# Actions and Recommendations (A/R) Summary

## Priority I: A National Cyberspace Security Response System

A/R 1-1: 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 1-2: 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 1-3: 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 the 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 1-4: 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 1-5: 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 1-6: 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 1-7: 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.

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

A/R 2-1: 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 2-2: 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 2-3: 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 2-4: 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 2-5: 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 2-6: 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 2-7: 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 2-8: 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 2-9: 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 2-10: 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 2-11: 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 2-12: 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 2-13: 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 2-14: 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 2-15: 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.

## Priority III: A National Cyberspace Security Awareness and Training Program

A/R 3-1: 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 3-2: 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 3-3: 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 3-4: 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 practices dissemination.

A/R 3-5: 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 3-6: 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 3-7: 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 3-8: 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 3-9: 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.

## Priority IV: Securing Governments' Cyberspace

A/R 4-1: Federal agencies will continue to expand the use of automated, enterprise-wide security assessment and security policy enforcement tools and actively deploy threat management tools to deter attacks. The federal government will determine whether specific actions are necessary (e.g., through the policy or budget processes) to promote the greater use of these tools.

A/R 4-2: Through the ongoing E-Authentication initiative, the federal government will review the need for stronger access control and authentication; explore the extent to which all departments can employ the same physical and logical access control tools and authentication mechanisms; and, consequently, further promote consistency and interoperability.

A/R 4-3: Federal agencies should consider installing systems that continuously check for unauthorized connections to their networks. Agency policy and procedures should reflect careful consideration of additional risk reduction measures, including the use of strong encryption, bi-directional authentication, shielding standards and other technical security

considerations, configuration management, intrusion detection, incident handling, and computer security awareness and training programs.

A/R 4-4: Additionally, the federal government will be conducting a comprehensive review of the National Information Assurance Partnership (NIAP), to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. This review will include lessons-learned from implementation of the Defense Department's July 2002 policy requiring the acquisition of products reviewed under the NIAP or similar evaluation processes.

A/R 4-5: The federal government will explore whether private sector security service providers to the federal government should be certified as meeting certain minimum capabilities, including the extent to which they are adequately independent.

A/R 4-6: State and local governments are encouraged to establish IT security programs for their departments and agencies, including awareness, audits, and standards; and to participate in the established ISACs with similar governments.

## Priority V: National Security and International Cyberspace Security Cooperation

A/R 5-1: The FBI and intelligence community should ensure a strong counterintelligence posture to counter cyber-based intelligence collection against the U.S. Government, and commercial and educational organizations. This effort must include a deeper understanding of the capability and intent of our adversaries to use cyberspace as a means for espionage.

A/R 5-2: The intelligence community, DoD, and the law enforcement agencies must improve the Nation's ability to quickly attribute the source of threatening attacks or actions to enable timely and effective response. Consistent with the *National Security Strategy*, these efforts will also seek to develop capabilities to prevent attacks from reaching critical systems and infrastructures.

A/R 5-3: The United States must improve interagency coordination between law enforcement, national security, and defense agencies involving cyber-based attacks and espionage, ensuring that criminal matters are referred, as appropriate, among those agencies. The National Security Council and the Office of Homeland Security will lead a study to ensure that appropriate mechanisms are in place.

A/R 5-4: When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies.

A/R 5-5: The United States will work through appropriate international organizations and in partnership with industry to facilitate dialogue between foreign public and private sectors on information infrastructure protection and promote a global "culture of security."

A/R 5-6: The United States will work with Canada and Mexico to make North America a "Safe Cyber Zone." We will expand programs to identify and secure critical common networks that underpin telecommunications, energy, transportation, banking and finance systems, emergency services, food, public health, and water systems.

A/R 5-7: The United States will urge each nation to build on the common Y2K experience and appoint a centralized point-of-contact who can act as a liaison between domestic and global cybersecurity efforts. Establishing points of contact can greatly enhance the international coordination and resolution of cyberspace

security issues. We will also encourage each nation to develop its own watch-and-warning network capable of informing government agencies, the public, and other countries about impending attacks or viruses.

A/R 5-8: To facilitate real-time sharing of the threat information as it comes to light; the United States will foster the establishment of an international network capable of receiving, assessing, and disseminating this information globally. Such a network can build on the capabilities of nongovernmental institutions such as the Forum of Incident Response and Security Teams.

A/R 5-9: The United States will encourage regional organizations, such as the APEC, EU, and OAS, to each form or designate a committee responsible for cybersecurity. Such committees would also benefit from establishing parallel working groups with representatives from the private sector. The United States will also encourage regional organizations—such as the APEC, EU, and OAS—to establish a joint committee on cybersecurity with representatives from government and the private sector.

A/R 5-10: The United States will encourage other nations to accede to the Council of Europe Convention on Cybercrime or to ensure that their laws and procedures are at least as comprehensive.