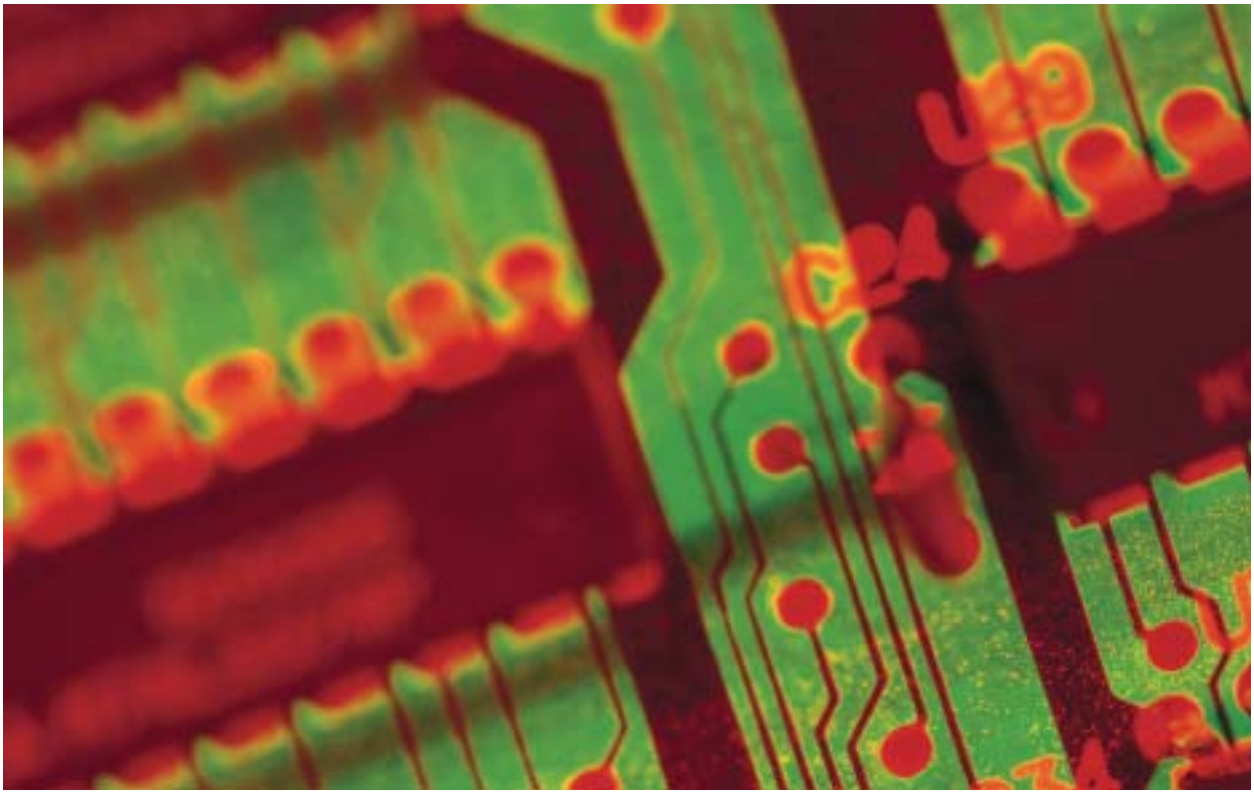

Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program

Malicious actors in cyberspace can take many forms including individuals, criminal cartels, terrorists, or nation states. While attackers take many forms, they all seek to exploit vulnerabilities created by the design or implementation of software, hardware, networks, and protocols to achieve a wide range of political or economic effects. As our reliance on cyberspace increases so too does the scope of damage that malicious actors can impose.

Waiting to act until we learn that a malicious actor is about to exploit a particular vulnerability is risky. Such warning information may not always be available. Even when warning data is available, remediation of some vulnerabilities may take days, weeks, or even years. As a result, vulnerabilities must be identified and corrected in critical networks before threats surface. The most dangerous vulnerabilities must be prioritized and reduced in a systematic fashion.

As technology evolves and new systems are introduced, new vulnerabilities emerge. Our strategy cannot be to eliminate all

vulnerabilities, or to deter all threats. Rather, we will pursue a three-part effort to:

(1) Reduce threats and deter malicious actors through effective programs to identify and punish them;

(2) Identify and remediate those existing vulnerabilities that could create the most damage to critical systems, if exploited; and

(3) Develop new systems with less vulnerability and assess emerging technologies for vulnerabilities.

The federal government cannot accomplish these goals acting alone. It can only do so in partnership with state and local governments and the private sector. Many federal agencies must play a part in this effort, which will be led and coordinated by DHS as part of its overall vulnerability reduction mandate.

The components of this program are discussed in this section. They include federal programs (both existing programs and initiatives that will be considered as part of the budget decision making process) and activities that the federal government recommends to its partners. Many activities that can be taken by individuals, companies, and other private organizations to reduce vulnerabilities will be stimulated and accelerated through awareness and are discussed as part of the awareness initiative described in Priority III.

A. REDUCE THREAT AND DETER MALICIOUS ACTORS

1. Enhance Law Enforcement's Capabilities for Preventing and Prosecuting

The *National Strategy to Secure Cyberspace* is especially concerned with those threats that could cause significant damage to our economy or security through actions taken using or against our cyber infrastructure. By identifying threats that would cause us significant harm, we can reduce the threats to homeland security, national security, and the economy. Law enforcement and the national security community play a critical role in preventing attacks in cyberspace. Law enforcement plays the central role in attributing an attack through the exercise of criminal justice authorities.

Many cyber-based attacks are crimes. As a result the Justice Department's Computer Crime and Intellectual Property Section, the FBI's Cyber Division, and the U.S. Secret Service all play a central role in apprehending and swiftly bringing to justice the responsible individuals. When incidents do occur, a rapid response can stem the tide of an ongoing attack and lessen the harm that is ultimately caused. The Nation currently has laws and mechanisms to ensure quick responses to large incidents. Ideally, an investigation, arrest, and prosecution of the perpetrators, or a diplomatic or military response in the case of a state-sponsored action, will follow such an incident.

Threat reduction, however, involves more than prosecution. Analyzing and disseminating practical information gathered by law enforcement can help promote national infrastructure security. For example, through various initiatives such as the FBI Infragard program and the U.S. Secret Service electronic crimes task forces, law enforcement can share lessons learned from attacks with private sector organizations. The information gleaned from investigations can provide the federal government and private industry a framework for examining the robustness of their cybersecurity skill sets, and assist in prioritizing their limited resources to manage the unique risk of their enterprise.

Justice and the FBI will need to work closely with DHS to ensure that the information gleaned from investigations is appropriately analyzed and shared with ISACs and other nongovernmental entities to promote improved risk management in critical infrastructure sectors.

The Nation will seek to prevent, deter, and significantly reduce cyber attacks by ensuring the identification of actual or attempted perpetrators followed by an appropriate government response. In the case of cybercrime this would include swift apprehension, and appropriately severe punishment.

DOJ and other appropriate agencies will develop and implement efforts to reduce cyber attacks and cyber threats through the following means: (1) identifying ways to improve information sharing and investigative coordination within the federal, state, and local law enforcement community working on critical infrastructure and cyberspace security matters, and with other agencies and the private sector; (2) exploring means to provide sufficient investigative and forensic resources and training to facilitate expeditious investigation and resolution of critical infrastructure incidents; and, (3) developing better data about victims of cybercrime and intrusions in order to understand the scope of the problem and be able to track changes over time. (A/R 2-1)

2. Create a Process for National Vulnerability Assessments to Better Understand the Potential Consequences of Threats and Vulnerabilities

a. Assess the Potential Impact of Strategic Cyber Attacks

To better understand how to further detect and prevent attacks, the Nation must know the threat it is facing. To date, no comprehensive assessment of the impact of a strategic cyber attack against the United States has been conducted. Because nation states and terrorists are developing capabilities for cyber-based attacks, it is important to understand the potential impact of such an attack and possible ways to mitigate the effects. *DHS, in coordination with appropriate agencies and the private sector, will lead in the development and conduct of a national threat assessment including red teaming, blue teaming, and other methods to identify the impact of possible attacks on a variety of targets. (A/R 2-2)*

B. IDENTIFY AND REMEDIATE EXISTING VULNERABILITIES

Reducing vulnerabilities can be resource intensive. Accordingly, our national efforts to identify and remediate vulnerabilities must be focused to reduce vulnerabilities in a cost effective and systematic manner. The United States must reduce vulnerabilities in four major components of cyberspace, including: (1) the mechanisms of the Internet; (2) digital control

How the Internet Works

Data sent from one computer to another across the Internet is broken into small packets of information containing addressing information as well as a portion of the total message. The packets travel across the Internet separately and are reassembled at the receiving computer. There are two primary protocols that enable these packets of data to traverse the complex networks and arrive in an understandable format. These protocols are: (1) the Transmission Control Protocol (TCP) which decomposes data into packets and ensures that they are reassembled properly at the destination; and (2) the Internet Protocol (IP), which guides or routes the packets of data though the Internet. Together they are referred to as TCP/IP.

IP is essential to almost all Internet activities including sending data such as e-mail. Data is transmitted based on IP addresses, which are a series of numbers. The Domain Name System (DNS) was developed to simplify the management of IP addresses. The DNS maps IP numbers to recognizable sets of letters, words or numbers. The DNS does this by establishing domains and a structured hierarchical addressing scheme.

systems/supervisory control and data acquisition systems; (3) software and hardware vulnerability remediation; and, (4) physical infrastructure and interdependency. These four areas have broad implications for the majority of the Nation's critical infrastructures. Initiating efforts to eliminate vulnerabilities in these important areas will reduce the vulnerability of critical infrastructure services to attack or compromise.

1. Secure the Mechanisms of the Internet

The development and implementation of the mechanisms for securing the Internet are responsibilities shared by its owners, operators, and users. Private industry is leading the effort to ensure that the core functions of the Internet develop in a secure manner. As appropriate, the federal government will continue to support these efforts. The goal is the development of secure and robust mechanisms that will enable the Internet to support the Nation's needs now and in the future. This will include securing the protocols on which the Internet is based, ensuring the security of the routers that direct the flow of data, and implementing effective management practices.

a. Improve the Security and Resilience of Key Internet Protocols

Essential to the security of the Internet infrastructure is ensuring the reliability and secure use of three key protocols: the Internet Protocol (IP), the Domain Name System (DNS), and the Border Gateway Protocol (BGP).

(i) Internet Protocol. The Internet is currently based on Internet Protocol version 4 (IPv4). Some organizations and countries are moving to an updated version of the protocol, version 6 (IPv6). IPv6 offers several advantages over IPv4. In addition to offering a vast amount of addresses, it provides for improved security features, including attribution and native IP security (IPSEC), as well as enabling new applications and capabilities. Some countries are moving aggressively to adopt IPv6. Japan has committed to a fully IPv6 based infrastructure by 2005. The European Union has initiated steps to move to IPv6. China is also considering early adoption of the protocol.

The United States must understand the merits of, and obstacles to, moving to IPv6 and, based on that understanding, identify a process for moving to an IPv6 based infrastructure. The federal government can lead in developing this understanding by employing IPv6 on some of its own networks and by coordinating its activities with those in the private sector. *The Department of Commerce will form a task force to examine the issues related to IPv6, including the appropriate role of government, international interoperability, security in transition, and costs and benefits. The task force will solicit input from potentially impacted industry segments. (A/R 2-3).*

(ii) Secure the Domain Name System. DNS serves as the central database that helps route information throughout the Internet. The ability to route information can be disrupted when the databases cannot be accessed or updated or when they have been corrupted. Attackers can disrupt the DNS by flooding the system with information or requests or by gaining access to the system and corrupting or destroying the information that it contains. The October 21, 2002 attacks on the core DNS root servers revealed a vulnerability of the Internet by degrading or disrupting some of the 13 root servers necessary for the DNS to function. The occurrence of this attack punctuates the urgent need for expeditious action to make such attacks more difficult and less effective.

(iii) Border Gateway Protocol. Of the many routing protocols in use within the Internet, the Border Gateway Protocol (BGP) is at greatest risk of being the target of attacks designed to disrupt or degrade service on a large scale. BGP is used to interconnect the thousands of networks that make up the Internet. It allows routing information to be exchanged between networks that may have separate administrators, administrative policies, or protocols.

Propagation of false routing information in the Internet can deny service to small or large portions of the Internet. For example, false routes can create "black holes" that absorb traffic destined for a particular block of address space. They can also lead to cascade failures that have occurred in other types of large routing/switching systems in the past, where the failure of one switch or mechanism results in the failure of those connected to it, resulting in additional waves of failures expanding outward from the initial fault.

More secure forms of BGP and DNS will benefit all owners, operators and users of the Internet. To address this issue, the Internet Engineering Task Force, a voluntary private body consisting of users, owners, and operators of the Internet, has established working groups for securing BGP and DNS. These groups have made progress, but have been limited by technical obstacles and the need for coordination.

The security and continued functioning of the Internet will be greatly influenced by the success or failure of implementing more secure and more robust BGP and DNS. The Nation has a vital interest in ensuring that this work proceeds. The government should play a role when private efforts break down due to a need for coordination or a lack of proper incentives.

b. Promote Improved Internet Routing

Routers on the Internet share a number of design characteristics that make them relatively easy to disable, especially through denial-of-service (DoS) attacks that overwhelm a router's processing capability. Internet routing can be substantially improved by promoting increased use of address verification and "out-of-band" management.

(i) Address Verification. Today there are few effective solutions available, even commercially, to mitigate the effect of DoS attacks, as the scale and lack of address verification and accountability makes filtering and contacting the sources of an attack impossible. One of the largest weaknesses in our current Internet infrastructure is the lack of source address verification. Establishing an Internet infrastructure that provides forged source address filtering is a critical step towards defeating these types of attacks.

(ii) Out-of-Band Management. DoS attacks are difficult to mitigate because they prevent control data from reaching the router. Separate control networks, commonly called "out-of-band" management links, are one technique that can be used to counter DoS attacks.

DHS will examine the need for increased research to improve router security through new technology or approaches to routing information. In particular, DHS will assess progress on out-of-band management and address filtering and recommend steps that can be taken by government or the private sector to improve their effectiveness and use. In addition, DHS will work with the private sector to understand the most efficient path and obstacles to increasing router security using current techniques and technology.

c. Improve Management

Much improvement can be made in the security of the Internet infrastructure if best practices for managing the Internet, including the data that flows through it and the equipment that supports it, are widely employed. DHS will work with organizations that own and operate the Internet to develop and promote the adoption of best practices. In particular, DHS will work with Internet service providers to help develop a widely accepted "code of conduct" for network management. This work will include a review of existing documented best practices such as those published by Network Reliability and Interoperability Council (NRIC) of the Federal Communications Commission (FCC).

DHS, in coordination with the Commerce Department and appropriate agencies, will coordinate public-private partnerships to encourage: (1) the adoption of improved security protocols; (2) the development of more secure router technology; and, (3) the adoption by ISPs of a "code of good conduct," including cybersecurity practices and security related cooperation. DHS will support these efforts as required for their success, subject to other budget considerations. (A/R 2-4)

2. Foster Trusted Digital Control Systems / Supervisory Control and Data Acquisition Systems

Many industries in America have radically transformed the way they control and monitor equipment over the last 20 years by employing digital control systems (DCS) and supervisory control and data acquisition systems (SCADA). DCS/SCADA are computer-based systems that are used by many infrastructures and industries to remotely control sensitive processes and physical functions that once had to be controlled manually. DCS and SCADA are present in almost every sector of the economy including water, transportation, chemicals, energy, and manufacturing, among others. Increasingly DCS/SCADA systems use the Internet to transmit data rather than the closed networks used in the past.

Securing DCS/SCADA is a national priority. Disruption of these systems can have significant consequences for public health and safety. However, securing these systems is complicated by various factors. First, adding security requires investment in systems and in research and development that companies cannot afford or justify on their own. Such research may require the involvement of multiple infrastructure operators or industries. Second, current technological limitations could impede the implementation of security measures. For example, DCS/SCADA systems are typically small and self-contained units with limited power supplies. Security features are not easily adapted to the space or power requirements. In addition, these systems operate in real time and security measures could reduce performance or impact the synchronization of larger processes.

Both the private and public sectors have a role in securing SCADA systems. DHS, in coordination with the Department of Energy and other concerned agencies, will work in partnership with private industry to ensure that there is broad awareness among industry vendors and users, both regulated and unregulated, of the vulnerabilities in DCS/SCADA systems, and the consequences of exploitation of those vulnerabilities. For operators of DCS/SCADA systems, these efforts should include developing and deploying training and certification of DCS/SCADA-oriented software and hardware security. In addition, DHS will work with the private sector to promote voluntary standards efforts, and security policy creation.

The development of adequate test bed environments and the development of technology in the areas of extremely low latency link encryptors/authenticators, key management, and network status/state-of-health monitoring will aid in the effort to secure DCS/SCADA. *DHS, in coordination with DOE and other concerned agencies and in partnership with industry, will develop best practices and new technology to increase security of DCS/SCADA, to determine the most critical DCS/SCADA-related sites, and to develop a prioritized plan for short-term cybersecurity improvements in those sites. (A/R 2-5)*

3. Reduce and Remediate Software Vulnerabilities

A third critical area of national exposure is the many flaws that exist in critical infrastructure due to software vulnerabilities. New vulnerabilities emerge daily as use of software reveals flaws that malicious actors can exploit. Currently, approximately 3,500 vulnerabilities are reported annually. Corrections are usually completed by the manufacturer in the form of a

patch and made available for distribution to fix the flaws.

Many known flaws, for which solutions are available, remain uncorrected for long periods of time. For example, the top ten known vulnerabilities account for the majority of reported incidents of cyber attacks. This happens for multiple reasons. Many system administrators may lack adequate training or may not have time to examine every new patch to determine whether it applies to their system. The software to be patched may affect a complex set of interconnected systems that take a long time to test before a patch can be installed with confidence. If the systems are critical, it could be difficult to shut them down to install the patch.

Unpatched software in critical infrastructures makes those infrastructures vulnerable to penetration and exploitation. Software flaws are exploited to propagate "worms" that can result in denial of service, disruption, or other serious damage. Such flaws can be used to gain access to and control over physical infrastructure. Improving the speed, coverage, and effectiveness of remediation of these vulnerabilities is important for both the public and private sector.

Several steps will help. First, the Nation needs a better-defined approach to the disclosure of vulnerabilities. The issue is complex because exposing vulnerabilities both helps speed the development of solutions and also creates opportunities for would be attackers. In addition, the clearinghouse for such disclosures must be a neutral body between vendors, security companies, and the public at large. Today the government partially funds such organizations. However, the appropriate level and form for this funding need to be reviewed. *DHS will work with the National Infrastructure Advisory Council and private sector organizations to develop an optimal approach and mechanism for vulnerability disclosure. (A/R 2-6)*

A second step that will speed the distribution of patches in software systems is the creation of common test-beds. Such test-beds running applications that are common among government agencies or companies can speed patch implementation by testing one time, for many users, the impact that a patch will have on a variety of applications. *GSA will work with DHS on an improved approach to implementing a patch clearinghouse for the federal government. DHS will also share lessons learned with the private sector and encourage the development of a voluntary, industry-led, national effort to develop a similar clearinghouse for other sectors including large enterprises. (A/R 2-7)*

Finally, best practices in vulnerability remediation should be established and shared in areas such as training requirements for system administrators, the use of automated tools, and management processes for patch implementation. DHS will work with public and private entities on the development and dissemination of such practices. More secure initial configurations for shipped cyber products would facilitate more secure use by making the default set-up secure rather than insecure. *The software industry is encouraged to consider promoting more secure "out-of-the-box" installation and implementation of their products, including increasing: (1) user awareness of the security features in products; (2) ease-of-use for security functions; and, (3) where feasible, promotion of industry guidelines and best practices that support such efforts. (A/R 2-8)*

4. Understand Infrastructure Interdependency and Improve Physical Security of Cyber Systems and Telecommunications

Reducing the vulnerability of the cyber infrastructure includes mitigating the potentially devastating attacks on cyberspace that can occur when key physical linkages are destroyed. The impact of such attacks can be amplified by cascading impacts through a variety of dependant infrastructures affecting both the economy and the health and welfare of citizens: a train derailed in a Baltimore tunnel and the

Internet slowed in Chicago; a campfire in New Mexico damaged a gas pipeline and IT-related production halted in Silicon Valley; a satellite spun out of control hundreds of miles above the Earth and affected bank customers could not use their ATMs.

Cyberspace has physical manifestations: the buildings and conduits that support telecommunications and Internet networks. These physical elements have been designed and built to create redundancy and avoid single points of failure. Nonetheless, the carriers and service providers are encouraged to independently and collectively continue to analyze their networks to strengthen reliability and intentional redundancy. The FCC, through its Network Reliability and Interoperability Council, and the National Security Telecommunications Advisory Committee, can contribute to such efforts and should identify any governmental impediments to strengthening the national networks.

DHS will work actively to reduce interdependencies and physical vulnerability. *DHS will establish and lead a public-private partnership to identify cross-sectoral interdependencies, both cyber and physical. The partnership will develop plans to reduce related vulnerabilities in conjunction with programs proposed in the National Strategy for Homeland Security. The National Infrastructure Simulation and Analysis Center in DHS will support these efforts by developing models to identify the impact of cyber and physical interdependencies. (A/R 2-9)*

DHS also will support, when requested and as appropriate, voluntary efforts by owners and operators of information system networks and network data centers to develop remediation and contingency plans to reduce the consequences of large-scale physical damage to facilities supporting such networks, and to develop appropriate procedures for limiting access to critical facilities. (A/R 2-10)

C. DEVELOP SYSTEMS WITH FEWER VULNERABILITIES AND ASSESS EMERGING TECHNOLOGIES FOR VULNERABILITIES

As the Nation takes steps to improve the security of current systems, it must also ensure that future cyber systems and infrastructure are built to be secure. This will become increasingly important as more and more of our daily economic and physical lives come to depend on cyber infrastructure. Future security requires research in cyberspace security topics and a commitment to the development of more secure products.

1. Prioritize the Federal Research and Development Agenda

Federal investment in research for the next generation of technologies to maintain and secure cyberspace must keep pace with an increasing number of vulnerabilities. Flexibility and nimbleness are important in ensuring that the research and development process accommodates the dynamic technology environment in the years ahead.

The Nation will prioritize and provide resources as necessary to advance the research to secure cyberspace. A new generation of enabling technologies will serve to "modernize" the Internet for rapidly growing traffic volumes, expanded e-commerce, and the advanced applications that will be possible only when next-generation networks are widely available. As a result, national research efforts must be prioritized to support the transition of cyberspace into a secure, high-speed knowledge and communications infrastructure for this century. Vital research is required for this effort. The Nation must prioritize its cyberspace security research efforts across all sectors and funding sources.

To meet these needs, the Director of OSTP will coordinate the development, and update on an annual basis, a federal government research and

development agenda that includes near-term (1-3 years), mid-term (3-5 years), and later (5 years out and longer) IT security research for Fiscal Year 2004 and beyond. Existing priorities include, among others, intrusion detection, Internet infrastructure security (including protocols such as BGP and DNS), application security, DoS, communications security (including SCADA system encryption and authentication), high-assurance systems, and secure system composition. (A/R 2-11)

To optimize research efforts relative to those of the private sector, DHS will ensure that adequate mechanisms exist for coordination of research and development among academia, industry, and government, and will develop new mechanisms where needed. (A/R 2-12)

An important goal of cybersecurity research will be the development of highly secure, trustworthy, and resilient computing systems. In the future, working with a computer, the Internet, or any other cyber system may become as dependable as turning on the lights or the water.

The Nation must seek to ensure that future components of the cyber infrastructure are built to be inherently secure and dependable for their users. Development of highly secure and reliable systems will be pursued, subject to budgeting constraints, through the national cyberspace security research agenda.

The private sector is encouraged to consider including in near-term research and development priorities, programs for highly secure and trustworthy operating systems. If such systems are developed and successfully evaluated, the federal government will, subject to budget considerations, accelerate procurement of such systems. (A/R 2-13)

In addition, DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development. (A/R 2-14)

2. Assess and Secure Emerging Systems

As new technologies are developed they introduce the potential for new security vulnerabilities. Some new technologies introduce security weaknesses that are only corrected over time, with great difficulty, or sometimes not at all. A person driving in a car around a city, for example, can access many wireless local area networks without the knowledge of their owners unless strong security measures are added to those systems.

As telephones and personal digital assistants, and many other mobile devices, incorporate more sophisticated operating systems and connectivity they may require security features to prevent their exploitation for distributed attacks on mobile networks and even the Internet.

Emerging areas of research also can produce unforeseen consequences for security. The emergence of optical computing and intelligent agents, as well as in the longer term, developments in areas such as nanotechnology and quantum computing, among others, will likely reshape cyberspace and its security. The Nation must be at the leading edge in understanding these technologies and their implications for security.

DHS, in coordination with OSTP and other agencies, as appropriate, will facilitate communication between the public and private research and the security communities, to ensure that emerging technologies are periodically reviewed by the appropriate body within the National Science and Technology Council, in the context of possible homeland and cyberspace security implications, and relevance to the federal research agenda. (A/R 2-15)