CYBER SECURITY INDUSTRY ALLIANCE

Agenda for the Next Administration

Proposals by the Cyber Security Industry Alliance

December 7, 2004

Cyber Security Agenda for the Next Administration

Proposals by the Cyber Security Industry Alliance

Three years ago, Americans were shocked with the dramatic need to strengthen security. Following the tragedy of 9/11, physical security has been the appropriate national focus. Now, security enhancement requires the added dimension of *cyber security*, especially as technology integrates more deeply with national defense, business and daily life. Cyber attacks and security breaches cost the U.S. economy billions of dollars in direct losses, downtime, stolen identities and intellectual property, and risks of catastrophic system failure from weakened critical infrastructure.

The Cyber Security Industry Alliance (CSIA) understands that the private sector bears a significant burden for improving cyber security. CSIA embraces the concept of sharing that responsibility between information technology suppliers and operators to improve cyber security. Cyber security also requires non-partisan government leadership. Work to strengthen cyber security began in the Clinton administration. The Bush administration has continued and boosted this work, through the creation of the National Strategy to Secure Cyberspace. The National Strategy remains timely and salient.

The Executive Branch, however, must exert more leadership. We urge President Bush in his second term to use his influence to follow through on the National Strategy to Secure Cyberspace – including adopting and fulfilling a concrete agenda that further protects and strengthens freedom for all Americans. CSIA proposes the following federal agenda aimed to (1) raise the profile of cyber security, (2) promote information sharing, threat analysis and contingency planning, and (3) boost efforts in research and development and in security education.

I

Raise the Profile of Cyber Security

The next administration should raise the national profile of cyber security by dedicating an assistant secretary position in the Department of Homeland Security, ratification of the Council of Europe's Convention on Cybercrime in the U.S. Senate, encouraging information security governance in the private sector, and leading by example with federal procurement practices.

Establish a dedicated cyber security post in the Department of Homeland Security

Currently in the Department of Homeland Security, the Under Secretary for Infrastructure Protection and Information Analysis has one Assistant Secretary responsible for both physical and cyber security. The House of Representatives has started an initiative to split this function between two Assistant Secretaries which is included in the 9-11 legislation currently being deliberated by House-Senate Conferees. We strongly urge President Bush to support this initiative. Critical information infrastructure underpins our economy and national security. Unlike other sectors, the information infrastructure is dynamic and will continue to evolve for the foreseeable future. Changes within the information infrastructure are driving change in all other sectors. Cyber and physical infrastructure security will receive greater respective attention with an Assistant Secretary for Cyber Security working alongside the Assistant Secretary for Infrastructure Protection, while remaining integrated under the leadership of the Undersecretary for Infrastructure Protection and Information Analysis. It is particularly important that the Assistant Secretary for Cyber Security have primary authority over the National Communications System given the convergence of voice and data networks.

Ratify the Council of Europe's Convention on Cybercrime

The Convention on Cybercrime is the first and only international treaty aimed to protect society from cybercrime. Cybercrime is more far-reaching than traditional crime because it transcends geographical and national boundaries. Cybercrime is also challenging existing legal concepts, particularly since it transcends sovereign borders. The Council of Europe, with significant input from the U.S. Justice Department, engineered the Convention on Cybercrime to promote a common, cooperative approach to prosecuting people who commit cybercrime. The Convention defines and prohibits cybercrime, provides national legal procedures, investigation tools and human rights safeguards, and establishes a regime for international cooperation. The U.S. signed the Convention on November 23, 2001; it was conveyed to the Senate on November 17, 2003. The Bush Administration should urge the Senate to rapidly consider and ratify the Convention, providing the U.S. with legal tools to combat and prevent cybercrime against Americans. By ratifying the treaty – including reservations and declarations by the State Department making it conform with federal law and the U.S. Constitution – the U.S. will show international leadership, will require no new legislation to comply with the treaty, will remove or minimize legal obstacles for international investigation and prosecution of cybercrime, will deny safe havens to cybercriminals, and will safeguard civil liberties of Americans.

Promote information security governance in the private sector

The Administration should lend additional support to efforts by the Departments of Commerce and Department of Homeland Security to encourage private sector boards of directors and chief executive officers to make cyber security an integral part of corporate governance. The Department of Commerce should urge CEOs to review cyber security measures during board meeting reviews of business operations. The effort should include helping corporate officers and executives understand the cyber security-related implications of the Sarbanes-Oxley Act of 2002, Gramm-Leach-Bliley Act of 1999, and the Health Care Insurance Portability and Accounting Act of 1996, which will help increase awareness about cyber security in the business community.

CSIA is organizing a summit in New York this spring 2005 to examine the IT security implications of Sarbanes-Oxley, which will include chief financial officers, chief information officers, auditors, and relevant government and regulatory authorities.

Lead by example with federal procurement practices

The diligent use of cyber security technology will help prevent attacks and promote the operational safety of federal information systems. Agencies have made progress over the past few years under Federal Information Security Management Act guidelines and procedures for procurement of cyber security technology. Federal agencies should continue to leverage these procurement practices by requiring government contractors, subcontractors and suppliers to take similar measures to secure their IT systems. Areas of focus include deployment of strong authentication and authorization controls, encrypting data and communications where appropriate, and using digital signatures. The importance of deploying these technologies has also been highlighted by the President's National Infrastructure Advisory Council (NIAC).

II

Information Sharing, Threat Analysis and Contingency Planning

There is a major requirement for broader, integrated information sharing, threat analysis and contingency planning between federal agencies and private sector operators of critical information infrastructure. The next administration should close the strategic gap between protection national security and private sector information systems, strengthen Information Sharing and Analysis Centers (ISACs), establish and test a survivable emergency information network, and develop and track the costs associated with cyber attacks.

Closing the strategic gap between government and the private sector information security efforts

The private sector has developed strong capabilities to provide indications and warning of cyber attacks over information networks. The private sector is providing this information to other members of the private sector as well as the Federal government. However, we are unaware of any effort by the Federal government to use existing national intelligence means or law enforcement authorities to collect and share classified information about cyber threats to the critical infrastructure and to share such information, as appropriate with the private sector. Currently, the Federal government is focused on collecting and analyzing intelligence associated with threats against federally-owned and operated information systems supporting national defense capabilities. Unfortunately, government systems are likely not to be the only target. This represents a strategic gap in the public and private sector's capability to protect and defend against attacks. The Administration should move swiftly to address this gap in coordination with the private sector by creating the means to fuse information collected through classified means with the capabilities of the private sector.

Strengthen Information Sharing and Analysis Centers (ISACs)

Information Sharing and Analysis Centers (ISACs) allow private industry-specific business sectors to share security-related data. Each sector's ISAC gathers, analyzes and disseminates the data to members for an integrated view of information system vulnerabilities, threats and security incidents. ISACs also share best security practices and solutions among members. Directives from Presidents Clinton and Bush shaped the creation of ISACs which now exist for most sectors of the economy.

ISACs provide valuable information but their methodologies vary from sector to sector, which leads to uneven data and synthesis of security risks and solutions. Funding is also uneven as some ISACs are funded with federal money, some with private funds, and others with a mixture of federal and private resources. The second Bush Administration should adopt the findings of the President's National Information Assurance Council (NIAC) and boost its support for ISACs by increasing federal funding and normalizing operational processes for better cross-sector use of data.

Establish and test a survivable Emergency Coordination Network

The Internet has become crucial for transacting business in the private sector and is a vital part of communications for most Americans. Many government services also use the Internet. Unfortunately, the Internet has suffered regional blackouts and sluggish performance during cyber attacks so it is not a failsafe communications asset. There is no offline communications contingency plan by the private sector or by government to enable revival of the Internet during a prolonged outage. Current efforts by the Department of Homeland Security to establish a Homeland Security Information Network are not sufficient as the network will not survive a large-scale Internet disruption. The Administration should direct the creation of a survivable Emergency Coordination Network to facilitate revival and reconstitution of the Internet during a

large scale attack or disruption. The Administration should also direct an annual cyber security response, recovery, and reconstitution exercise involving key sectors of the economy, state and law enforcement authorities, and international partners, and support ongoing cyber exercises among ISACs. The response exercise should simulate cyber attacks from within and without the U.S. and include test recovery procedures and plans. The Bush Administration should also direct the National Institute of Standards and Technology (NIST) to coordinate improving the resilience of key Internet protocols to help minimize disruption of the Internet.

Direct a federal agency to track costs associated with cyber attacks

There is no national program or methodology for measuring the cost of cyber attacks. The primary measures of these costs are ad hoc pronouncements by analysts and industry experts published in newspapers. 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 much national efforts to improve cyber security are working. President Bush should direct the Department of Commerce or another agency to develop a methodology to measure the true cost of cyber attacks, and to track those associated costs as part of ongoing national economic assessment.

III

Education, Research and Development

As cyber security threats mount, the Bush Administration should ensure that federal appropriations meet related requirements for education, research and development, strengthen the federal security certification process to improve the quality of security in commercial software, and focusing on the vulnerabilities associated with digital control systems supporting critical infrastructure.

Increase R&D funding for cyber security

The effect on society of federally funded research and development has been enormous. For example, the Defense Advanced Research Projects Agency (DARPA) has been credited with up to half of all major innovations in computer science and technology. The National Research Council argues that information technology is the "control loop" of all critical national infrastructures, including energy, commerce, finance, telecommunications, food, transportation, health and social services, law enforcement, homeland and national security. The Council recommends five categories of R&D for better protecting this infrastructure: improved information and networking security; command, control, communications and information (C3I) for emergency response; information fusion; privacy and confidentiality; and planning for the future.

A recent Security Subcommittee meeting of the President's Information Technology Advisory Committee (PITAC), however, presented testimony by the Computing Research Association that documents shortcomings in achieving cyber security R&D recommendations by the Council. One is poor funding. The Department of Homeland Security (DHS) currently has an R&D budget of almost $1 billion, yet less than two percent goes to cyber security R&D. The Bush Administration should direct DHS to dramatically increase cyber security R&D and coordinate the production of a government-wide R&D agenda.

Related to funding is the matter of R&D policy. Currently, Department of Homeland Security cyber security R&D is focused on short term objectives; the agency says it relies on the National Science Foundation (NSF) and DARPA for long-range research. Appropriations for cyber security R&D at NSF, however, allow that agency to fund but a small fraction of proposed projects. Cyber security at DARPA is also focused on short-term deliverables, which frustrates creating and completing traditional long-range basic research. The second Bush administration should direct these agencies to allocate a bigger proportion of appropriations for the achievement of critical cyber security R&D – especially long range programs. The Administration must encourage a sustained commitment for protecting the nation's information infrastructure.

Fund authorized responsibilities for NIST Computer Security Division and White House Office of Management and Budget

The Computer Security Division in the National Institute of Standards and Technology (NIST) has long played a key role in the development of standards and guidelines for cyber security. NIST essentially brings together the details for implementing cyber security. Their traditional responsibilities were substantially increased by two laws passed in 2002: the Federal Information Security Management Act and the Cyber Security Research and Development Act.

Some of NIST's new responsibilities for cyber security include developing minimum security requirements for all government systems and finding improved ways to meet the security product testing needs of federal agencies, consumers and producers of information technology. NIST has also been tasked with running security research grants and fellowships programs, nether of which is funded. Other new responsibilities include developing a mandatory government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (see *Homeland Security Presidential Directive 12*), and developing security standards

and requirements for e-voting for the Elections Assistance Commission and its Technical Guidelines Development Committee.

We applaud the Bush Administration's proposal to increase NIST funding appropriations to fulfill previously authorized NIST obligations; however, the anticipated enhancements in '05 will only provide a fraction of the authorized appropriations level. We strongly urge to the Administration and Congress to ensure that NIST's Computer Security Division, in fact, receives funding commensurate with their important responsibilities. The White House Office of Management and Budget (OMB) also receives inadequate funding for properly executing its policy and oversight responsibilities under the Federal Information Security Management Act. Currently, only a handful of people with limited budget oversee FISMA at OMB. The second administration should ensure adequate staffing and appropriations for this critical responsibility.

Improve quality of software cyber security by strengthening NIAP certification

The National Information Assurance Partnership (NIAP) is a government initiative to meet cyber security testing needs of consumers and producers of information technology. NIAP is a collaboration of the National Institute of Standards and Technology and the National Security Agency. It oversees U.S. implementation of the international information technology security standards called Common Criteria – the essence of a certification program managed by NIAP. The intention of NIAP is to increase the level of trust in information technology systems and networks with cost-effective security testing, evaluation and validation programs. But comments by user and industry organizations, and other experts via the National Cyber Security Partnership have identified issues with NIAP certification that impede its intended goal of improving security in software. Common challenges for improving certification include reducing costs and increasing speed of the process; leveraging the process to address both private sector and government needs; fostering broader input from users and the industry; and ensuring federal procurement policy related to NIAP certification is understood and consistently applied. The next administration should direct NIST and NSA to address these challenges and promote the quality of cyber security in commercial software products and protect critical infrastructure.

Secure Digital Control Systems

Our nation's utilities including the electrical transmission grid, water, waste water and many critical manufacturing processes are controlled by digital control systems. These systems, sometimes referred to as Supervisory Control and Data Acquisition Devices (SCADA) – are designed to be open and interoperable and are vulnerable to attack. Such attacks could have "devastating consequences," endangering public health and safety, according to the GAO. During his second term the President should direct the formation of a task force with key government agencies, appropriate regulators, experts in the cyber security field, and representatives from utilities and suppliers to meet and recommend concrete actions to improve the security of control systems supporting critical infrastructure.

About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is an advocacy group to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. Launched in February 2004, the CSIA is the only public policy and advocacy group exclusively focused on cyber security policy. Members include BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc., Juniper Networks, Inc., McAfee, Inc., PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation, Symantec Corporation, and TechGuard Security, LLC.

Cyber Security Industry Alliance
1201 Pennsylvania Avenue, NW
Suite 300 #3011
Washington, DC 20004
202-204-0838
www.csialliance.org