Priority I: A National Cyberspace Security Response System

In the 1950s and 1960s, our Nation became vulnerable to attacks from aircraft and missiles for the first time. The federal government responded by creating a national system to: monitor our airspace with radar to detect unusual activity, analyze and warn of possible attacks, coordinate our fighter aircraft defenses during an attack, and restore our Nation after an attack through civil defense programs.

Today, the Nation's critical assets could be attacked through cyberspace. The United States now requires a different kind of national response system in order to detect potentially damaging activity in cyberspace, to analyze exploits and warn potential victims, to coordinate incident responses, and to restore essential services that have been damaged.

The fact that the vast majority of cyberspace is neither owned nor operated by any single group —public or private—presents a challenge for creating a National Cyberspace Security Response System. There is no synoptic or holistic view of cyberspace. Therefore, there is no panoramic vantage point from which we can see attacks coming or spreading. Information that indicates an attack has occurred (worms, viruses, denial-of-service attacks) accumulates through many different organizations. However, there is no organized mechanism for reviewing

these indicators and determining their implications.

To mitigate the impact of cyber attacks, information about them must disseminate widely and quickly. Analytical and incident response capabilities that exist in numerous organizations could be coordinated to determine how to best defend against an attack, mitigate effects, and restore service.

Establishing a proper administrative mechanism for the National Cyberspace Security Response System presents another challenge. Unlike the U.S. airspace-monitoring program during the Cold War, individuals who operate the systems that enable and protect cyberspace usually are not federal employees. Thus, the National Cyberspace Security Response System must operate from a less formal, collaborative network of governmental and nongovernmental organizations.

DHS is responsible for developing the national cyberspace security response system, which includes:

- Providing crisis management support in response to threats to, or attacks on, critical information systems; and
- Coordinating with other agencies of the federal government to provide specific warning information, and advice about appropriate protective measures and countermeasures, to state and local government agencies and authorities, the private sector, other entities, and the public.

DHS will lead and synchronize efforts for the National Cyberspace Security Response System as part of its overall information sharing and crisis coordination mandate; however, the system itself will consist of many organizations from both government and private sectors. The authorizing legislation for the Department of Homeland Security also created the position of a privacy officer to ensure that any mechanisms associated with the National Cyberspace Security Response System appropriately balance its mission with civil liberty and privacy concerns. This officer will consult regularly with privacy advocates, industry experts, and the public at large to ensure broad input and consideration of privacy issues so that we achieve solutions that protect privacy while enhancing security.

The National Cyberspace Security Response System

The National Cyberspace Security Response System is a public-private architecture, coordinated by the Department of Homeland Security, for analyzing and warning; managing incidents of national significance; promoting continuity in government systems and private sector infrastructures; and increasing information sharing across and between organizations to improve cyberspace security. The National Cyberspace Security Response System will include governmental entities and nongovernmental entities, such as private sector information sharing and analysis centers (ISACs).

Among the system components outlined below are existing federal programs and new federal initiatives pending budget-review consideration, as well as initiatives recommended for our partners.

A. ESTABLISH PUBLIC-PRIVATE ARCHITECTURE FOR RESPONDING TO NATIONAL-LEVEL CYBER INCIDENTS

Establishing the National Cyberspace Security Response System will not require an expensive or bureaucratic federal program. In many cases the system will augment the capabilities of several important federal entities with existing cyberspace security responsibilities, which are

National Cyberspace Security Response System

Components/ Capabilities

DHS Analysis Center

- Strategic group
- Tactical group
- Vulnerability assessments

DHS Incident Operations Center

- Cyber Warning and Information Network
- ISACs

DHS Incident Management Structure

- Federal coordination
- Private, state and local coordination

National Response Contingency Plans

- Federal plans
- Private plan coordination

now part of DHS. The synergy that results from integrating the resources of the National Communications System, the National Infrastructure Protection Center's analysis and warning functions, the Federal Computer Incident Response Center, the Office of Energy Assurance, and the Critical Infrastructure Assurance Office under the purview of the Under Secretary for Information Analysis and Infrastructure Protection will help build the necessary foundation for the National Cyberspace Security Response System.

The Nation's private-sector networks are increasingly targeted, and they will therefore likely be the first organizations to detect attacks with potential national significance. Thus, ISACs will play an increasingly important role in the National Cyberspace Security Response System and the overall missions of homeland security. ISACs possess unique operational insight into their industries' core functions and will help provide the necessary analysis to support national efforts.

Typically, an ISAC is an industry-led mechanism for gathering, analyzing, sanitizing, and disseminating sector-specific security information and articulating and promulgating best practices. ISACs are designed by the various sectors to meet their respective needs and financed through their memberships. DHS will work closely with ISACs as appropriate to ensure that they receive timely and actionable threat and vulnerability data and to coordinate voluntary contingency planning efforts. The federal government encourages the private sector to continue to establish ISACs and, further, to enhance the analytical capabilities of existing ISACs.

1. Analysis

a. Provide for the Development of Tactical and Strategic Analysis of Cyber Attacks and Vulnerability Assessments

Analysis is the first step toward gaining important insight about a cyber incident, including the nature of attack, the information it compromised, and the extent of damage it caused. Analysis can also provide an indication of the intruder's possible intentions, the potential tools he used, and the vulnerabilities he exploited. There are three closely related, but discrete, categories of analysis related to cyberspace:

(i) Tactical analysis examines factors associated with incidents under investigation or specific, identified vulnerabilities to generate indications and warnings. Examples of tactical analysis include: examining the delivery mechanism of a computer virus to develop and issue immediate guidance on ways to prevent or mitigate damage; and studying a specific computer intrusion, or set of intrusions, to determine the perpetrator, his motive, and his method of attack.

(ii) Strategic analysis looks beyond specific incidents to consider broader sets of incidents or implications that may indicate threats of potential national importance. For example, strategic analyses may identify long-term trends related to threat and vulnerability that could be used to provide advanced warnings of increasing risks, such as emerging attack methods. Strategic analysis also provides policymakers with information they can use to anticipate and prepare for attacks, thereby diminishing the damage they cause. Strategic analysis also provides a foundation to identify patterns that can support indications and warnings.

(iii) Vulnerability assessments are detailed reviews of cyber systems and their physical components to identify and study their weaknesses. Vulnerability assessments are an integral part of the intelligence cycle for cyberspace security. These assessments enable planners to predict the consequences of possible cyber attacks against specific facilities or sectors of the economy or government. These projections then allow infrastructure owners and operators to strengthen their defenses against various types of threat. (This will be discussed in the *Cyberspace Security Threat and Vulnerability Reduction Program.*)

DHS will foster the development of strong analytic capabilities in each of these areas. It should seek partnership and assistance from the private sector, including the ISACs, in developing these capabilities.

2. Warning

a. Encourage the Development of a Private Sector Capability to Share a Synoptic View of the Health of Cyberspace

The lack of a synoptic view of the Internet frustrates efforts to develop Internet threat analysis and indication and warning capabilities. The effects of a cyber attack on one sector have the potential to cascade across several other sectors, thereby producing significant consequences that could rapidly overwhelm the capabilities of many private companies and state and local governments. DHS's integration of several key federal cybersecurity operations centers creates a focal point for the federal government to manage cybersecurity emergencies in its own systems, and, if requested, facilitate crisis management in non-federal critical infrastructure systems.

Separately, industry is encouraged to develop a mechanism—whether virtual or physical—that could enable the sharing of aggregated information on Internet health to improve analysis, warning, response, and recovery. To the extent permitted by law, this voluntary coordination of activities among nongovernmental entities could enable different network operators and Internet backbone providers to analyze and exchange data about attacks. Such coordination could prevent exploits from escalating and causing damage or disruption of vital systems.

DHS will create a single point-of-contact for the federal government's interaction with industry and other partners for 24 x7 functions, including cyberspace analysis, warning, information sharing, major incident response, and national-level recovery efforts. Private sector organizations, which have major contributions for those functions, are encouraged to coordinate activities, as permitted by law, in order to provide a synoptic view of the health of cyberspace on a 24 x 7 basis. (A/R 1-1)

b. Expand the Cyber Warning and Information Network to Support DHS's Role in Coordinating Crisis Management for Cyberspace

Hours and minutes can make a difference between a major disruption and a manageable incident. Improving national capabilities for warning requires a secure infrastructure to provide assured communications between critical asset owners and operators and their service providers. The Cyber Warning and Information Network (CWIN) will provide an out-of-band private and secure communications network for government and industry, with the purpose of sharing cyber alert and warning information. The network will include voice conferencing and data collaboration.

While the first phase was implemented between the federal government cyber watch centers, CWIN participants will ultimately include other critical government and industry partners, such as ISACs that deal with cyber threats on a daily basis. As other entities expand in this area, membership will increase as well. Key to CWIN membership is the ability to share sensitive cyber threat information in a secure, protected, and trusted environment.

As outlined in the 2003 budget, the federal government will complete the installation of CWIN to key government cybersecurity-related network operation centers, to disseminate analysis and warning information and perform crisis coordination. The federal government will also explore linking the ISACs to CWIN. (A/R 1-2)

3. National Incident Management

Enhancing analytical capabilities within DHS, the private sector ISACs, and expanding CWIN will contribute to the improvement of national cyber incident management. However, incident management within the federal government will still require coordination with organizations other than those being transferred to DHS. For example, the Departments of Justice, Defense, and Commerce all have roles to perform in response to incidents in cyberspace. Within the White House a number offices have responsibilities, including the Office of Science and Technology Policy, which is responsible for executing emergency telecommunications authorities, the National Security Council, which coordinates all matters related to national security and international cooperation, and the Office of Management and Budget.

In addition, national incident management capabilities will also integrate state chief information officers as well as international entities, as appropriate. (See, *Priorities IV and V.*)

4. Response and Recovery

a. Create Processes to Coordinate the Voluntary Development of National Public-Private Continuity and Contingency Plans

Among the lessons learned from security reviews following the events of September 11, 2001, was that federal agencies had vastly inconsistent, and in most cases incomplete, contingency capabilities for their communications and other systems. Contingency planning is a key element of cybersecurity. Without adequate contingency planning and training, agencies may not be able to effectively handle disruptions in service and ensure business continuity. OMB, through the Federal Information Security Management Act requirements and with assistance from the inspectors general, is holding agencies accountable for developing continuity plans.

b. Exercise Cybersecurity Continuity Plans in Federal Cyber Systems

DHS has the responsibility for providing crisis management support in response to threats to, or attacks on, critical information systems for other government agencies, state and local governments and, upon request, the private sector. In order to establish a baseline

understanding of federal readiness, DHS will explore exercises for the civilian agencies similar to the Defense Department "Eligible Receiver" exercises that test cybersecurity preparedness.

To test civilian agencies' security preparedness and contingency planning, DHS will use exercises to evaluate the impact of cyber attacks on governmentwide processes. Weaknesses discovered will be included in agency corrective action plans and submitted to OMB. DHS also will explore such exercises as a way to test the coordination of public and private incident management, response and recovery capabilities. (A/R 1-3)

(i) Encourage increased cyber risk management and business continuity. There are a number of measures that nongovernmental entities can employ to manage the risk posed by cyberspace and plan for business continuity. Risk management is a discipline that involves risk assessment, risk prevention, risk mitigation, risk transfer, and risk retention.

There is no special technology that can make an enterprise completely secure. No matter how much money companies spend on cybersecurity, they may not be able to prevent disruptions caused by organized attackers. Some businesses whose products or services directly or indirectly impact the economy or the health, welfare or safety of the public have begun to use cyber risk insurance programs as a means of transferring risk and providing for business continuity.

An important way to reduce an organization's exposure to cyber-related losses, as well as to help protect companies from operational and financial impairment, is to ensure that adequate contingency plans are developed and tested.

Corporations are encouraged to regularly review and exercise IT continuity plans and to consider diversity in IT service providers as a way of mitigating risk. (A/R 1-4)

(ii) Promote public-private contingency planning for cybersecurity. It may not be possible to prevent a wide-range of cyber attacks. For those attacks that do occur, the Nation needs an integrated public-private plan for responding to significant outages or disruptions in cyberspace. Some organizations have plans for how they will recover their cyber network and capabilities in the event of a major outage or catastrophe. However, there is no mechanism for coordinating such plans across an entire infrastructure or at a national level.

The legislation establishing DHS also provides a trusted mechanism for private industry to develop contingency planning by using the voluntary preparedness planning provisions that were established in the Defense Production Act of 1950, as amended.

Infrastructure sectors are encouraged to establish mutual assistance programs for cybersecurity emergencies. DoJ and the Federal Trade Commission should work with the sectors to address barriers to such cooperation, as appropriate. In addition, DHS's Information Analysis and Infrastructure Protection Directorate will coordinate the development and regular update of voluntary, joint government-industry cybersecurity contingency plans, including a plan for recovering Internet functions. (A/R 1-5)

B. INFORMATION SHARING

1. Improve and Enhance Public-Private Information Sharing about Cyber Attacks, Threats, and Vulnerabilities

Successfully developing capabilities for analysis, indications, and warnings requires a voluntary public-private information sharing effort. The voluntary sharing of information about such incidents or attacks is vital to cybersecurity. Real or perceived legal obstacles make some organizations hesitant to share information about cyber incidents with the government or with each other. First, some fear that shared data that is confidential, proprietary, or

potentially embarrassing could become subject to public examination when shared with the government. Second, concerns about competitive advantage may impede information sharing between companies within an industry. Finally, in some cases, the mechanisms are simply not yet in place to allow efficient sharing of information.

The legislation establishing DHS provides several specific mechanisms intended to improve two-way information sharing. First, the legislation encourages industry to share information with DHS by ensuring that such voluntarily provided data about threats and vulnerabilities will not be disclosed in a manner that could damage the submitter. Second, the legislation requires that the federal government share information and analysis with the private sector as appropriate and consistent with the need to protect classified and other sensitive national security information.

As required by law, DHS, in consultation with appropriate federal agencies, will establish uniform procedures for the receipt, care, and storage by federal agencies of critical infrastructure information that is voluntarily submitted to the government.

The procedures will address how the Department will:

- Acknowledge the receipt of voluntarily submitted critical infrastructure information;
- Maintain the information as voluntarily submitted critical infrastructure information;
- Establish protocols for the care and storage of such information; and
- Create methods for protecting the confidentiality of the submitting entity while still allowing the information to be used in the issuance of notices and warnings for protection of the critical infrastructure.

DHS will raise awareness about the removal of impediments to information sharing about cybersecurity and infrastructure vulnerabilities between the public and private sectors. The Department will also establish an infrastructure protection program office to manage the information flow, including the development of protocols for how to care for "voluntarily submitted critical infrastructure information." (A/R 1-6)

2. Encourage Broader Information Sharing on Cybersecurity

Nongovernmental organizations with significant computing resources are encouraged to take active roles in information sharing organizations. Corporations, colleges, and universities can play important roles in detecting and reporting cyber attacks, exploits, or vulnerabilities. In particular, both corporations and institutions of higher learning can gain from increased sharing on cyberspace security issues. Programs such as ISACs, FBI Infragard, or the United States Secret Service electronic crimes task forces can also benefit the respective participants. Because institutions of higher learning have vast computer resources that can be used as launch pads for attacks, colleges and universities are encouraged to consider establishing an on-call point-of-contact to Internet service providers (ISPs) and law enforcement officials.

Corporations are encouraged to consider active involvement in industrywide programs to share information on IT security, including the potential benefits of joining an appropriate ISAC. Colleges and universities are encouraged to consider establishing: (1) one or more ISACs to deal with cyber attacks and vulnerabilities; and, (2) an on-call point-of-contact, to Internet service providers and law enforcement officials in the event that the school's IT systems are discovered to be launching cyber attacks. (A/R 1-7)