CYBER SECURITY
INDUSTRY ALLIANCE

National Agenda for Information Security in 2006

Proposals by the
Cyber Security Industry Alliance

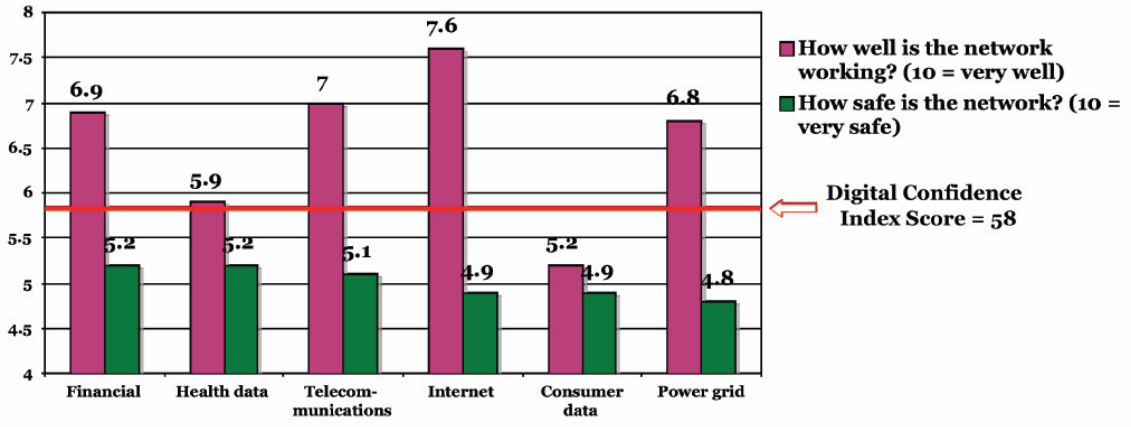
December 13, 2005

Ensuring the privacy, reliability and integrity of information has become one of the most pressing issues facing the global community. Cyber attacks and security breaches cost billions of dollars in direct losses, downtime, stolen identities and intellectual property. Misunderstanding or even neglect of information security can bring huge economic consequences. Consumers are already limiting their online activities for fear of identity theft. Businesses lose productivity needlessly due to downtime. And governments suffer from an inability to communicate effectively in times of crisis.

The massive data breaches in 2005, a barrage of security vulnerabilities and disruption in communications during Hurricane Katrina demonstrate the urgent need for improvement of the security and reliability of the information infrastructure. According to the Privacy Rights Clearinghouse, personal information from more than 50 million Americans has been exposed since the announcement of multiple security breaches from February through October of 2005. The CERT Coordination Center at Carnegie Mellon University reports that new security incidents rose more than 500% from 2000 to 2003, and the organization no longer tracks individual security incidents because automated tools have made attacks pervasive and non-stop. As for Katrina, the hurricane demonstrated the vulnerability of communications, and how overwhelmed civilian response assets required military intervention to bring order to chaos.

The Cyber Security Industry Alliance (CSIA) believes the status quo of minimal attention to information security creates an Achilles heel for the global community. Every American shares personal responsibility to secure information infrastructure under his or her own control. But government has a special role to lead, set priorities, coordinate, and facilitate improved information security protection and response. Last year CSIA proposed several actions for the U.S. government to improve cyber and information security. This document reviews progress on those initiatives. CSIA also identifies key new actions for the Administration and Congress to help improve the cyber and information security for consumers, businesses and government. A companion piece to this Agenda is research by CSIA and Pineda Consulting on consumer attitudes toward information security and the role of government. The graph below depicts the current national Digital Confidence Index of 58 – a low score that shows need for improvement. Details are in the CSIA report, *Internet Security National Survey II.*

Evaluating Confidence in the Nation's Digital Infrastructure



Source: CSIA & Pineda Consulting

The Year 2005 in Review

Last year CSIA encouraged Congress and the Administration to raise the profile of information security; improve information sharing, threat analysis, and contingency planning; and to prioritize and fund research and development. Progress was limited given the absence of strategic leadership and commitment. CSIA is encouraged by a decision to establish a dedicated post within the Department of Homeland Security to address cyber and telecommunications security. Unfortunately there is no forward momentum or clear set of priorities for action in 2006.

AGENDA 2005	ACTION	GOV'T GRADE
Establish a new cyber security post in the Department of Homeland Security	Secretary Chertoff announced creation of an Assistant Secretary for Cyber Security and Telecommunications; however this post has yet to be filled	C
Ratify the Council of Europe's Convention on Cyber Crime	Senate Foreign Relations Committee referred Convention to Senate for Ratification but no vote has been taken to date	B
Promote information security corporate governance in the private sector	Little to no action	D
Lead by example in federal procurement practices	OMB may establish a separate line of business for cyber security to promote more efficient and consistent security standards across government; and an interim rule under the Federal Acquisition Regulation requires agencies to plan for security and seek advice from security professionals, however enforcement is unclear .	C
Closing the strategic gap between the government and private sector information security efforts	The Federal government is too focused on collecting information relevant only to the security of national security systems; it must include data for the private sector to effectively improve information security	D
Strengthen information sharing	Little action by the Federal government while legal and organizational issues continue to cause uncertainly in the private sector – slowing information sharing mechanisms	D
Establish and test a survivable emergency coordination network	DHS established the Homeland Security Information Network-Critical Infrastructure (HSIN-CI), but the network is Internet-based and subject to outage.	C
Direct a federal agency to track costs associated with cyber attacks	Little action, though DHS is sponsoring limited economic analysis of the cost of cyber attacks and Justice has initiated a survey on the costs to business of attacks	D
Increase R&D funding for cyber security	Despite a presidential panel that declared a crisis in cyber security R&D, funding remains flat and clear priorities absent	D
Fund authorized responsibilities for NIST and OMB	Appropriated funding does not cover statutory responsibilities for cyber security by these agencies	D
Improve the quality of software cyber security by strengthening NIAP Certification	A study by DoD and DHS on the effectiveness of NIAP was not shared with the public, so no data is available to show how NIAP certification improves information assurance	F
Secure Digital Control Systems	DoE and DHS are creating a roadmap to secure energy controls and are funding digital control systems testbeds	C

Looking Forward — National Agenda for 2006

CSIA urges the President, the Administration, and Congress to enhance the nation's information security and reliability by enacting the following National Agenda for 2006. The federal government can take several steps that will improve information security for consumers, industry, and the government itself. We included some items from last year's agenda that we believe are critical to complete next year. We have also included several important new initiatives. CSIA looks forward to working with Congress and the Administration to accomplish these initiatives.

The recommendations are in three categories: The first addresses privacy and security of consumers' data. The second focuses on enhancing the security and resiliency of information infrastructure such as for healthcare and communications systems. The last includes programs by the Federal government in information assurance, including the appointment of an Assistant Secretary for Cyber Security.

I

Privacy & Security for Consumers

II

Security & Resiliency of Information Infrastructure

III

Federal Information Assurance Initiatives

I

Privacy & Security for Consumers

Consumers are nearly unanimous in their fear of identity theft and spyware, according to survey research conducted by CSIA. About 97 percent of consumers rate identity theft as a serious problem, while 93 percent say spyware is a serious problem, according to the research. About 48 percent say they avoid making purchases on the Internet because they are afraid their financial information may be stolen. Overall, CSIA research finds that 71 percent of consumers believe new laws are needed to protect consumer privacy on the Internet. Toward that end, CSIA urges Congress pass laws to ensure the security citizens' sensitive personal information and to protect consumers from spyware.

Pass a National Data Breach Notification Bill

A firestorm of reaction to dozens of recent breaches of security at data brokers, financial institutions, retailers, universities, and other entities that have large databases filled with personally identifiable information has resulted in calls for regulating the storage and processing of sensitive information. Twelve bills in Congress propose new legislation for protecting consumer privacy, reducing identity theft, and ensuring the safekeeping of individually identifiable information. In addition, security breach legislation was introduced in at least 35 states and adopted in at least 22. Multiple laws requiring potentially different requirements will quickly make compliance an overly complex task. It is time for Congress to establish a comprehensive national Data Breach Notification bill. The primary objectives of national legislation are to simplify and improve consumer privacy and identity protection, and to help consumers feel confident in their safe use of online commerce. The bill should establish a strong national data breach notification standard and enable state attorney generals to prosecute the Federal law with notification to the U.S. Attorney General. A properly crafted statute from Congress may alleviate much concern and consternation within the industry and the public as a whole. CSIA urges passage of a national bill during 2006. The bill should require organizations processing personal information to regularly identify and mitigate security vulnerabilities through appropriate policies, procedures, and technologies. The bill should also promote best practices such as encryption, without mandating specific technologies. We believe a final bill should not be limited to data brokers, should use existing applicable federal law, enable federal pre-emption, should foster and provide incentives of the adoption of reasonable security practices, define "breach," and establish the Federal Trade Commission as the authority to oversee breach notification.

Pass a National Spyware Protection Bill

Spyware has become more than an online nuisance. Now it is discouraging use of e-commerce. Many people feel as if they have lost control of their PCs and are trapped in a cyclical battle against programs that install themselves without warning, exploit security holes, and reinstall themselves after being deleted. Malicious programs allow online crooks to hijack Americans' sensitive personal information at will. Even benign malware can slow computers to a crawl by wasting processing power on unwanted "services." Spyware purveyors frequently use opaque "bundling" arrangements and other cons to spread their unwanted payloads. There is a big need to improve consumer confidence in e-commerce and use of the Internet with a coordinated defense against unwanted programs. Several proposed Congressional bills address spyware issues. CSIA supports passage of a national Spyware Protection Bill during 2006 with a "Safe Harbor" provision, which will protect anti-spyware vendors from frivolous lawsuits for removing spyware that is believed in good faith to violate the law. CSIA has joined with organizations supporting legislation for spyware protection such as the Business Software Alliance, Center for Democracy and Technology, and the AntiSpyware Coalition. The latter is a group building an industry and consumer advocate consensus about definitions and best practices for spyware and other potentially unwanted technologies.

II

Security & Resiliency of Information Infrastructure

The information infrastructure is a technical ecosystem of networks, computers, applications and digital information. It includes control systems for the nation's entire critical infrastructure – and our citizens' most critical data, such as health records and financial data. While the vast majority of information infrastructure is owned and operated by the private sector, the government plays a critical role in promoting security and resiliency across the cyber infrastructure. An important national priority is protecting information infrastructure for healthcare. There is also a pressing need to better understand the costs associated with cyber attacks. Stronger cyber protection is needed for Digital Control Systems used to operate critical infrastructure. Finally, closer cooperation should be established between the private sector and agencies responsible for certifying information security products purchased by the federal government.

Ensure Cyber Security Protection be Applied to Healthcare Infrastructure

CSIA welcomes President Bush's initiative to provide all Americans access to electronic health records within the next ten years. Technology enabling this access will also improve the quality of healthcare, save billions of dollars for providers and reduce the cost of healthcare for all Americans. Hospitals using electronic prescription systems have already cut prescription errors by up to 80 percent. Quality-of-care measurement systems used by Medicare in hundreds of hospitals are showing improvements of about six percent. The Department of Health and Human Services (HHS) conservatively estimates savings from technology will reach $140 billion a year by 2014 – about six percent of healthcare spending in that year. Healthcare accounts for about 15 percent of the U.S. economy so these gains will have significant impact on the overall economy.

Cyber security is a major priority for enabling electronic healthcare systems. Personally identifiable healthcare information must be protected from all unauthorized access. Equally important is the integrity of health records – they must be assured and available immediately for urgent medical procedures. CSIA urges Congress and HHS to ensure cyber security protection be applied to healthcare infrastructure. Toward that end, they should establish national policy for security and privacy of electronic health records; create or adopt upfront security and privacy standards for healthcare IT; and integrate security and privacy with Standards Harmonization Process. In this context, CSIA believes a security and privacy expert should be added American Health Information Community.

Promote Information Security Governance in the Private Sector

Information assurance in the private sector is critical to creating a more secure infrastructure. While many organizations have taken steps to implement policies, best practices and technology to secure their infrastructure, more can and should be done. The federal government should encourage the private sector to apply information security governance to business operations. Little was done toward this requirement during 2005. The Administration should lend additional support to efforts by the Departments of Commerce and Homeland Security raising awareness of 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. That effort must 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 raise the awareness of cyber security in the business community. The Department of Commerce may wish to model some of this effort after work done by the Business Roundtable and the Center for Internet Security.

Direct a Federal Agency to Track Costs Associated with Cyber Attacks

There is no national program or methodology for measuring the cost of information security attacks. The primary measures of these costs are ad hoc pronouncements by analysts and industry experts published in newspapers. Some private sector studies are underway, such as by VISA International. However, 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. CSIA commends the Departments of Justice and Homeland Security for commencing the first-ever effort to create national estimates of prevalence and cost of cyber security incidents for business. The National Computer Security Survey will be administered in early 2006. CSIA urges the Administration to direct a Federal agency to use data from this survey as a baseline for ongoing measurement. The real objective is to develop a methodology that measure the true cost of cyber attacks, and to track those associated costs as part of ongoing national economic assessment.

Secure Digital Control Systems for Physical Infrastructure

Our nation relies on a digitally controlled utility and commercial infrastructure such as the electrical transmission grid, oil and natural gas, water, waste water, chemicals, telecommunications, transportation, banking and finance – and many critical manufacturing processes. Remote control of distributed critical infrastructure occurs with Supervisory Control and Data Acquisition (SCADA) systems. These systems are designed to be open and interoperable; but their increasing use of the Internet for communications makes them vulnerable to cyber attack. Such attacks could have devastating consequences such as endangering public health and safety, according to the Government Accounting Office. Some progress has been made during the past year. The Energy Policy Act of 2005 includes specific provisions requiring information security for the nation's power grid. Private sector efforts are also helping to strengthen SCADA security, such as the American Chemistry Council's Responsible Care Code. CSIA commends collaboration by the Department of Homeland Security and the Department of Energy on creating a roadmap to secure SCADA systems for the energy sector. CSIA also commends the Department of Energy for creating SCADA test beds at Idaho National Laboratories and Sandia National Laboratories. But much work remains to properly secure all sectors' critical infrastructure from cyber attacks. CSIA urges President Bush to form a task force of 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.

Improve Quality of Software Cyber Security by Strengthening NIAP Certification

The National Information Assurance Partnership (NIAP) is a government program to test the assurance of information technology products deployed in secure government systems. 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. These 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 the absence of metrics to measure how the programs improves assurance. DoD and DHS recently completed a study on the effectiveness of NIAP but the findings and recommendations have not been released. The complete study should be released to the public. The reformed NIAP must move beyond being a "check box" in the federal purchasing process. NIAP must demonstrate quantifiable benefits for its more stringent levels of assurance requirements.

III

Federal Information Assurance Initiatives

The federal government plays a critical role in shepherding national initiatives for stronger information security. The Department of Homeland Security is a key driver for federal information security; it needs to swiftly appoint a person who can lead its cyber security initiatives. As witnessed by recent natural disasters, the DHS must also establish emergency communications, continuity of operations and reconstitution programs that work no matter what disaster might take place. On the legal front, the Senate should ratify the Council of Europe's Convention on Cybercrime to strengthen our nation's ability to globally combat cyber crime. Since the federal government is also the driver of scientific research and development, it should increase R&D funding for cyber security. CSIA commends the Office of Management and Budget for encouraging implementation of a new common authentication standard for physical and logical access to federal facilities and systems by federal employees and contractors – Homeland Security Presidential Directive/HSPD-12. CSIA urges agencies to meet the directive's deadline in October 2006. CSIA also urges the Administration and Congress to ensure appropriate funding is available for agencies to fully implement the directive. Finally, the government should step up implementation of telework programs to help ensure continuity of operations in the event of a disaster.

Fill New Cyber Security Post in Department of Homeland Security

CSIA commends Homeland Security Secretary Michael Chertoff and the Department of Homeland Security (DHS) for their decision in July to create an Assistant Secretary for Cyber Security and Telecommunications. CSIA also commends Congress, especially the House Committee on Homeland Security, for its continued attention to cyber security issues and the role it has played in helping to reach this important milestone. Critical information infrastructure underpins our economy and national security. Enabling DHS to focus attention on cyber security will help address urgent requirements for research and development, public-private collaboration, and implementation of cyber security technologies and best practices. The new Assistant Secretary position, however, remains vacant. Swiftly filling the position with a qualified expert is a top priority for early 2006. CSIA urges Secretary Chertoff and the new Assistant Secretary to execute on the following priorities:

Establish emergency communications. Vulnerability-resistant communication systems and procedures must be in place for nationally-coordinated response to disasters such as a hurricane or terrorist attack.

Continuity of operations. DHS should steer appropriate planning and resources to enable continuity of critical information operations during a large scale disruption of the information infrastructure, such as that following Hurricane Katrina. Clearly defined roles and responsibilities and procedures are critical.

Reconstitution programs. DHS, in coordination with other agencies, must be able to lead the reconstitution of information infrastructure in the government and private sector to ensure social order, safety, health, and economic stability.

Presidential Directive on Roles and Responsibilities. CSIA urges the President to issue a directive setting national policy and procedures to assure the security of critical U.S. information technology and telecommunications infrastructures. The directive should address roles and responsibilities during an incident of national significance, including the role of the Department of Defense.

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 a new type of criminal act called cybercrime. The Council of Europe engineered the Convention on Cybercrime to promote a common, cooperative approach to prosecuting people who commit cybercrime. Examples of computer network-based crime include fraud, identity theft, hacking, and child exploitation. The U.S. signed the Convention on November 23, 2001; it was conveyed to the

Senate on November 17, 2003. During 2005, the Senate Foreign Relations Committee passed the Convention to the floor for a vote. CSIA commends Chairman Richard G. Lugar (R-IN), Ranking Member Joseph R. Biden, Jr. (D-DE), and the Committee for taking this action. Unfortunately, the Senate has not acted on this vote. CSIA urges the Senate to review and ratify the Convention as quickly as possible. CSIA leads a coalition of 12 industry associations supporting ratification. Ratification will provide 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.

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. Nevertheless, the 2005 track record for federal funding of cyber security R&D was poor.

The President's Information Technology Advisory Committee (PITAC) recommended in March substantial increases in funding at the National Science Foundation, Department of Homeland Security, and the Defense Advanced Research Projects Agency. The call came, in part, because funding for R&D at NSF and the National Institute of Science & Technology has been well below levels authorized in the Cyber Security Research and Development Act. PITAC was subsequently disbanded, although it was announced that its activity would be subsumed into the President's Council of Advisors on Science and Technology (PCAST). Similar calls for funding have been echoed by a broad range of private sector organizations but to no avail. The DHS currently has an R&D budget of almost $1 billion, yet less than two percent goes to cyber security R&D. In Fiscal Year 2006, the DHS Science and Technology Directorate requested $16.7 million for cyber security R&D programs – a seven percent decrease from FY2005. At NSF, funding for cyber security research during FY2005 was just $65 million. At NIST, total funding for the Computer Security Division was just $19 million during FY05.

CSIA urges the Administration to dramatically increase cyber security R&D and coordinate the production of a government-wide R&D agenda. Development of a prioritized national policy for cyber security R&D is crucial. Most projects are currently focused on short-term objectives so CSIA recommends the Administration to direct DHS, NSF and DARPA 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.

Complete HSPD-12 Initiative for Government Wide Authentication

CSIA commends the Office of Management and Budget for encouraging implementation of a new common authentication standard for physical and logical access to facilities and information systems by federal employees and contractors – Homeland Security Presidential Directive/HSPD-12, signed on Aug. 27, 2004 by President Bush. This directive aims to eliminate risks of unauthorized access to secure Federal and other facilities where there is the potential for terrorist attacks. It mandates a government-wide standard for secure and reliable forms of identification issued by the federal government. Stronger digital authentication will significantly improve information sharing and security in the federal government. Testing is currently in process to verify technical performance of new smart card IDs. Smart cards must comply by October 27, 2006 with technical standards from the National Institute of Standards and Technology. CSIA urges agencies to meet the directive's deadline. CSIA also urges OMB and Congress to ensure appropriate funding is available to help agencies bear the costs of testing and implementation. CSIA urges agencies to develop an

infrastructure that can use smart cards for authentication and physical access to facilities and for logical access to computer and communications systems.

Ensure Continuity of Government Operations with Telework

Telework provides flexibility in the locations where employees may perform their jobs. Some call it telecommuting, flexiwork, flexiplace, or enabling a remote work force. Telework lets employees work at home, at an alternate office closer to home, or at other defined locations. The idea is popular and widely used in private industry because it is a valued employee benefit, saves organizations money through higher productivity and reduces overhead. Adoption of telework in the federal government began in 1990 and is on the upswing, but the level seriously lags private industry. CSIA urges the federal government to quickly step up use of telework – not only for the obvious financial and organizational benefits – but to facilitate continuity of operations (COOP) in times of crisis. CSIA encourages the Administration to call out telework in the President's Management Agenda. The Office of Management and Budget should ensure that all agencies include telework plans in COOP. Agency heads and their executives should provide a clear, forceful and sincere endorsement of telework to facilitate acceptance and implementation of telework mid-level managers. The Administration should also urge adoption of telework by state and local governments to help assure continuity of their respective operations during times of crisis.

Include Information Security Planning in Transition to IPv6

Federal agencies are currently poised to begin transitioning the Federal Enterprise Architecture from Internet Protocol version 4 to IPv6. The long-needed shift is required to solve the limited address space within IPv4, and to gain advanced functionality such as Quality of Service (QoS), stronger security, mobility, auto configuration and extension headers. This transition will affect every information system that uses IP – virtually everything used by the government and its contractors. CSIA commends the Office of the Secretary of Defense and the Office of Management and Budget for starting this transition. IPv6 promises stronger security but agencies must carefully plan its implementation. Otherwise, information systems using IPv6 may be subject to exploitation by unauthorized parties, resulting in increased risk of exposure for critical systems and higher costs for cyber security. CSIA urges these departments to study and implement new best practices for the IPv6 transition related to information security, which were released this month at the IPv6 Summit. CSIA also recommends agencies follow recommendations by the Government Accounting Office published in May, "Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks."

About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. The organization is led by CEOs from the world's top security providers, who offer the technical expertise, depth and focus to encourage a better understanding of security issues. It is the belief of the CSIA that a comprehensive approach to ensuring the security of information systems is fundamental to global protection and economic stability. Members of the CSIA include Application Security, Inc.; BindView Corp. (NASDAQ: BVEW); CA (NYSE: CA); Check Point Software Technologies Ltd. (NASDAQ: CHKP); Citadel Security Software Inc. (NASDAQ: CDSS); Citrix Systems, Inc. (NASDAQ: CTXS); Entrust, Inc. (NASDAQ: ENTU); Internet Security Systems Inc. (NASDAQ: ISSX); iPass Inc. (NASDAQ: IPAS); Juniper Networks, Inc. (NASDAQ: JNPR); McAfee, Inc. (NYSE: MFE); PGP Corporation; Qualys, Inc.; RSA Security Inc. (NASDAQ: RSAS); Secure Computing Corporation (NASDAQ: SCUR), Surety, Inc.; Symantec Corporation (NASDAQ: SYMC); TechGuard Security, LLC; Visa International; and Vontu, Inc.

Cyber Security Industry Alliance
2020 North 14th Street, Suite 750 • Arlington, VA 22201 • (703) 894-CSIA • www.csialliance.org