level; companies of all sizes invested in cybersecurity; academic entities; and associations representing technology, education, and business interests.

As the Subcommittee completes its work in the 108<sup>th</sup> Congress, there are several areas which should be the focus of future work on cybersecurity policy and legislation. Securing cyberspace must be a national security and homeland security priority that requires strong oversight from Congress and an organized effort from DHS.

## **CASE FOR ACTION**

---

The United States is the world leader in the information revolution with technological innovations, products, and services. The vast majority of America's critical infrastructures, including the information infrastructure, is owned and operated by the private sector. These infrastructures are increasingly susceptible to attack. If vulnerabilities and threats are not adequately managed throughout product and services lifecycles and by individuals, businesses, and government, the way America conducts business, manufacturing, and even recreational activities will be negatively affected as criminals, terrorists and other adversaries seek to gain profit and do us harm.

### **Vulnerabilities**

Information technology and American ingenuity have revolutionized almost every facet of our lives. From education to recreation and from business to banking, the nation is dependent on telephones, cellular phones, personal digital assistants, computers, and the physical and virtual infrastructure that ties them all together. Almost all data and voice communications now touch the Internet—the global electronic network of computers (including the World Wide Web) that connects people, ideas, and information around the globe.

Technology provides the nation with immeasurable opportunities, giving citizens global access and making daily transactions more affordable, efficient, and interactive. Unfortunately, the same characteristics that make information technologies so valuable also make those technologies attractive to criminals, terrorists, and others who would use the same tools to harm society and the economy.

Despite the growing threat, security and efforts to protect information often remain an afterthought frequently delegated to a Chief Information Officer or a Chief Technology Officer. Cybersecurity should be treated as a cost of doing business by the highest levels of an enterprise's leadership because the ability to conduct business and assure delivery of services to consumers—whether it is banking, electrical, or manufacturing—depends on ensuring the availability of information and related infrastructure.

During a June 25, 2003, hearing of the Subcommittee entitled "Overview of the Cyber Problem: A Nation Dependent and Dealing with Risk," Richard Pethia, Director, CERT® Centers, Software Engineering Institute, Carnegie Mellon University testified:

"Government, commercial, and educational organizations depend on computers to such an extent that day-to-day operations are significantly hindered when the computers are 'down.' It is easy to exploit the many security holes in the Internet and in the software commonly used in conjunction with it; and it is easy to disguise or hide the true origin and identity of the people doing the exploiting....Moreover, the Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries."

Addressing vulnerabilities requires additional attention. For example, companies that develop hardware, software, and networking platforms should continue to strive to eliminate as many flaws and vulnerabilities as possible before their products enter the market. While it is nearly impossible to create a product that is 100% error-free, several IT security businesses stated that they have efforts underway to increase the security and dependability of pre-marketed technologies. The Subcommittee views these initiatives as positive. More, however, can be done. Both Congress and the Department of Homeland Security should consider incentives and recognition programs to encourage private industry to develop more secure cyber products.

Additionally, all users—from the individual consumer to the large corporation—should strive to understand vulnerabilities within their networked environment and safeguard against them. It is also necessary to prepare mitigation and contingency plans to respond if a vulnerability is exploited.

## **Threats**

Cyber threats are growing and perpetrators are becoming more organized. Cyber threats can take a variety of forms, including espionage, hacking, identity theft, crime, and terrorism. Terrorists, criminals, and foreign governments are all known players. One homeland security concern is that criminal, espionage, and terrorist operations may converge in cyberspace as terrorist motivation shifts from “destroying” an adversary’s economy to one of “controlling” it. Taken in total, illegal cyber activities may soon become one of the principal long-term threats to the homeland.

As stated in a 1990 report by the National Research Council, "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." During the 1980s, several hacking “incidents” demonstrated how the United States could be affected by poor cybersecurity. In 1986, the U.S. experienced cyber espionage when a \$ .75 discrepancy in two accounting programs in Berkeley, California, led to Germany and the discovery of KGB agents trying to ferret out U.S. military secrets.

The first widespread worm attack through networked computers occurred in 1988 when Robert Morris, Jr., a Cornell University student and the son of a prominent NSA scientist, developed a program that crippled approximately 6,200 computers and caused over \$98 million in damage in approximately 48 hours. Also in 1988, a hacker group called “Legion of Doom” demonstrated the vulnerability of the critical infrastructures by penetrating sensitive administrative computers. Even Hollywood contributed to the cybersecurity mystique. In 1983, the film *War Games* helped frame the view that cyber crime is mostly about smart teenagers testing their intellect and knowledge of computers.

Today, a prime motivation for cyber attacks is money: a high return on minimal investment and a high degree of anonymity. Terrorists or criminals can obtain or launder money across the Internet, typically by disguising their activities through miscreant cutouts. The orderliness and command structure of criminal and terrorist organizations is growing. The anonymous and complex nature of the Internet makes it even more difficult to monitor and track violators. Hacking crews and individuals are working together across the globe in a virtual, anonymous network of individuals who specialize in different types and parts of attacks, such as propagation speed, denial of service, password logging, and data theft.

One way to understand the potential magnitude of the problem is to compare the current Internet “underground” environment with the evolution and growth of organized crime in the 1920s. During the early years, a period of chaos existed until leaders organized themselves into neighborhood territorial gangs. Eventually operations grew into nationally controlled enterprises of gambling, prostitution, and drugs. Larger geographic territories were staked out among leaders who established an extensive command and control network for using local mobsters to perform various jobs. Personal contact was a primary method for authentication and contact within the organization.

Just as 1920s gangsters evolved into organized crime syndicates, a sophisticated command and control network is emerging within the Internet with agreed-upon boundaries of control and “gangs” working for a “boss.” These modern criminals and terrorists often don’t know or meet the crews who carry out the actual cyber attacks, making it even more difficult to track and prosecute them.

As the National Intelligence Council stated in response to a request from the Subcommittee in June 2003, “an increasing number of adversaries are developing new options for exerting leverage over the United States through cyberspace....Creating damage as well as conducting espionage against the U.S. Cyberspace provides clear avenues and the prospect of anonymity.”

As with organized crime, terrorists are becoming more structured to take advantage of “hackers for hire.” Better educated and now motivated by a movement against Western states, multi-generational terrorist leaders can move quickly and virtually through cyberspace to strike at the very heart of the Western economic infrastructure.

A capitalist market could easily become a funding mechanism to support traditional terrorist tactics. As a result, organized crime, terrorists, and state sponsors may well be able to operate in the same environment, ultimately negotiating for control and access to financial information and the money it brings to their respective activities.

Espionage, mostly from state-sponsored activities, is another motivation for cyberattacks against government and academic facilities. The National Intelligence Council advised the Subcommittee in their June 2003 response:

"Foreign governments, hackers and industrial spies are constantly attempting to obtain information and access through clandestine entry into computer networks and systems. This is not just ‘surfing’ the open Internet for information voluntarily placed in the public domain, but intruding into closed and protected systems to steal secrets and proprietary information....Foreign corporations also could turn to computer intrusion to tamper with competitors’ business proposals, in order to defeat competing bids. Such computer network espionage or sabotage can affect U.S. economic competitiveness and result in technology transfer—directly or through product sales—to U.S. adversaries."

Statistics from a variety of sources also support the notion that the cyber threat faced by our nation is growing in magnitude and consequence:

- 27 million Americans have suffered identity theft since 1999 (this includes credit card, Social Security, and personal data). (*Source: Federal Trade Commission*)

- Over \$222 billion in losses were sustained by the global economy as a result of ID theft. (Source: Aberdeen Group June 2003 Report on the Economic Impact of ID Theft)
- 4,700 Suspicious Activity Reports per Computer Intrusion were reported in 2003—a 100% increase. (Source: FINCEN, U.S. Treasury)
- 3600% increase in domestic computer crime since 1997. FBI Director named Cyber-crime the nation’s number one criminal problem. (Source: ITAA book "Long Campaign")
- Between 1999 and 2003 in the U.S., attacks on computer servers increased by over 530% to over 140,000 incidents for 2003. The number of new vulnerabilities discovered in software is growing at 140% per year and is now in excess of 4,000 per year. (Source: CERT/CC)

In his July 2003 testimony before the Subcommittee, Mr. Philip Reiting, Senior Security Strategist at Microsoft Corporation and former Department of Justice official, stated, “because most cyber attacks are not discovered or, if discovered, are not reported, and because we have no national or international statistically rigorous measurement of damages from cyber crime, the exact cost of cyber attacks to companies and consumers is unknown.” He went on to say that bad actors in cyberspace “act with the knowledge that they are highly unlikely to be caught, let alone prosecuted and imprisoned.”

Mr. Reiting’s statements support the information provided to the Subcommittee by law enforcement and intelligence agencies. A cyber attack on the backbone of one of the nation’s critical information infrastructures could disrupt America’s physical and economic well-being and have a substantial worldwide impact.

While connectivity and convenience are pivotal in the technologically advanced world, the need to protect cyber assets becomes even more important because of the transformation of modern day crime and terrorism. The Information Age and the nation’s reliance on computer networks coupled with less than robust security help facilitate fraud. The inherently transnational and anonymous nature of the Internet also facilitates criminal activity.

The evidence of the cyber threat is growing. New vulnerabilities are found each day. Those interested in exploiting these vulnerabilities are becoming a well-organized underground. A priority for the Department of Homeland Security must be to improve its ability to correlate vulnerabilities and threats in a given environment, produce a dynamic risk assessment, and plan for how to move forward with securing critical portions of the information infrastructure. The private sector, the Department of Homeland Security, the intelligence community, and law enforcement must also work together more productively and more rapidly. There is still much to be done in this area, both domestically and internationally, as illegal cyber activities may soon become one of the principal long-term threats to the homeland.

## **Economic Perspective**

Any individual, business, or government entity suffering an outage due to a cyber attack is faced with inconvenience and the need to divert resources to recover. Unfortunately, little empirical information is available on actual costs of cyber attacks to the nation, companies, or individuals. To help understand the complexities in measuring the cost impact from cyber attacks, the Subcommittee requested the Congressional Research Service (CRS) investigate and prepare a report

on this topic. As part of its analysis, CRS provided a comparative analysis of proposals and activities relating to cost measurement, drawing on experiences of industry and academia.

CRS determined that an economic business case for evaluating cybersecurity does not exist. However, CRS was able to identify the elements of an end-to-end business case that would be needed to make such an assessment. These include measuring the costs of preventive actions as well as costs of recovery from attacks. While extensive research has gone into preventive measures, little is known about how to measure the effects of an attack.

In April 2004, CRS provided the Subcommittee with its report, "*The Economic Impact of Cyber Attacks*." The report concluded, "No one in the field is satisfied with our present ability to measure the costs and probabilities of cyber attacks. There are no standard methodologies for cost measurement, and study of the frequency of attacks is hindered by the reluctance of organizations to make public their experiences with security breaches."

The insurance industry has the ability to contribute to the development of a cost methodology through its customer base but is currently limited in the number of specialized cyber risk policies available. CRS found that the "growth of cyber risk insurance is hindered primarily by a lack of reliable actuarial data related to the incidence and costs of information security breaches; enhanced collection of such figures would probably be the most important contribution that policy can make."

Most everyone will agree on the need for accurate and statistically comprehensive data on the incidence and costs of cyber attacks. As a 2002 World Bank study found, "the existing base of information that supports projections about the extent of the electronic security problem is substantially flawed."

If information gathering has the potential to reduce costs and risks, why does the data shortfall persist? According to the CRS report, "[T]here are two chief obstacles. First, there are strong incentives that discourage the reporting of breaches of information security. Second, organizations are often unable to quantify the risks of cyber attacks they face, or even to set a dollar value on the cost of attacks that have already taken place. Thus, even if all the confidential and proprietary information that victims have about cyber attacks were disclosed and collected in a central database, measurement of the economic impact would still be problematical."

Regrettably, many people continue to use metrics and methodologies from the physical environment when thinking about cyberspace. As CRS determined, "There is a fundamental difference between a cyber attack and a conventional physical attack in that a cyber attack generally disables—rather than destroys—the target of the attack. Because of that difference, direct comparison with previous large-scale disasters may be of limited use."

There are two events, however, that may assist in the development of a cybersecurity model. The first is the "Y2K" fix that was required to prevent anticipated computer hardware and software problems as the calendar changed from 1999 to 2000. The second event was the electrical blackout that affected much of the northeastern United States in August 2003. Unfortunately, "Y2K" may be of limited value since it involved a specific problem and there was a certain date by which solutions were needed. However, cyber vulnerabilities are constantly evolving. An analysis of the electrical blackout of August 2003 provides more useful information: the CRS *Report on Economic Impact*

*of Cyber Attacks* indicated the power failure cost between \$6 billion and \$10 billion, disrupted production, affected earnings and profits, spoiled food supplies, and increased first responder costs for some communities. Like a cyber attack, there was little, if any, destruction of physical capital.

Building an economic business case for cybersecurity is possible, but more research is needed in modeling and simulation and in developing a cost methodology. If market forces are to drive investment in cybersecurity, insurance and auditing industries may have the most salient and helpful experience.

Still, one main obstacle must be overcome: obtaining information and data from companies that have experienced a cyber attack. As CRS found during its research, “comprehensive data on information security breaches are lacking not because the value of such data is not generally recognized. The problem is that organizations have real economic incentives not to reveal such information.” Many companies accept losses as a cost of doing business while others believe that sharing loss information could reduce customer confidence in their products and services. Providing market incentives and building trusted relationships could help inroads with the private sector.

## **Private Sector**

When it comes to cybersecurity in the private sector, significant responsibility resides within the corporate boardroom. The Cyber Summit Task Force on Corporate Governance tackled this issue, producing an April 2004 report entitled, “Information Security Governance: A Call to Action.” In the report, the task force calls for the private sector to incorporate information security into its corporate governance efforts:

“The road to information security goes through corporate governance. America cannot solve its cybersecurity challenges by delegating them to government officials or CIOs [Chief Information Officers]. The best way to strengthen U.S. information security is to treat it as a corporate governance issue that requires the attention of Boards and CEOs [Chief Executive Officers]....Although information security is often viewed as a technical issue, it is also a governance challenge that involves risk management, reporting and accountability. As such, it requires the active engagement of executive management.”

It is clear that information security governance requires that corporate management take the lead in securing computer systems. The April 2004 Congressional Research Service paper on *The Economic Impact of Cyber Attacks* suggests that “firms that best manage cyber risk will be rewarded by a competitive market. It may be useful for public and private groups to put forward sets of guidelines and best practices, but only to the extent that these are seen as minimum requirements, not complete and sufficient responses to cyber risk.”

CRS further suggests that the private sector may move forward on information security efforts to avoid liability: “The prospect of being sued for damages when confidential information is stolen or destroyed is a major incentive for firms to improve information security. It is also, however, a major disincentive for sharing information about cyber attacks. Some may suggest that limits or caps on liability related to cybersecurity breaches would make firms less reluctant to disclose incidents. In theory, lower liability would also reduce the incentive to invest in security, but, in

practice, since liability is only one of many costs that influence risk management decisions, this effect might be very slight.”

As the CRS report implies, market forces may need some assistance in stimulating the private sector to move towards stronger corporate governance and investments in cybersecurity. These are areas where new legislation could be explored. However, it is important to realize that industry may be incentivized to do more than government could regulate. The nation cannot afford for legislative mandates to become both a floor and a ceiling with respect to organizations’ efforts to secure their systems, because it is difficult to stay ahead of technology and the free market. Others have expressed the view that we may already have enough laws to implement strong cybersecurity and need to understand the implications of existing legislation such as Sarbanes-Oxley and Health Insurance Portability and Accountability Act (HIPAA). Other options are available to promote cybersecurity practices, such as tax incentives, safe harbor provisions, contractual incentives, and insurance. All these areas need to be explored further to ensure they could be effective and not result in unintended consequences for our nation.

## **Emerging Technology and the Future**

As the nation’s dependence on information technology grows, so should the means to protect this asset. Continued research and development in cybersecurity will be needed.

In response to a Subcommittee request in June 2003, the National Intelligence Council offered:

“The rapid pace of change in information technology suggests that the appearance of new and unforeseen computer and network technologies and tools could suddenly and dramatically shift the advantage in cyber warfare toward the defender or the attacker. Wildcards for the years beyond 2005 include the quantum computing against PKI [Public Key Infrastructure] type encryption and...better use of encryption by the defense. These changes could improve processing power, information storage, and bandwidth enough to dramatically alter the nature of computer network operations. Continuing growth of the interconnectivity of critical infrastructure will be a significant opening of threat pathways, particularly as convergence unfolds into telecom.”

The Subcommittee conducted a hearing entitled, “Cybersecurity—Getting It Right: The Importance of Research in Cybersecurity and What More Our Country Needs to Do,” on July 22, 2003. Representatives from academia, industry, and government discussed cybersecurity research issues. The general consensus from the panel was that more cybersecurity research and better technology transfer were needed. The panel also noted the government has a role in cyber research, particularly in improving coordination across public and private sectors. During this hearing, Dr. Shankar Sastry, Chairman, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, California, said the following:

“In today’s environment there is heightened awareness of the threat of well-funded professional cyber hackers and the potential for nation-state sponsored cyber warfare. A parallel and accelerating trend of the last decade has been the rapidly growing integration role of computing and communication in critical infrastructure systems, such as financial, energy distribution, telecommunication and transportation, which now have complex

interdependencies rooted in information technologies. These overlapping and interacting trends force us to recognize that trustworthiness of computer systems is not just an information technology issue anymore; it has a direct and immediate impact on critical infrastructure.”

At the same time, it is clear that homeland security efforts must take advantage of existing technology, including those from the national security community. Mr. Daniel G. Wolf, Director of Information Assurance, National Security Agency, emphasized this point in testimony to the Subcommittee by stating,

“Homeland security presents another reason to suggest that cybersecurity requirements must converge....In almost all cases the cybersecurity requirements found in national security systems are identical to those found in e-commerce systems or critical infrastructures. It follows that the research challenges, security features and development models are also quite similar. Our goal is to leverage our deep understanding of cyber threat and vulnerability in a way that lets us harness the power and innovation provided by the information technology industry. We believe that the resulting cybersecurity solutions will protect all critical cyber systems, regardless of the information they process.”

Information technology advances are both complex and rapid. To make information systems safe and available for use, security must be included in the initial research and development stages. This is especially true for homeland security applications where wireless, biometric, and other products are increasingly connected and integral to keeping the nation safe. These technologies should have security features included as part of their design. In addition, the Department of Homeland Security must bring together existing expertise in the government, private sector, and academia to promote emerging and innovative cybersecurity technologies.

# **ROLE OF THE DEPARTMENT OF HOMELAND SECURITY**

---

## **Information Analysis and Infrastructure Protection Directorate**

The Information Analysis and Infrastructure Protection (IAIP) Directorate was created to bring together threat and vulnerability information for meaningful risk assessments of critical infrastructure. According to a February 2004 DHS Office of Inspector General Report,

“IAIP analyzes and integrates terrorist threat information, mapping those threats against both physical and cyber vulnerabilities to critical infrastructure and key assets, and implementing actions that protect the lives of Americans, ensures the delivery of essential government services, and protects infrastructure assets owned by US industry. IAIP is unique in that no other federal organization has the statutory mandate to carry out these responsibilities under one organizational framework.

“Within IAIP, there are two organizations devoted to cyber functions—the National Cyber Security Division (NCS) and the National Communications System (NCS). The NCS is responsible for identifying, analyzing and reducing cyber threats and vulnerabilities; disseminating cyber-threat warning information; coordinating incident response; providing technical assistance in continuity of operations and recovery planning; and outreach, awareness, and training. The NCS monitors the vulnerabilities of the telecommunications industry; and coordinates national security and emergency preparedness (NS/EP) communications for the federal government during non-terrorism related emergencies, terrorist attacks, and recovery and reconstitution operations.”

These responsibilities are explained in more detail in the sections that follow.

## **Cybersecurity Duties and Responsibilities**

The Department of Homeland Security derives its cybersecurity responsibilities and duties from legislation and Presidential orders and strategies. The Congressional Research Service prepared a summary of these roles and responsibilities:

- Statutory Responsibilities;
- Lead Agency;
- Implementing the *National Strategy to Secure Cyberspace*;
- Support for the National Infrastructure Advisory Council; and
- Support for the National Security Telecommunications Advisory Committee.

### **Statutory Responsibilities**

The Homeland Security Act of 2002 (P.L. 107-296) mandated several infrastructure protection responsibilities that relate to the Department’s cybersecurity mission. The Act also transferred many of the existing federal cyber programs to DHS. Among those programs and functions transferred were the following:

- National Infrastructure Protection Center (from the Federal Bureau of Investigation);
- National Communication System (an interagency group formerly supported by the Department of Defense);
- Critical Infrastructure Assurance Office (from the Department of Commerce);
- National Infrastructure Simulation and Analysis Center (a partnership between Sandia and Los Alamos National Laboratories, supported by the Department of Energy); and
- Federal Computer Incident Response Center (from the General Services Administration).

The Act also required DHS to take the lead in coordinating infrastructure protection activities, including working with state and local governments, private sector critical infrastructure owners and operators, and intelligence and law enforcement agencies. The Department became responsible for threat and vulnerability analysis and warning and also for analyzing related intelligence and law enforcement information.

The Homeland Security Act additionally authorized DHS to establish a National Technology Guard, NET Guard, to assist local communities in responding to and recovering from information and communications systems attacks. The Science and Technology Directorate is responsible for evaluating information security programs for university-based centers for homeland security. The Department is also required to consult with the National Institute of Standards and Technology (NIST) to ensure that appropriate federal information security policies are enacted. Lastly, the Act outlines requirements for the Department's own information technology systems.

### **Lead Agency**

Work on protecting critical infrastructure began before DHS was created. In 1998, *Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* assigned certain federal agencies with responsibilities for helping mission-related sectors of the economy to coordinate, among themselves and with the federal government, for the protection of privately-owned critical infrastructure. At the time, the Department of Commerce was designated the Lead Agency for the Information and Telecommunications Sector.

Subsequently, the *National Strategy for Homeland Security* endorsed the Lead Agency concept, but, in anticipation of the formation of the Department of Homeland Security, assigned DHS as the Lead Agency for Information and Telecommunications.

In December 2003, *Homeland Security Presidential Directive 7 (HSPD-7)* defined lead agency responsibilities for DHS and other departments and agencies. According to the July 2004 Government Accountability Office *Report on Critical Infrastructure Protection*, HSPD-7

“instructed federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. The Secretary of Homeland Security is assigned several responsibilities, including establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors. HSPD-7 designated sector specific agencies with responsibility for infrastructure protection activities

within their assigned infrastructure sectors. Responsibilities include coordinating and collaborating with relevant federal agencies, state and local governments and the private sector and facilitating information sharing about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. Further, the sector-specific agencies are to continue to encourage development of information-sharing and analysis mechanisms and to support sector-coordinating mechanisms.”

Under HSPD-7, the Department of Homeland Security has responsibility for the following critical infrastructure sectors:

- Chemicals and hazardous materials: transforms natural raw materials into commonly used products benefiting society’s health, safety, and productivity;
- Emergency services: saves lives and property from accidents and disaster, including fire, rescue, emergency medical services, and law enforcement organizations;
- Government: ensures national security and administers key public functions;
- Information technology and telecommunications: provides communications and processes to meet the needs of businesses and government;
- Postal and shipping: delivers private and commercial letters, packages, and bulk assets, including the U.S. Postal Service and other carriers; and
- Transportation: enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.

### **Implementing the *National Strategy to Secure Cyberspace***

The President’s February 2003 *National Strategy to Secure Cyberspace* outlined an initial framework for organizing and prioritizing efforts. It provided direction to federal departments and agencies that have roles in cyberspace security. It also identified steps that state and local governments, private companies and organizations, and individual Americans can take to improve cybersecurity. The *Strategy* articulated five national priorities, including:

1. Developing a cybersecurity response system;
2. Creating a threat and vulnerability reduction program;
3. Creating awareness and training programs;
4. Unveiling plans for securing government computers; and
5. Developing plans detailing national security and international cooperation.

### **Support for the National Infrastructure Advisory Council**

Issued in February 28, 2003, Executive Order 13286, Section 3, tasked the National Infrastructure Advisory Council (NIAC) (established by Executive Order 13231 in October 16, 2001) with reporting to the President through the Secretary of Homeland Security and instructed DHS to provide the Council with appropriate administrative and financial support. The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of information systems for critical infrastructure supporting other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services.

## **Support for the National Security Telecommunications Advisory Committee**

Executive Order 13286, Section 47, issued in February 28, 2003, directed the National Security Telecommunications Advisory Committee (NSTAC) (established by Executive Order 12382 in September 1982) to report to the President through the Secretary of Homeland Security. DHS is tasked with providing the Council with appropriate administrative services and financial support. The NSTAC provides the President advice on the security and continuity of communications systems essential for national security and emergency preparedness.

## **National Cybersecurity Division Activities**

The National Cybersecurity Division (NCSA) was created to be the primary organization for cybersecurity activities within DHS. As a result of its oversight activities, the Subcommittee has found the overriding focus for NCSA has been the creation and operation of the U.S. Computer Emergency Readiness Team (US-CERT) and a watch and warning system. While a warning system is needed, the Subcommittee is concerned that other important cybersecurity areas have not received appropriate management attention, including performance of critical information infrastructure threat analysis and risk assessment; building more effective partnerships with the private sector and state governments; and adequate education, training, and outreach efforts.

According to DHS, the US-CERT Operations Center was created to serve as a national real-time focal point for cybersecurity: “It is a 24x7x365 watch and warning capability that provides operational support for monitoring the status of systems and networks in order to provide a synoptic view of the health of the Internet on a continual basis and to facilitate securing those systems and networks. The US-CERT Operations Center conducts daily conference calls across U.S.-based watch and warning centers to share classified and unclassified security information, and provides daily information feeds to US-CERT’s analysis and production functions.”

While the goals of this effort are commendable, the NCSA may not have adequate secure facilities or ready access to classified information to improve the quality and quantity of its analysis and reporting. Without the ability to provide significant and timely value-added information to public and private sector partners, it is unknown whether this reporting center can achieve its full potential or entice the private sector to share additional information.

The US-CERT website is an important outreach tool for the general public, and its secure portal offers a venue for sensitive information collaboration, but much more work is needed to exceed current basic functionalities. It should also be noted that much of this work previously existed in the Carnegie Mellon CERT/CC in Pittsburgh, Pennsylvania.

The National Control Systems Center (NCSC), a subset of the US-CERT, is tasked with addressing complex security issues associated with the use of control systems in most critical cyber systems within the U.S. infrastructure. According to DHS, this is a new function that focuses on what many in government and industry agree is a significant risk area for the nation, particularly after the August 2003 Northeast electric grid blackout. If successful, this Center will facilitate incident coordination, create a testbed for control systems, and investigate technology gaps in control systems.

DHS also announced creation of the National Cyber Alert System to identify, analyze, and prioritize emerging vulnerabilities and threats. According to DHS, the system is managed by the US-CERT and relays computer security update and warning information to all users. It provides all citizens—from computer security professionals to home computer users with basic skills—with free, timely, actionable information to better secure their computer systems. The system sends alerts and other cybersecurity information that provide guidelines and security actions through e-mail.

- *Cybersecurity Alerts*: Available in two forms—regular for home users and advanced for technical users—Cybersecurity Alerts provide timely information about security issues, vulnerabilities, and exploits currently occurring.
- *Cybersecurity Tips*: Written for non-technical home and corporate computer users, the bi-weekly Cybersecurity Tips provide information on computer security best practices.
- *Cybersecurity Bulletins*: Written for technical audiences, Cybersecurity Bulletins provide bi-weekly summaries of security issues, new vulnerabilities, potential impact, patches and workarounds, as well as actions recommended to mitigate risk.

Sharing this type of data among all levels of users is an important initiative that began with advisories and bulletins that were issued by the former FBI's National Infrastructure Protection Center (NIPC). The Subcommittee encourages the DHS to build upon and improve the earlier foundation established by the NIPC.

Several other programs announced by the Department previously existed under the President's Critical Infrastructure Protection Board (PCIPB) within the White House. The Subcommittee is concerned that the transition from more than ten committees under the PCIPB has been difficult and some worthwhile initiatives may not be realizing their full potential. Specifically, the education and infrastructure interdependencies committees require additional management attention. In addition, there is some confusion on DHS's role as it "partners" with other federal agencies which have historically taken the lead in cybersecurity programs, either within government or with the private sector.

Other efforts also require additional attention. For example, rejuvenating the Federal Computer Incident Reporting Center (FedCIRC) program, which previously existed in the General Services Administration, is a critical element to help with cybersecurity problems for federal agencies with non-national security systems.

Over the past year DHS has established or re-established several governmental entities, such as:

- The Government Forum of Incident Response and Security Teams (GFIRST) is a group of technical and tactical practitioners of security response teams responsible for securing government information technology systems. Members work together to understand and handle computer security incidents and to encourage proactive and preventative security practices.
- The National Cyber Response Coordination Group (NCRCG) is a forum of key agencies that coordinates intra-governmental and public-private preparedness and operations to respond to and recover from large-scale cyber attack. The senior level membership of

NCRCG helps ensure that during a significant national incident, the full range and weight of federal capabilities will be deployed in a coordinated and effective fashion.

- The Chief Information Security Officers Forum (CISO Forum) was created to bring together federal officials responsible for the information security of their respective agencies and provides a trusted venue for them to collaborate; to leverage one another's experiences, capabilities, programs, and lessons learned; and to address and discuss particularly problematic or challenging areas.

The Subcommittee recommends that DHS consider reviewing and possibly reconstituting previous programs and processes in the areas of incident response, education, and interdependencies. The Subcommittee also believes that the NCSD and the National Communications Systems (NCS) should work more closely together given the convergence of data and voice technologies. Well-established processes and technology programs already exist with the NCS that could be used to help US-CERT collaborate with the telecommunications industry (through NCS), particularly where incidents and outages could cause cascading effects for other critical infrastructures. During a national crisis, clear lines of communication must be defined so that federal, state, local, and private sector organizations understand the process for response and recovery. With the established national security and emergency preparedness operations for telecommunications, economies can be realized and best practices can be shared within the Department.

# **SUBCOMMITTEE OVERSIGHT**

---

## **Subcommittee Jurisdiction**

Responsibilities for the Subcommittee on Cybersecurity, Science, and Research & Development include authorization and oversight of the Department’s activities related to security of computer, telecommunications, information technology, industrial control, electric infrastructure, and data systems, including science and research and development; protection of government and private networks and computer systems from domestic and foreign attack; and prevention of injury to civilian populations and physical infrastructure caused by cyber attack.

## **Subcommittee Membership**

<b>Mac Thornberry, Texas, Chairman</b>	<b>Zoe Lofgren, California, Ranking Member</b>
Pete Sessions, Texas, Vice Chairman	Loretta Sanchez, California
Sherwood Boehlert, New York	Robert E. Andrews, New Jersey
Lamar Smith, Texas	Sheila Jackson-Lee, Texas
Curt Weldon, Pennsylvania	Donna M. Christensen, U.S. Virgin Islands
Dave Camp, Michigan	Bob Etheridge, North Carolina
Robert W. Goodlatte, Virginia	Ken Lucas, Kentucky
Peter King, New York	James R. Langevin, Rhode Island
John Linder, Georgia	Kendrick B. Meek, Florida
Mark Souder, Indiana	Ben Chandler, Kentucky
Jim Gibbons, Nevada	<i>Jim Turner, Texas, ex officio</i>
Kay Granger, Texas	
<i>Christopher Cox, California, ex officio</i>	

## **Subcommittee Activities**

### ***Congressional Staff Workshop on Cybersecurity***

On July 21, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development sponsored a half-day cybersecurity workshop that was hosted by the Congressional Research Service for Congressional staff from the House and Senate. The purpose of the workshop was to provide staff with fundamental knowledge of cyberspace, cybersecurity, and associated threats. Briefings and demonstrations were received from the following: Alan Paller, Research Director of the SANS Institute; John Nugent, Director of the Center for Information Assurance, University of Dallas; Bruce Schneier, President of Counterpane Systems; Jack Moteff, Specialist in Science and Technology, Congressional Research Service; Tom Donahue, Central Intelligence Agency; Kevin Barry, Lumeta Corporation; Cristin Flynn and Chris Morrow, MCI Telecommunications; and Timothy Allen and Derrick Day, U.S. Secret Service.

### ***Information Sharing and Department Plans***

On August 22, 2003, the Chairman and Ranking Member of the Subcommittee on Cybersecurity, Science, and Research & Development requested a Government Accountability Office report covering two areas:

- The status of the Department’s Information Analysis and Infrastructure Protection Directorate’s plans to protect the computer systems that support our nation’s critical infrastructures; and the extent to which such plans or other actions adequately address the cyber CIP responsibilities established for the Department by law and by Administration policy, including the national strategies and related presidential directives and orders; and
- The status of the efforts of the Information Sharing and Analysis Centers (ISACs), established by federal policy and/or recognized by the Department of Homeland Security, in achieving the objectives of federal policy and current legislation.

***Report on Economic Impact of Cyber Attacks***

On April 1, 2004, the Congressional Research Service (CRS) provided a report to the Subcommittee entitled, “Economic Impacts of Cyber-Attacks,” to help understand the complexities in measuring the cost impact from cyber attacks and their potential impact to the nation. As part of its analysis, CRS provided a comparative analysis of proposals and activities relating to cost measurement, drawing on experiences of industry and academia.

***Report on Critical Infrastructure Information Sharing***

In July 2004, the Government Accountability Office completed its report for the Subcommittee on *Critical Infrastructure Protection—Improving Information Sharing with Infrastructure Sectors*. The report provided specific recommendations to help improve the effectiveness of DHS’s information sharing efforts with the private sector, including the following:

- Proceed with and establish milestones for the development of an information-sharing plan that includes (1) a clear description of the roles and responsibilities of DHS, the ISACs, the sector coordinators, and the sector-specific agencies; and (2) actions designed to address information-sharing challenges. Efforts to develop this plan should include soliciting feedback from the ISACs, sector coordinators, and sector-specific agencies to help ensure that challenges identified by the ISACs and the ISAC Council are appropriately considered in the final plan.
- Considering the roles, responsibilities, and actions established in the information-sharing plan, develop appropriate DHS policies and procedures for interacting with ISACs, sector coordinators, and sector-specific agencies and for coordination and information sharing within the IAIP Directorate and other DHS components that may interact with the ISACs.

***Radio Frequency Identification Systems***

On August 30, 2004, the Chairman and Ranking Member of the Subcommittee on Cybersecurity, Science, and Research & Development requested a Government Accountability Office report on the implementation of radio frequency identification systems.

***Cyber Exercise***

On February 24, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development sponsored a cyber exercise hosted by the Secretary of Defense and National Defense University. Members of the Select Committee participated in a scenario driven mock event that explored the vulnerabilities of national information infrastructure to attack and asked for Members’ input on how best to restore and strengthen the infrastructure.

### ***Congressional Staff Roundtable on Information Technology and High Tech Venture Capital***

On November 18, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development hosted a roundtable discussion with House professional staff members and several venture capital firms to discuss homeland and national security technology needs and priorities and how these firms could be helpful.

### **Oversight Activities – DHS Correspondence**

#### ***Budget Request***

On February 2, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development submitted a letter to the Department of Homeland Security requesting information on its cybersecurity budget, organizational and planning documentation, internal and external coordination processes and activities, and copies of internal and external service level agreements.

#### ***US-CERT and CERT/CC Partnership***

On March 19, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development submitted a letter to the Department of Homeland Security regarding the US-CERT partnership with the Carnegie Mellon University Computer Emergency Response Team Coordination Center (CERT/CC), requesting feedback on how this arrangement would impact pre-existing arrangements with the private sector and international community.

#### ***National Cybersecurity Summit Task Forces***

On April 7, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development submitted a letter to the Department of Homeland Security encouraging the Department to consider recommendations from the public-private task forces created during the DHS-sponsored National Cybersecurity Summit, including the following:

- Awareness for Home Users and Small Businesses
- Cybersecurity Early Warning
- Corporate Governance
- Security Across the Software Development Life Cycle
- Technical Standards and Common Criteria

#### ***National Cybersecurity Mission***

On April 28, 2004, the Select Committee on Homeland Security and the Subcommittee on Cybersecurity, Science, and Research & Development submitted a letter to the Department of Homeland Security requesting a detailed action or implementation plan that links the Department's cyber program and budget needs to the *National Strategy to Secure Cyberspace*. The letter also requested the Department's views on both the effectiveness and organizational placement of the National Cybersecurity Division.

### **Oversight Activities – Hearings and Briefings**

#### ***Cybersecurity Challenges***

On April 10, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development was briefed on the cybersecurity challenges facing the United States. The briefing was provided by Mr.

Daniel G. Wolf, Director of Information Assurance, National Security Agency. The briefing provided members with additional information on the threats to the nation posed by increases in cyber crime and espionage and overseas outsourcing of some software and hardware products.

### ***Threat to Cyber Infrastructure***

On June 4, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development received a classified briefing from representatives of the Director of Central Intelligence, the National Intelligence Council, and the Federal Bureau of Investigation on the threat to U.S. cyber infrastructure.

### ***Cybersecurity Overview***

On June 25, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development held an oversight hearing entitled, “Overview of the Cyber Problem: A Nation Dependent and Dealing with Risk.” Testimony was received from Bruce Schneier, Founder and Chief Technical Officer, Counterpane Internet Security, Inc.; Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University; and Alan Paller, Director of Research, SANS Institute. This hearing focused on the commercial information infrastructure from technical, think-tank, and academic perspectives.

### ***Industry Perspective on Cybersecurity***

On July 15, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development held an oversight hearing entitled, “Industry Speaks on Cybersecurity.” Testimony was received from: Mr. Phil Reitinger, Senior Security Strategist, Microsoft Corporation; Mr. Whitfield Diffie, Vice President and Chief Security Officer, Sun Microsystems, Inc.; Dr. James Craig Lowery, Ph.D., Chief Security Officer, Dell Computer Corporation; Mr. Jay Adelson, Chief Technology Officer and Founder, Equinix, Inc.; Mr. Frank Ianna, President, Network Services, AT&T Corporation; and Ms. Tatiana Gau, Chief Trust Officer and Senior Vice President, America On-Line (AOL) Core Services, AOL Time Warner. Each witness represented a major association or part of the cyber community. From service providers to hardware and software manufacturers, all agreed that there was room for improvement and coordination in cybersecurity.

### ***Cybersecurity Research Needs***

On July 22, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development held a hearing entitled, “Cybersecurity—Getting It Right.” Testimony was received from: Daniel G. Wolf, Director of Information Assurance, National Security Agency; Dr. Shankar Sastry, Ph.D., Chairman and Professor of Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, California; and Dr. Steven M. Bellovin, Ph.D., Technology Leader, Network Services Research Laboratory, AT&T Laboratory Research. These witnesses stressed the importance of continuing research in cybersecurity and noted how rapidly the technology in this area is moving ahead along with the challenges to keep pace.

### ***Review of Electricity Power Grid Outage***

On September 4, 2003, and September 17, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security held a Joint Hearing entitled, “Implications of Power Blackouts for the Nation’s Cybersecurity and Critical Infrastructure Protection: The Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness.” Testimony was received on September 4, 2003, from the following witnesses: the

Honorable Cofer Black, Coordinator for Counterterrorism, Department of State; Mr. Larry A. Mefford, Executive Assistant Director, FBI Counterterrorism; Mr. Paul H. Gilbert, Former Chair, Panel on Energy Facilities, Cities, and Fixed Infrastructure, National Research Council; Dr. Peter Orzag, Ph.D., Senior Fellow, the Brookings Institution; Mr. John McCarthy, Executive Director, Critical Infrastructure Protection Project, George Mason University; Mr. Karl Rauscher, Founder and President, Wireless Emergency Response Team; and Mr. Kenneth Watson, President and Chairman, Partnership for Critical Infrastructure Security. Testimony was received on September 17, 2003, from the following witnesses: Mr. Robert Liscouski, Assistant Secretary, Infrastructure Protection Directorate, Department of Homeland Security; Ms. Denise Swink, Acting Director, Office of Energy Assurance, Department of Energy; Col. Michael McDaniel, Assistant Adjutant General, Homeland Security, State of Michigan; and Mr. Robert F. Dacey, Director, Information Security Issues, General Accounting Office.

### ***Status of Department of Homeland Security Efforts in Cyberspace***

On Tuesday, September 16, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development held a hearing entitled, “The Invisible Battleground: What Is the Department of Homeland Security Doing to Make America’s Cyberspace More Secure?”. Testimony was received from Mr. Robert Liscouski, Assistant Secretary for Infrastructure Protection, Department of Homeland Security. Assistant Secretary Liscouski outlined several DHS initiatives.

### ***Private Sector Interaction with DHS - Financial and Telecommunications Sectors***

On Tuesday, March 23, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security held a joint briefing entitled, “Private Sector Operations and Interaction with DHS—Financial and Telecommunications Sectors.” Remarks were presented by Ms. Suzanne Gorman, Chair, Information Sharing and Analysis Center (ISAC) Council and Chair of the Financial Services Information Sharing and Analysis Center; Mr. Byron T. Yancey, Jr., Executive Director, Financial Services ISAC; Mr. William (Bill) J. Marlow, Board Advisor, Financial Services ISAC; Mr. Ernestine (Ernie) B. Gormsen, Industry Chair, Telecommunications ISAC; and Mr. Harry Underhill, Industry Vice Chair, Telecommunications ISAC. The closed briefing provided information on how these two infrastructure organizations—the financial and telecommunications sectors—work to secure their infrastructure and how they work with the Department of Homeland Security to share information that will help protect U.S. critical infrastructures.

### ***Private Sector Interaction with DHS - Energy, Electric, and Chemical Sectors***

On Monday, March 29, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security continued their joint briefing on Private Sector Interaction with the Department of Homeland Security. This briefing was entitled, “Private Sector Operations and Interaction with DHS—Energy, Electric, and Chemical Sectors.” Representatives from the three Information Sharing and Analysis Center (ISAC) sector leads, as well as a representative of the National Petrochemical Refiners Association, described how their sectors were addressing security concerns and how they engage with federal and state governments in this area. Briefers included Ms. Lynn Costantini and Mr. Lou Leffler from the North American Electric Reliability Council; Mr. Steven Bandy, Mr. John Williams, and Mr. William Koch representing the National Petrochemical Refiners Association; and Mr. Martin Durbin, Mr. James Conrad, and Ms. Nancy Wilson from the American Chemistry Council.

### ***Department of Homeland Security - Cybersecurity and Enterprise Architecture Budget for Fiscal Year 2005***

On Tuesday, March 30, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development held a hearing entitled, "Homeland Cybersecurity and DHS Enterprise Architecture Budget Hearing for Fiscal Year 2005." Testimony was received from Mr. Robert Liscouski, Assistant Secretary for Infrastructure Protection, Department of Homeland Security; and Mr. Steven Cooper, Chief Information Officer, Department of Homeland Security. Each witness briefly outlined the Administration's budget plan for the year.

### ***Critical Infrastructure Information Sharing with the Department of Homeland Security***

On Wednesday, April 21, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security held a joint hearing entitled, "The DHS Infrastructure Protection Division: Public-Private Partnerships to Secure Critical Infrastructures." Testimony was received from: Mr. Robert Liscouski, Assistant Secretary of Homeland Security for Infrastructure Protection, Department of Homeland Security; Mr. George Newstrom, Secretary of Technology/Chief Information Officer, Commonwealth of Virginia; Mr. Robert Dacey, General Accounting Office; the Honorable Dave McCurdy, Executive Director, Internet Security Alliance; and Ms. Diane VanDe Hei, Vice Chair, Information Sharing and Analysis Center (ISAC) Council. (Ms. VanDe Hei is also the Executive Director for the Association of Metropolitan Water Agencies). Industry groups were generally supportive of DHS but acknowledged that more work is needed in these areas.

### ***Cyber Threat to Critical Infrastructure***

On July 14, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development received a closed briefing from representatives of the Department of Homeland Security Information Analysis and Infrastructure Protection Directorate and the U.S. Secret Service on the impact of cyber attacks on the critical infrastructure, particularly those that could negatively impact the national economy.

### **Legislative Activities**

During the 108<sup>th</sup> Congress, the Subcommittee heard from private sector critical information infrastructure owners and operators as well as government and academic professionals who shared their perspectives on their experiences in working with the Department of Homeland Security. The Subcommittee also actively sought feedback from cybersecurity stakeholders on ways to improve cybersecurity for the nation. As a result of input from a variety of experts, the Subcommittee offered legislation to create an Assistant Secretary for Cybersecurity within DHS, to define cybersecurity, and to enhance cybersecurity research and development.

These provisions were initially contained in H.R. 4285, "Department of Homeland Security Authorization Act for Fiscal Year 2005." Subsequently the Chairman and Ranking Member of the Subcommittee jointly introduced H.R. 5068 and H.R. 5069, which contained the same cybersecurity elements contained in the original authorization bill. Later, the Subcommittee worked with other Committees to include a section in the "9/11 Recommendations Implementation Act" to create an Assistant Secretary for Cybersecurity within DHS.

## Legislative Chronology

**H.R. 4852** was introduced July 19, 2004, as the “Department of Homeland Security Authorization Act for Fiscal Year 2005.”

- Title II – Cybersecurity.
- Title III – Science and Technology, Section 307, “Cybersecurity training programs and equipment.”

**H.R. 5068** was introduced September 13, 2004, as the “Department of Homeland Security Cybersecurity Enhancement Act of 2004.”

**H.R. 5069** was introduced September 13, 2004, as the “Department of Homeland Security Science and Technology Enhancement Act of 2004.”

- Section 8 – Cybersecurity training programs and equipment.

**S2845** as passed by the House, October 16, 2004, as the “National Intelligence Reform Act of 2004.”

- Sec. 5028. Assistant Secretary for Cybersecurity.

## Explanation of Proposed Legislation

### **H.R. 5068: Elevation of the cybersecurity mission within DHS to an Assistant Secretary for Cybersecurity within Information Analysis and Infrastructure Protection (IAIP) Directorate**

It is essential for DHS to establish a “cybersecurity” framework to support the nation’s economy, security, and way of life. As cyber threats to the nation grow, it is clear that the United States should further develop and maintain a comprehensive “cybersecurity” strategy.

Cybersecurity remains a cross-cutting thread across every other infrastructure; it is the underlying foundation for the operation of every business and government function. Unlike physical vulnerabilities, cybersecurity vulnerabilities and threats can change in seconds, and protective measures can become obsolete just as quickly. As the February 2003 President’s *National Strategy to Secure Cyberspace* (National Strategy) states:

“A network of networks directly supports the operation of all sectors of our economy—energy (electric power, oil, gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, defense industrial base, food, agriculture, and postal and shipping....They also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars.”

To address these concerns, the Subcommittee drafted legislation to elevate the National Cybersecurity mission within DHS’ Directorate for Information Analysis and Infrastructure Protection (IAIP). It also establishes an Assistant Secretary for Cybersecurity (Assistant Secretary), who will have primary authority for all DHS IAIP cybersecurity-related critical infrastructure programs, including policy formulation and program management.

The Assistant Secretary's responsibilities would, among other things, include the establishment and management of a national cybersecurity response system, a national cybersecurity threat and vulnerability reduction program, a national cybersecurity awareness and training program, a government cybersecurity program, and a national security and international cybersecurity cooperation program. These responsibilities are based primarily on the President's *National Strategy to Secure Cyberspace*.

The Subcommittee believes that specifically authorizing the cybersecurity mission and elevating it within IAIP's organizational structure would help resolve cybersecurity integration difficulties at DHS and enable the Assistant Secretary to influence the cross-cutting functions of cybersecurity throughout the Department. These changes also integrate vulnerability and threat analysis into one organization so that efficiencies could be gained in correlating data and coordinating with myriad organizations dealing with cybersecurity.

Under this proposed legislation, the Assistant Secretary would have enhanced opportunities to coordinate across critical infrastructure elements, with other DHS organizations (including the Chief Information Officer and the Under Secretary for Science and Technology), and with other government organizations. The Assistant Secretary would be in a position to provide higher level input into national level policy decisions in this area. And elevating the position to the Assistant Secretary level would enable DHS to provide a single, visible point of contact within the Federal government, instead of multiple overlapping points of contact and improve the interface for the private sector, which owns and operates the majority of the nation's cyber infrastructure.

The elevation of the cybersecurity mission will not split cyber and physical functions but rather will place authority for both under equal footing within the IAIP Directorate. Therefore, missions and leadership will remain within the IAIP Directorate and existing programs should not be diverted from their current courses. Elevating the cyber element of DHS recognizes that the "first responders" of cybersecurity incidents are generally not the same as in the physical world. Budget and programmatic decisions, personnel actions, and overall strategic direction within DHS should not be impacted, except to provide more focus and authority for the vital cybersecurity mission. This elevation is also critical to the success of DHS's partnership with the private sector.

In providing the general authority of the Assistant Secretary for Cybersecurity, it is the Subcommittee's intent that all cybersecurity-related critical infrastructure protection programs operated by the U.S. Secret Service and Immigration and Customs Enforcement (ICE) Cyber Crimes Center remain under the primary management and control of those respective organizations. The Secret Service retains concurrent jurisdiction over computer-based crimes under 18 U.S.C. §1030, and the ICE Cyber Crimes Center retains its investigative jurisdiction under pre-existing law.

The Subcommittee also encourages the Assistant Secretary to request that state homeland security directors develop cybersecurity strategies and focus on continuity of operations and disaster recovery strategies for the critical information and communications technology systems and technology assets that support emergency services at the state and local levels. The Assistant Secretary should encourage the states to consider risk and needs assessments that take into account the all-hazard threats to relevant cybersecurity systems, including coordination with state homeland

security directors, state chief information officers, and the DHS Office for Domestic Preparedness to develop and promulgate a consistent methodology for developing such strategies.

### **Assistant Secretary includes authority over the National Communications System**

Organizationally, DHS treats telecommunications separately from information technology, thus dividing the mission and operations. Given the rapid convergence of communications technology, however, DHS needs to have one comprehensive and coherent mission element. For the short term, the legislation allows for the highly effective telecommunications mission to remain intact within the National Communications System, so that a gradual transition to bring the cyber and telecommunications together can be achieved, while also ensuring strategic policy and program direction is established under one leader.

Executive Order 12472 created the National Communications System in 1984 when telephone systems were vital to the communications for national security and emergency preparedness. But, with the convergence of telephones and data over the Internet and other communications mediums, DHS needs to keep pace with technological evolution. Today, continuity of operations depends heavily on the functioning of multiple communications mediums. This fact is best exemplified by two recent events: the terrorist attacks of September 11, 2001, when cellular telephones were the primary communications medium, and the August 2003 electrical power blackout, when personal digital assistants (e.g., Blackberry units) were the primary communications medium. These two events demonstrated that the nation cannot depend on only one method of communication in emergency situations. Similarly, DHS must evolve to meet national needs for multiple and, when warranted, secure communications mediums for emergency communications in terrorist events.

### **Authoritative definition for “cybersecurity” to be used by DHS**

There is no government-wide definition of cybersecurity. Therefore the Subcommittee sought input from a variety of sources to develop standard terminology for use by DHS. From a security standpoint, this definition recognizes the convergence of emerging technologies, particularly between information technology and telecommunications. Technology is increasingly allowing individuals to transmit voice communications via the Internet and electronic data through wire lines. The Subcommittee believes that there must be a comprehensive and consistent approach to securing these two types of networks, as well as future types of networks that might emerge. Given the rapid convergence of technology, the Subcommittee strongly urges the Department of Homeland Security (DHS) to use this definition to guide its mission and policy functions.

The term “cybersecurity” is defined in the legislation as “the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.” This definition references terms from federal statutes used by the U.S. Justice Department to prosecute electronic crimes (18 U.S.C. 1030 and 18 U.S.C. 2510):

- The term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

- The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
- The term "electronic communications system" means any wire, radio, electromagnetic, photo-optical or photo-electronic facility for the transmission of wire or electronic communications, and any computer facility or related electronic equipment for the electronic storage of such communications;
- The term "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;
- The term "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce; and
- The term "electronic communications" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce.

### **Additional Report Language**

#### **H.R. 5068: Setting the Example**

The Subcommittee encourages DHS to establish and maintain a leadership role in cybersecurity by setting an example for other government agencies, the private sector, and academia. Although a September 2004 DHS Inspector General (IG) Report indicated that DHS was making progress in complying with existing Federal Information Security Management Act (FISMA) (Public Law 107-347) requirements, there is much work to be done. For example, the IG found that DHS organization components have not yet fully aligned their respective security programs with DHS's overall policies, procedures, and practices, and most elements lack an accurate and complete system inventory.

In addition to measures recommended by the IG, DHS may wish to consider an independent assessment of its internal cybersecurity posture and take appropriate actions to correct problems found in such assessment. Securing multiple layers of information exchange, including critical data and application layers, should also be a high priority for DHS to accomplish in the near term. By expanding the use of content level threat protection and content level trust management beyond transport and storage security, DHS should be able to increase the overall security of data at all stages of the information lifecycle. DHS should also evaluate the value of diversity within its enterprise architecture.

The Subcommittee remains concerned that DHS is not taking all the steps necessary to fully protect classified material within its information systems. Indeed, DHS must recognize national security

systems (classified systems) and the special measures that must be taken to secure these systems. National security systems within DHS should adhere to security policy established by the entities responsible for those systems. DHS is entrusted to protect some of the nation's most sensitive information, including intelligence, critical infrastructure, and private sector data. It is imperative, therefore, that DHS take strong measures to prevent unauthorized access to this information.

Computer network security is an essential element in protecting sensitive information. In addition to authenticating network users, it is now possible to authenticate devices that access computer networks, significantly enhancing security. The Subcommittee, therefore, encourages DHS to examine device authentication and other alternatives for security and cost-effectiveness and to incorporate innovative security techniques in its computers.

### **H.R. 5068: Best Practices**

Another area of importance is the promotion and distribution of cybersecurity best practices. The responsibilities of the Assistant Secretary include promoting voluntary cybersecurity best practices, standards, and benchmarks that are responsive to rapid technology changes and to the security needs of critical infrastructure. As such, the Subcommittee encourages DHS to work with the private sector and academia to determine the best mechanisms for developing a distribution system for cybersecurity best practices and programs. To assist in this effort, DHS may want to invest in research centers at universities. Such centers also could work with the federal government, the private sector, and non-profit institutions to provide economic and policy analysis of risk management and loss assessments caused by cyber incidents, and to develop cybersecurity seals of approval.

### **H.R. 5069: Funding for community college cybersecurity education and training**

Section 8 allows DHS to provide funds to encourage community colleges to develop cybersecurity professional development programs, core curriculum, and virtual laboratories that provide hands-on training for cybersecurity specialists. This section uses the existing National Science Foundation competitive process for grant distribution, expanding its already successful university programs to the community college level.

In order to create an educated workforce, the United States must have in place educational programs to provide future information technology professionals with specialized skills in information security. The increasing threats to and vulnerabilities of the nation's computer systems have increased the need for such an educated and skilled workforce. System administrators and cybersecurity professionals are the first line of defense for cybersecurity.

Today, over 1,200 community college campuses are located within commuting distance of more than 90% of the U.S. population. A number of these campuses also offer distance and Internet education opportunities for even more students. To meet the increasing need for cybersecurity professionals, funds should be identified for developing programs and regional laboratories at universities, colleges, and community colleges to educate information technology professionals about cybersecurity. These academic institutions are the ones that serve their regional workforces and can quickly develop relevant programs and curricula based on their ties with local businesses. For example, the student bodies of community colleges include first-generation college students and

workers seeking further education or training for new careers. As such, these institutions are also in the best position to develop a culture of security within their communities to ensure that all citizens are part of the plan to defend our homeland.

### **Support for Cyber Legislation**

The Subcommittee worked closely with state, industry, and academic associations on legislative and policy matters. The associations listed below provided letters to the Subcommittee endorsing various aspects of the cyber legislation:

- Business Software Alliance (BSA) – represents commercial software industries in more than 60 countries, promoting a safe and legal digital world, educating consumers on software management and copyright protection, cybersecurity, trade, e-commerce and other Internet-related issues.
- Computer & Communications Industry Association (CCIA) – nonprofit organization for companies and senior executives from diverse sectors of the computer and communications industry to promote competitive and fair open markets, open systems, and open networks.
- Cyber Security Industry Alliance (CSIA) – an advocacy group of leading cybersecurity software, hardware and services companies that are dedicated to the improvement of cybersecurity through public policy, education, and technology-focused initiatives.
- Financial Services Roundtable – BITS is the technology group for the Financial Services Roundtable, formed by the CEOs of over 100 of the largest bank-holding institutions in the U.S. as the strategic "brain trust" for the financial services industry in the e-commerce arena.
- Higher Education Information Technology Alliance (HEIT Alliance) – comprising higher education and library associations, the HEIT Alliance helps define and promote the higher education and library community's collective interests in federal information technology policy. Bill supporters include:
  - American Association of Community Colleges
  - American Association of State Colleges and Universities
  - American Council on Education
  - Association of American Universities
  - Association of Research Libraries
  - EDUCAUSE
  - Internet2
  - National Association of College and University Business Officers
  - National Association of Independent Colleges and Universities
  - National Association of State Universities and Land-Grant Colleges
- Information Technology Association of America (ITAA) – major trade association representing the broad spectrum of the world-leading U.S. Information Technology industries, working on such issues as e-health, e-learning, intellectual property, finance, and information security.
- Information Technology Industry Council (ITIC) – trade association representing leading U.S. providers of information technology products and services, advocating policies that advance industry leadership in technology and innovation; open access to new and emerging markets;

promotes e-commerce expansion; protects consumer choice; and enhances the global competitiveness of members.

- National Association of State Chief Information Officers (NASCIO) – represents state chief information officers and information resource executives and managers from the 50 states, six U. S. territories, and the District of Columbia.
- Software & Information Industry Association (SIIA) – principal trade association with over 600 members in the software and digital content industry, providing global services in government relations, business development, corporate education and intellectual property protection.
- TechNet – represents over 150 chief executive officers and senior partners of companies in the fields of information technology, biotechnology, venture capital, investment banking, and law; represents a bipartisan network of CEOs that promotes the growth of technology industries and the economy.

# CYBERSECURITY ROADMAP FOR THE FUTURE

---

The Subcommittee has identified six core areas where DHS and Congress should work together to improve cybersecurity for the nation. In some instances the Department may act on its own. In other areas it will be important for Congress to help, and in other cases the Department must embrace solutions and recommendations from and with private industry. These areas are:

1. **Assistant Secretary for Cybersecurity**—Creating an Assistant Secretary of Homeland Security within the Information Analysis and Infrastructure Protection Directorate to improve integration of the cybersecurity mission within the Department and coordination of cybersecurity best practices, risk assessments and warnings across all levels of government and with the private sector.
2. **Budget and Program**—Developing comprehensive and detailed program and budget information that delineates current and future plans and links expenditures to the goals of the *National Strategy to Secure Cyberspace*. Such a plan should include implementation guidance and personnel recruiting, retention, and assignment goals.
3. **Private Sector Outreach and Information Sharing**—Updating the plan for outreach and coordination and improved information sharing with the private sector. Such a plan should consider the varying needs of different segments of the private sector: owners and operators of the critical information infrastructure; companies that provide products and services that help secure the critical information infrastructure; small and large business users; and individual citizens. The plan should also include developing innovative mechanisms for information sharing on cybersecurity threats, vulnerabilities, best practices, emergency response, and solutions.
4. **Risk Assessment and Remediation**—Improving performance on cyber risk assessments and remediation activities, including a plan for Internet-related recovery in the event of a disaster or coordinated attack, and working closely with the “cyber first responders” across international, federal, state, local, and private sectors.
5. **NCSD/NCS**—Identifying specific initiatives for National Cybersecurity Division (NCSD) and the National Communications System (NCS) to work together because of the increasing similarities of their missions and the convergence of voice and data technology.
6. **R&D and Education**—Supporting research and development (R&D) and educational activities to improve cybersecurity products and services that are user friendly and keep pace with risk and technology.

## **Department of Homeland Security Activity for 2005**

### **Assistant Secretary for Cybersecurity**

To date, the cybersecurity mission has not received the proper level of management or operational attention within the Department. Previous public statements by the outgoing Secretary of Homeland Security indicate that he may support creating an Assistant Secretary for Cybersecurity to act as a focal point for the private sector and other elements of government. The Secretary may establish this position on his own and is encouraged to do so.

## **Budget and Program**

Almost two years after its release, the *National Strategy to Secure Cyberspace* has not been fully implemented by the Department of Homeland Security. DHS is encouraged to provide greater focus and attention in this area.

In an April 2004 letter, the Subcommittee requested that the Department provide information describing how it was implementing the *National Strategy to Secure Cyberspace*. The Department's response showed that more work is needed on a number of issues, such as personnel management, hiring, salaries, retention, and skill set development.

It has also been difficult for the Subcommittee to effectively evaluate the Department's progress on cybersecurity because the information provided has not adequately addressed the roles and responsibilities of the various DHS offices and divisions that may have cybersecurity responsibilities. Also, detailed information regarding milestones and substantive achievements has not been fully shared, making Subcommittee assessments and progress difficult to measure.

The Subcommittee believes that creating a more detailed program structure, as outlined by the House Homeland Security Appropriations Subcommittee, which specifically links budgets to mission priorities, is an important step that would aid in clearly delineating programs from each other, assigning projects to different programs, and clarifying roles and responsibilities within the Department. Additionally, such documentation might aid in Congressional oversight and accountability activities.

Providing program, implementation, and spend rate plans (to include processes, procedures, and guidelines) will aid integration of the cybersecurity mission across the Department. Planning documentation is also important to define how DHS will interact with international, federal, state, local, and private stakeholders of the national information infrastructure.

The Subcommittee additionally encourages DHS to take a more active role in incorporating cyber elements in other Department-wide activities. For example, emergency management planning (National Response Plan), alerts and warnings (Homeland Security Advisory System), Office of Domestic Preparedness-sponsored exercises, and research and development should incorporate cybersecurity as a mission element.

## **Private Sector Outreach and Information Sharing**

Because the Department of Homeland Security has been given the national charter for securing the critical infrastructure, its relationship and interaction with the private sector, which owns a majority of America's critical infrastructures, is vital for success. Following the conclusion of the December 2003 National Cybersecurity Summit, a public-private partnership was established to develop shared strategies and programs to better secure and enhance America's critical information infrastructure. The partnership established the following five task forces, comprised of cybersecurity experts from industry, academia and government:

- Awareness for Home Users and Small Businesses
- Cybersecurity Early Warning

- Corporate Governance
- Security Across the Software Development Life Cycle
- Technical Standards and Common Criteria

In an April 2004 letter to the Department, the Subcommittee “strongly supported the need for closer public-private partnerships, particularly in cybersecurity where much of the protection and response depends on the owners of those information infrastructures. The Department recently announced that they have created a special position within the US-CERT for public outreach. While this may be a positive step, the Subcommittee also encourages the Department to consider adopting recommendations [from the Cybersecurity Task Forces] as the Department implements the President’s *National Strategy to Secure Cyberspace*.”

Today it remains unclear what recommendations have been acted upon by the Department of Homeland Security almost a year after the Cyber Summit. Recognizing the importance to maintain momentum, industry co-sponsors from the earlier Summit decided to self-organize under the auspices of the National Cybersecurity Partnership (NCSP), holding their first meeting in August 2004. They are defining priorities and next steps for action, to include creation of a matrix of existing private sector efforts on cybersecurity and mapping those efforts to the *National Strategy to Secure Cyberspace*. This effort would prioritize existing efforts and conduct a gap analysis to determine what issues should be addressed. This is one type of public-private partnership that is needed, and the Subcommittee encourages the NCSP to continue its cybersecurity efforts.

In August 2003, the Subcommittee requested the Government Accountability Office (GAO) to investigate and report on information sharing efforts between the Department of Homeland Security and critical infrastructure elements, believing that “it is important that these responsibilities be appropriately integrated in transitioning CIP [Critical Infrastructure Protection] functions and entities to the Department.” GAO identified major challenges related to these responsibilities, including the need to (1) develop a comprehensive and coordinated national plan for securing the key resources and critical infrastructures of the United States; (2) enhance information sharing on threats and vulnerabilities both within the government and between the federal government and the private sector and state and local governments; (3) provide more robust analysis and warning capabilities to identify threats and provide timely warnings; and (4) provide incentives to encourage non-federal entities to increase their CIP efforts.”

In April 2004, GAO testified during a Subcommittee hearing entitled, “The DHS Infrastructure Protection Division: Public-Private Partnerships to Secure Critical Infrastructures,” which reviewed information sharing within the private sector Information Sharing and Analysis Centers (ISAC). GAO also produced a July 2004 report on Critical Infrastructure Protection entitled, “Improving Information Sharing with Infrastructure Sectors,” providing specific recommendations to help improve the effectiveness of DHS’s information sharing efforts with the private sector, including the following:

- “Proceed with and establish milestones for the development of an information-sharing plan that includes (1) a clear description of the roles and responsibilities of DHS, the ISACs, the sector coordinators, and the sector-specific agencies and (2) actions designed to address information-sharing challenges. Efforts to develop this plan should include soliciting

feedback from the ISACs, sector coordinators, and sector-specific agencies to help ensure that challenges identified by the ISACs and the ISAC Council are appropriately considered in the final plan.

- Considering the roles, responsibilities, and actions established in the information-sharing plan, develop appropriate DHS policies and procedures for interacting with ISACs, sector coordinators, and sector-specific agencies and for coordination and information sharing within the IAIP Directorate (such as the National Cybersecurity Division and Infrastructure Coordination Division) and with other DHS components that may interact with the ISACs, including the Transportation Security Administration (TSA).”

Whether it is vulnerability assessments, threat warning, best practices, or emergency response, information sharing with the private sector is critical to securing the United States from terrorist attacks. This begins with a trusted partnership that must be based on agreed-upon roles and responsibilities, procedures and processes, and actions. For example, a mechanism could be established for best practices that can be applied across critical infrastructure sectors. An ongoing process for sharing information related to making secure products or managing secure information systems based on new technologies and accepted, consensus-based standards would be helpful. The Subcommittee encourages the Department to consider GAO’s recommendations in this area.

### **Risk Assessment and Remediation**

Another priority for the Department of Homeland Security should be to improve its ability to correlate cyber vulnerabilities and threats in a given environment, produce a dynamic risk assessment, and plan for how to move forward with securing critical portions of the information infrastructure. The private sector, state and local governments, the Department of Homeland Security, the intelligence community, and law enforcement must also work together more productively and more rapidly. There is still much to be done in this area, both domestically and internationally, as illegal cyber activities may soon become one of the principal long-term threats to the homeland.

No national level plan exists for Internet-related recovery. The National Communications System has responsibility for telecommunications for national security and emergency preparedness, but NCSA asserts responsibility for other cyber aspects. The Office for Domestic Preparedness conducts national planning. Closer coordination is needed for cyber response and recovery, and DHS should consider developing a remediation and recovery plan in the event of a major attack or outage of critical information infrastructures. In addition to physical aspects, the National Response Plan and the Homeland Security Advisory System should also incorporate cyber elements. Incident planning should include other stakeholders and “cyber first responders” at state, local, and private levels. For example, state and local cybersecurity officials informed the subcommittee that the NCSA's inclusion of state and local sectors under more generalized private-sector coordination efforts has resulted in awkward and inadequate attention being paid to the cyber portion of the nation's governmental information and communications technology infrastructure.

### **NCSA/NCS**

Organizationally DHS treats telecommunications separately from information technology, thus dividing the mission and operations. Given the rapid convergence of communications technology,

however, DHS should have one comprehensive and coherent mission element. Because of the best practices and other established mechanisms NCS can bring, DHS should seriously consider development of a plan to gradually integrate the cyber and telecommunications mission, while also ensuring strategic policy and program direction is established under one leader.

## **R&D and Education**

Research and Development activities will be imperative for the United States to retain its lead in cybersecurity. NCSD should continue to coordinate with the Undersecretary for Science and Technology to define needs and requirements to include prevention, detection, and response capabilities. Additionally, NCSD should help set requirements for the type of training, education, and skills that will be needed in the future to better protect the information and related infrastructures.

## **Congressional Activity for the 109<sup>th</sup> Congress**

This year, the Subcommittee worked toward establishing a foundation for and a constituency within Congress for elevating the importance of cybersecurity issues for the nation. Providing assistance for and oversight of cybersecurity issues was an extremely high priority for the Subcommittee. It should now be possible for the Subcommittee to build upon these initial efforts.

### **Legislation**

The top priority for the Subcommittee in the 109<sup>th</sup> Congress should be passing legislation to create a DHS Assistant Secretary for Cybersecurity. This will be the first step in improving management and resources matters. Since cybersecurity is becoming more important for the nation, the Subcommittee should also consider enacting a standard definition for cybersecurity and expand education to the community college level and beyond.

Other elements of H.R.5068 should also be considered for legislative action, particularly those portions that deal with technical, privacy, and policy concerns across government and the private sector. This is not just a national issue because cyberspace has no borders, and our international partnerships are vital for implementing many of the actions in the *National Strategy to Secure Cyberspace*.

The Subcommittee does not recommend cybersecurity industry or standards regulation at this time. Industry may do more than government could regulate. Because the threat and the technology move so quickly in this area, the nation cannot afford for industry to be hamstrung by outdated laws and regulations that could impose temporal minimum requirements. Instead, the Subcommittee may want to research, in collaboration with other Committees, the possibility of insurance and other incentives that would promote innovation to improve cybersecurity.

## **Potential Oversight for 109<sup>th</sup> Congress**

### **Budget and Program**

Continued review of Department-wide cybersecurity budget programs is necessary, and DHS should be required to adopt budgetary documentation methods used by more mature federal agencies, such as the Department of Defense. Because current DHS programs do not easily match to the *National Strategy to Secure Cyberspace*, the FY06 program should either be structured around the five strategy priorities or revamped to reflect priorities deemed appropriate for their mission.

Continued oversight will be required on the key functions that DHS must establish to become effective (i.e., functional definition, structure, personnel, resource, and programmatic planning). Success could be measured by the Department's ability to provide its workforce—and Congress—the core planning documentation that the Department needs in order to function and grow. From these plans, progress could be measured in terms of results and outcomes, such as the following:

- Request DHS identify programs and personnel managed by each organizational section and identify what priorities are the responsibilities of each section. With this approach, the organizational chart could provide a baseline for oversight.
- Review budget, contractual, and acquisition processes within NCS and NCS to ensure conformance with current law and Departmental direction and policies.
- Review personnel hiring and delineation of duties within the NCS and NCS to ensure balance between government, contractor, and detailed assignments.
- Review cybersecurity interaction within the Department to ensure funding, projects, and personnel skill sets are adequately coordinated. This should include interaction between NCS, NCS, ICE, USSS, and CIO organizations.
- Review progress of public-private partnership and information sharing initiatives.

### **National Strategy**

The Subcommittee should consider reviewing progress and planning for each of the mission areas outlined in the *National Strategy to Secure Cyberspace* and determine if these areas are still relevant in today's environment and how well DHS is meeting these goals, including the following:

- A National Cyberspace Security Response System
- A National Cyberspace Security Threat and Vulnerability Reduction Program
- A National Cyberspace Security Awareness and Training Program
- Securing Governments' Cyberspace
- National Security and International Cyberspace Security Cooperation

### **Cybersecurity Cost Assessment**

The Subcommittee should conduct a series of hearings to investigate the costs associated with cybersecurity, to include preventive and recovery costs. Much has already been written on prevention, but there is no national program or methodology for measuring the cost of cyber

attacks. Precise national measurement is crucial because losses—whether direct or indirect—affect national statements on production and productivity. These data in turn form the basis for executive policy decisions, business regulations, and new legislation. The lack of a methodology or measurement program also prohibits knowing how well national efforts to improve cybersecurity are working.

### **Market-Driven Solutions**

The Subcommittee may want to review measures to incentivize the market towards stronger cybersecurity. Some options that have been mentioned during Subcommittee testimony and briefings include using the federal government as the “reinsurer of last resort” by providing a financial backstop in cases of massive cyber disaster; possibly expanding the Terrorism Risk Insurance Act to include cyber; or considering “safe harbor” or “tax incentive” legislation that would reward best practices for securing the critical infrastructure. Both Congress and the Department of Homeland Security could consider incentives and recognition programs to encourage the private sector to develop more secure cyber products.

### **Updated Tools of the Trade**

The Subcommittee should consider working with other House Committees including the House Armed Services Committee, the Judiciary Committee, and the House Permanent Select Committee on Intelligence to review current statutes and determine if each Agency and Department has the proper authority and tools to work together to trace, track, and act against cyber criminals and cyber attackers. This effort could include improved ways to incorporate the private sector that own and operate most of the critical information infrastructure. Private industry is often considered the first line of cyber defense and often serves as cyber first responders. The Department of Homeland Security could help by bringing together elements of the public and private sectors to analyze information and assist in tracking cyber attacks.

### **Conclusion**

Today the government is working to make the nation safer than it was in the days preceding and immediately following the terrorist attacks on our homeland in September 2001. The men and women of the Department of Homeland Security, other parts of government, state and local first responders, businesses, and individual citizens have worked to make it so. Whether it is protecting borders, bolstering transportation security, or improving first responder capabilities, the cyber infrastructure often provides the basis for successful operations and communications.

DHS has a unique opportunity and mandate to bring different government and non-government entities together to improve cybersecurity. The nation still faces homeland security challenges on many fronts. But with challenges come opportunities for improved cooperation, advances in technology, and more efficient and effective government. We are hopeful that with a renewed spirit among all Americans to do our part in homeland security, including cybersecurity, we will continue to become safer in the days and years ahead.