Priority III: A National Cyberspace Security Awareness and Training Program

Everyone who relies on part of cyberspace is encouraged to help secure the part of cyberspace that they can influence or control.

To do that, users need to know the simple things that they can do to help to prevent intrusions, cyber attacks, or other security breaches. All users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace.

In addition to the vulnerabilities in existing information technology systems, there are at least two other major barriers to users and managers acting to improve cybersecurity: (1) a lack of familiarity, knowledge, and understanding of the issues; and (2) an inability to find sufficient numbers of adequately trained and/or appropriately certified personnel to create and manage secure systems.

Among the components of this priority are the following:

- Promote a comprehensive national awareness program to empower all Americans—businesses, the general workforce, and the general population—to secure their own parts of cyberspace;
- Foster adequate training and education programs to support the Nation's cybersecurity needs;

- Increase the efficiency of existing federal cybersecurity training programs; and
- Promote private sector support for well-coordinated, widely recognized professional cybersecurity certification.

Key to any successful national effort to enhance cybersecurity must be a national effort to raise awareness (of users and managers at all levels) and maintain an adequate pool of well trained and certified IT security specialists. The federal government cannot by itself create or manage all aspects of such an effort. It can only do so in partnership with industry, other governments, and nongovernmental actors.

Many federal agencies must play a part in this effort, which will be led and coordinated by DHS. The components of this program will include the following federal programs (both existing programs and initiatives which will be considered as part of the budget decision making process) and activities, which we recommend to our partners.

A. AWARENESS

1. Promote a Comprehensive National Awareness Program to Empower All Americans—Businesses, the General Workforce, and the General Population—to Secure their Own Parts of Cyberspace

In many cases solutions to cybersecurity issues exist, but the people who need them do not know they exist or do not know how or where to find them. In other cases people may not even be aware of the need to make a network element secure. A small business, for example, may not realize that the configuration of its web server uses a default password that allows anyone to gain control of the system. Education and outreach play an important role in making users and operators of cyberspace sensitive to security needs. These activities are an important part of the solution for almost all of the issues discussed in the *National Strategy to Secure Cyberspace*, from securing digital control systems in industry, to securing broadband Internet access at home.

DHS, working in coordination with appropriate federal, state, and local entities and private sector organizations, will facilitate a comprehensive awareness campaign including audience-specific awareness materials, expansion of the StaySafeOnline campaign, and development of awards programs for those in industry making significant contributions to security. (A/R 3-1)

Increasing awareness and education prepares private sectors, organizations, and individuals to secure their parts of cyberspace. Actions taken by one entity on a network can immediately and substantially affect one or many others. Because the insecurity of one participant in cyberspace can have a major impact on the others, the actions they take to secure their own networks contribute to the security of the whole. For example, a few subverted servers recently enabled an attack on some of the Internet Domain Name System root servers and threatened to disrupt service for many users. Through improved awareness the Nation can stimulate actions to secure cyberspace by creating an understanding at all audience levels of both cybersecurity issues and solutions. DHS will lead an effort to increase cybersecurity awareness for key audiences:

a. Home Users and Small Business

Home users and small business are not part of the critical infrastructures. However, their systems are being increasingly subverted by malicious actors to attack critical systems. Therefore, increasing the awareness about cybersecurity among these users contributes to greater infrastructure security. Home users and small business owners of cyber systems often start with the greatest knowledge gap about cybersecurity.

DHS, in coordination with other agencies and private organizations, will work to educate the

general public of home users, students, children, and small businesses on basic cyberspace safety and security issues. As part of these efforts, DHS will partner with the Department of Education and state and local governments to elevate the exposure of cybersecurity issues in primary and secondary schools. In addition, the Federal Trade Commission will continue to provide information on cybersecurity for consumers and small businesses through http://www.ftc.gov/infosecurity.

DHS, in coordination with the Department of Education, will encourage and support, where appropriate subject to budget considerations, state, local, and private organizations in the development of programs and guidelines for primary and secondary school students in cybersecurity. (A/R 3-2)

In recent years, with the spread of "always on" connections for systems, such as cable modems, digital subscriber lines (DSL), and wireless and satellite systems, the security of home user and small business systems has become more important not only to the users themselves, but to others to which they are connected through the Internet. For example, these connections generally mean that larger amounts of data can be sent and done so in a continuous stream. These two factors can be exploited and used to attack other systems, possibly even resulting in nationally significant damage. The Internet service providers, antivirus software companies, and operating system/application software developers that provide services or products to home users and small businesses can help raise their awareness of cybersecurity issues.

Home users and small businesses can help the Nation secure cyberspace by securing their own connections to it. Installing firewall software and updating it regularly, maintaining current antivirus software, and regularly updating operating systems and major applications with security enhancements are actions that individuals and enterprise operators can take to help secure cyberspace. To facilitate such actions, DHS will create a public-private task force of private companies, organizations, and consumer users groups to identify ways that providers of information technology products and services, and other organizations can make it easier for home users and small businesses to secure their systems. (A/R 3-3)

b. Large Enterprises

The security of large enterprises is important not only to individual businesses, but to the Nation as a whole. Large enterprises own major cyber networks and computing systems that, if not secure, can be exploited for attacks on other businesses in an increasingly interconnected economy, and could, in the case of a massive attack, have major economic consequences. The cybersecurity of large enterprises can be improved through strong management to ensure that best practices and efficient technology are being employed, especially in the areas of configuration management, authentication, training, incident response, and network management. DHS will continue the work of sensitizing the owners of these networks to their vulnerabilities and what can be done to mitigate them. DHS, working with other government agencies and private sector organizations, will build upon and expand existing efforts to direct the attention of key corporate decision makers (e.g., CEOs and members of boards of directors) to the business case for securing their companies' information systems.

Decision makers can take a variety of steps to improve the security of their enterprise networks and to ensure that their networks cannot be maliciously exploited. *Large enterprises are encouraged to evaluate the security of their networks that impact the security of the Nation's critical infrastructures. Such evaluations might include: (1) conducting audits to ensure effectiveness and use of best practices; (2) developing continuity plans which consider offsite staff and equipment; and, (3) participating in industrywide information sharing and best practice dissemination. (A/R 3-4)*

(i) Insider Threats. Many cyber attacks on enterprise systems are perpetrated by trusted "insiders." Insiders are people trusted with legitimate access rights to enterprise information systems and networks. Such trusted individuals can pose a significant threat to the enterprise and beyond. The insider threat poses a key risk because it provides a potential avenue for individuals who seek to harm the Nation to gain access to systems that could support their malicious objectives. Effectively mitigating the insider threat requires policies, practices, and continued training. Three common policy areas which can reduce insider threat include: (1) access controls, (2) segregation of duties, and, (3) effective policy enforcement.

- Poor access controls enable an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage.
- Segregation of duties is important in assuring the integrity of an enterprise's information system. No one person should have complete control of any system.
- Effective enforcement of an enterprise security policy can be challenging and requires regular auditing. New automated software is beginning to emerge which can facilitate efficient enforcement of enterprise security. These programs allow the input of policy in human terms, translation to machine code, and then monitoring at the packet level of all data transactions within, and outbound from, the network. Such software can detect and stop inappropriate use of networks and cyber-based resources.

c. Institutions of Higher Education (IHEs)

Awareness plays an especially important role in increasing the cybersecurity of IHEs. As recent experience has shown, organized attackers have collectively exploited many insecure computer systems traceable to the campus networks of higher education as a platform from which to launch denial-of-service attacks and other threats to unrelated systems on the Internet. Such attacks harm not only the targeted systems, but also the owners of those systems and those who desire to use their services. IHEs are subject to exploitation for two reasons: (1) they possess vast amounts of computing power; and (2) they allow relatively open access to those resources. The computing power owned by IHEs is extensive, covering over 3,000 schools, many with research and significant central computing facilities.

The higher education community, collectively, has been actively engaged in efforts to organize its members and coordinate action to raise awareness and enhance cybersecurity on America's campuses. Most notably, through EDUCAUSE, the community has raised the issue of the Strategy's development with top leaders of higher education, including the American Council on Education and the Higher Education IT Alliance. Significantly, through this effort, top university presidents have adopted a 5-point Framework for Action that commits them to giving IT security high priority and to adopting the policies and measures necessary to realize greater system security:

(1) Make IT security a priority in higher education;

(2) Revise institutional security policy and improve the use of existing security tools;

(3) Improve security for future research and education networks;

(4) Improve collaboration between higher education, industry, and government; and

(5) Integrate work in higher education with the national effort to strengthen critical infrastructure.

Colleges and universities are encouraged to secure their cyber systems by establishing some or all of the following as appropriate: (1) one or more ISACs to deal with cyber attacks and vulnerabilities; (2) model guidelines empowering Chief Information Officers (CIOs) to address cybersecurity; (3) one or more sets of best practices for IT security; and, (4) model user awareness programs and materials. (A/R 3-5)

d. Private Sectors

DHS will work with private sectors on general awareness as well as on specific issues impacting particular sectors. Private sectors own and operate the vast majority of the Nation's cyberspace. As long time partners in the effort to secure cyberspace, many sectors have developed plans in parallel with the *National Strategy to Secure Cyberspace* to help secure their critical infrastructures. The sectors can serve a vital role in the reduction of vulnerabilities by creating sector-wide awareness of issues that affect multiple members. Members can develop and share best practices and work together toward common security solutions. For example, SCADA systems are a widespread security issue in the energy sector. Solutions are being coordinated with the Department of Energy and across the sector. The sectors also play a role in the identification of research needs. DHS will closely coordinate with private sectors on plans and initiatives to secure cyberspace.

A public-private partnership should continue work in helping to secure the Nation's cyber infrastructure through participation in, as appropriate and feasible, a technology and R&D gap analysis to provide input into the federal cybersecurity research agenda, coordination on the conduct of associated research, and the development and dissemination of best practices for cybersecurity. (A/R 3-6)

e. State and Local Governments

DHS will implement plans to focus key decision makers in state and local governments—such as governors, state legislatures, mayors, city managers, and county commissioners/boards of supervisors—to support investment in information systems security measures and adopt enforceable management policies and practices.

B. TRAINING

In addition to raising general awareness, the Nation must focus resources on training a talented and innovative pool of citizens that can specialize in securing the infrastructure. While the need for this pool has grown quickly with the expansion of the Internet and the pervasiveness of computers, networks, and other cyber devices, the investment in training has not kept pace. Universities are turning out fewer engineering graduates, and much of their resources are dedicated to other subjects, such as biology and life sciences. This trend must be reversed if the United States is to lead the world with its cyber economy.

1. Foster Adequate Training and Education Programs to Support the Nation's Cybersecurity Needs

Improvements in cybersecurity training will be accomplished primarily through the work of private training organizations, institutions of learning, and the Nation's school systems.

DHS will also encourage private efforts to ensure that adequate opportunities exist for continuing education and advanced training in the workplace to maintain high skills standards and the capacity to innovate.

The federal government can play a direct role in several ways. First, *DHS will implement and encourage the establishment of programs to advance the training of cybersecurity professionals in the United States, including coordination with NSF, OPM, and NSA, to identify ways to leverage the existing Cyber Corps Scholarship for Service program as well as the various graduate, postdoctoral, senior researcher, and faculty development fellowship and traineeship programs created by the*

Cyber Security Research and Development Act, to address these important training and education workforce issues. (A/R 3-7)

2. Increase the Efficiency of Existing Federal Cybersecurity Training Programs

Second, DHS will explore the benefits of a center for the development of cybersecurity training practices that would draw together expertise and be consistent with the federal "build once, use many" approach. *DHS, in coordination with other agencies with cybersecurity training expertise, will develop a coordination mechanism linking federal cybersecurity and computer forensics training programs. (A/R 3-8)*

C. CERTIFICATION

1. Promote Private Sector Support for Well-coordinated Widely Recognized Professional Cybersecurity Certifications

Related to education and training is the need for certification of qualified persons. Certification can provide employers and consumers with greater information about the capabilities of potential employees or security consultants. Currently, some certifications for cybersecurity workers exist; however, they vary greatly in the requirements they impose. For example, some programs emphasize broad knowledge verified by an extensive multiple-choice exam, while others verify in-depth practical knowledge on a particular cyber component. No one certification offers a level of assurance about a person's practical and academic qualifications, similar to those offered by the medical and legal professions.

To address this issue, a number of industry stakeholders including representatives of both consumers and providers of IT security certifications are beginning to explore approaches to developing nationally recognized certifications and guidelines for certification.

Aspects that warrant consideration by these organizations include levels of education and experience, peer recognition, continuing education requirements, testing guidance, as applicable for various levels of certification that may be established, and models for administering a certification for IT security professionals similar to those successfully employed in other professions. DHS and other federal agencies, as downstream consumers (prospective employers of certified personnel), can aid these efforts by effectively articulating the needs of the federal IT security community.

DHS will encourage efforts that are needed to build foundations for the development of security certification programs that will be broadly accepted by the public and private sectors. DHS and other federal agencies can aid these efforts by effectively articulating the needs of the federal IT security community. (A/R 3-9)