Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

What is the Federal Government Doing to Improve the State of Information Security?

The United States government sees a clear and present danger in cyber terrorism and cyber crime and is taking decisive action to improve the state of information security in the United States. The pieces to the overall plan include presidential directives and policies, legislative acts, executive agencies, special programs, and agreements with other nations. Some of the major themes are government-industry partnerships, cooperation with law enforcement abroad, Government sponsored research, developing a larger cadre of...

Copyright SANS Institute
Author Retains Full Rights

AD

Jason Hiney
GSEC Practical Version 1.4b Option 1

What is the Federal Government Doing to Improve the State of Information Security?

People often complain that the Government is slow in acting and reacting or joke about the $300 toilet seat or the $200 hammer. In some cases such charges appear to be valid. However, it seems that Uncle Sam sees a clear and present danger in cyber terrorism and cyber crime and is taking decisive action to improve the state of information security in the United States. The pieces to the overall plan include presidential directives and policies, legislative acts, executive agencies, special programs, and agreements with other nations. Some of the major themes are government-industry partnerships, cooperation with law enforcement abroad, Government sponsored research, developing a larger cadre of information technology professionals, empowering the individual, and protecting the right to privacy. Information security is crucial to protecting our economy and national infrastructure since most critical infrastructure sectors rely on data networks and computer systems for data input and communications. Indeed, many of these sectors are linked together by data networks, and a single hacker penetration could bring several of them down at once. The objective of this paper is to take a broad look at recent Government actions improve the state of information security in the United States and prevent such problems.

The executive branch has provided and continues to provide most of the leadership and focus on improving the state of information security in the United States. Presidents Clinton and George W. Bush and the President's Critical Infrastructure Protection Board (PCIPB) are responsible for the overall strategies and policies. Many new programs and executive offices have been established in recent years to place the strategies and policies into effect. Some of the new offices and programs are the Department of Homeland Security (DHS), the Total Information Awareness Project (TIAP), the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Awareness Office (CIAO), the National Infrastructure Simulation and Analysis Center (NISAC), the Federal Computer Incident Response Center (FedCIRC), and the Secret Service Electronic Crimes Special Agent Program (SSECSAP). Other executive offices like the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), the Department of Justice (DOJ), the Office of Science and Technology Policy (OSTP), the National Communication System (NCS) and the Defense Advanced Research Projects Agency (DARPA) predate the concerns of cyber crime and cyber terrorism but have adapted their missions to address the new threat.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

In 1997 President Clinton established the President's Commission on Critical Infrastructure to report on critical infrastructure vulnerabilities. The foremost concern was that the infrastructure might be vulnerable to attack through the information systems that now interconnected and controlled them. The report led to presidential decision directive 63 (executive order 13110), which was given in May of 1998. PDD 63 is the basis for many of the strategies, polices, plans, projects, partnerships and offices in place today. For example, PDD 63 directs the establishment of Information Sharing and Analysis Centers (ISAC) to encourage public-private cooperation in protecting eight defined sectors of the national critical infrastructure. The ISACs are up and functional today and include sub-ISACs where appropriate. Each of the ISACs provides a forum for discussion of sector wide problems and solutions. The ISACs also provide staff personnel to analyze input data from members, CERT, NIPC, and private organizations and disseminate an integrated and tailored view of vulnerabilities, threats and incidents (Allor). The PDD also identifies a lead federal agency for each sector and directs the lead agency and industry liaison for each sector to contribute to a sectoral National Infrastructure Assurance Plan (NIAP). The contribution must include an assessment of vulnerabilities, recommendations to eliminate these vulnerabilities, a proposal for identifying and preventing attacks, development of a plan for containing an attack and restoring essential capabilities, and implementation of a vulnerability awareness and education program for the sector.

PDD 63 commits the federal government to research, development and procurement towards increasingly capable methods of infrastructure protection and sets forth that the Government is to serve as a model to the private sector on infrastructure protection. It calls for cooperation between the federal government, the private sector and local agencies and for market forces to be the primary means in encouraging infrastructure security. The PDD establishes a Critical Infrastructure Coordination Group composed of representatives from the lead federal agencies to coordinate the implementation of policies laid out in the directive. It also creates the National Infrastructure Awareness Council to enhance the partnership between the public and private sectors. The PDD directs each federal agency to protect its critical infrastructure with an emphasis on cyber-based systems. Each agency must appoint a Chief Information Assurance Officer, who is responsible for critical infrastructure protection and vulnerability assessments. The PDD states that the NIAP shall include a vulnerability analysis and remedial plan and addresses issues such as a warning center, a response system, reconstitution, education & awareness, research and development, intelligence, international cooperation and legislative and budgetary requirements. Finally, it authorizes the FBI to expand the NIPC as part of a national warning and information sharing system.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

PDD 63 states that the United States must have an initial operating capability to protect the nation's infrastructure by the year 2000. The National Plan for Information Systems Protection fulfilled that requirement when it was published in January 2000. The plan proposes programs to accomplish the following:

- Identify critical infrastructure assets and shared interdependencies and address vulnerabilities
- Detect attacks and unauthorized intrusions
- Develop robust intelligence and law enforcement capabilities
- Share attack warnings and information in a timely manner
- Create capabilities for response and recovery
- Enhance research and development
- Train and employ adequate numbers of information security specialists
- Make Americans aware of the need for improved cyber security
- Adopt legislation and appropriations in support of above
- Ensure civil liberties and the right to privacy in each program

President George W. Bush's executive order 13231 of October 2001 also builds upon the foundation established by PDD 63. It creates the President's Critical Infrastructure Protection Board (PCIPB) to coordinate programs that protect federal agency critical infrastructures or establish information sharing capabilities between the Government, state and local governments, private industry, and academia. The order gives the PCIPB the additional duties of incident handling and crisis response, developing strategies for recruiting and training executive branch security professionals, coordinating with the OSTP on research and development, coordinating international infrastructure protection, providing legislative advice, and coordinating with the Office of Homeland Security. The order also establishes the National Infrastructure Advisory Council to advise the president on security of information systems supporting the banking and finance, transportation, energy, manufacturing, and emergency government services infrastructures.

The latest guidance from the White House on cyber security is the National Policy to Secure Cyberspace. The policy seeks to engage home, small business, large enterprise, federal government, state and local government, higher education, and industry sector users in securing the collective information infrastructure by each user securing his or her individual piece of the whole. To that end, it recommends specified actions for each user level. The plan includes strategies from industry sectors and input from individuals and provides instruction to federal agencies that have roles in cyber security. It further explains that the private sector is best suited to addressing information security threats and that the Government plans to take action only in certain areas where private industry does not have adequate resources or interest. Thus, the federal government would still be responsible for activities such as forensics and attacker identification, protection of networks essential to national security,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

protection against organized attacks capable of inflicting massive damage to the economy, and long term research and development. The policy outlines five critical priorities for cyberspace security. These are a national response system, a national cyberspace security threat and vulnerability reduction program, a national cyberspace security awareness and training program, securing Government's cyberspace, and national security and international cyberspace security cooperation.

President Bush is following up on the proposed plans and strategies to protect the critical infrastructure and improve the state of information security by making appropriate budget requests to Congress. Page 9 of the National Strategy to Secure Cyberspace states, "For fiscal year 2003, President Bush requested that Congress increase funds to secure federal computers by 64 percent." The Bush Administration is also proposing a 56 percent increase for cyber security funding in fiscal year 2003 and a 12 percent increase on top of that increase for fiscal year 2004 (Miller).

One can see that the executive policy and strategy to date is logical and comprehensive. But what is happening to improve the state of information security at the next level, the executive branch offices and programs that implement the directives? These offices and programs fall into the general mission areas of critical infrastructure protection, research and development, policing the public networks, education and training and information sharing.

Until November 2002 there were five independent agencies managing critical infrastructure protection. The functions of these offices have been transferred to the Department of Homeland Security (DHS) under Title II of the Homeland Security Act. The first of these agencies, the FBI/DHS National Infrastructure Protection Center (NIPC), serves "as the U.S. government's focal point for threat assessment, warning, investigation and response..." (Plehal). It provides law enforcement and intelligence information to other federal agencies, state and local governments, and the ISACs. NIPC issues threat warnings and guidance on protection measures and sponsors Infragard, a cooperative effort between government, businesses, academia, state and local law enforcement and others to exchange information and ideas and increase the security of the critical infrastructure (http://www.nipc.gov/). Infragard uses a secure web site to share information about hacking attempts. Paul Nowell of the Associated Press gives the following detail about Infragard:

> A key feature of the system is a two-pronged method of reporting attacks. A "sanitized" description of a hacking attempt or other incident-one that doesn't reveal the name or sensitive information about the victim-can be shared with the other members to spot trends. Then a more detailed description also can be sent to the FBI's computer crimes unit to determine if there are grounds for an investigation.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Department of Defense (DoD)/DHS National Communication System conducts secure network research and provides emergency voice communications between telecommunications providers and the Government if the public switched telephone network goes down. It also facilitates the restoration of national security preparedness telecommunications and runs the SHARES high frequency radio backup communications system in support of government and industry (http://www.ncs.gov/NCS/HTML/NCSProjects.html).
The Department of Commerce/DHS Critical Infrastructure Assurance Office (CIAO) is responsible for coordinating and implementing the federal government's initiative on critical infrastructure protection. The CIAO assess the Government's risk exposure and dependencies on the critical infrastructure, educates the public to raise participation in infrastructure protection, and coordinates legislative and public affairs to achieve assurance objectives (http://www.ciao.gov/publicaffairs/about.html).

The Department of Energy/DHS has a piece of the action as well. Its National Infrastructure Simulation and Analysis Center (NISAC) provides a modeling and simulation capability for analyzing critical infrastructure interdependencies and vulnerabilities to include cyber security. FedCIRC also manages critical infrastructure protection activities but is a little different in that it supports only the federal government infrastructure. The "About FedCIRC" web page (http://www.fedcirc.gov) states, "FedCIRC provides a central focal point for incident reporting, handling, prevention and recognition." Other major functions include providing alert and advisory information and tools to include centralized software patch management.

Agencies and programs responsible for research and development in support of information security include the National Science Foundation (NSF), the Office of Science & Technology Policy (OSTP), Defense Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology (NIST). The NSF supports information security research through grants, contracts and fellowships. Current areas of interest include privacy, data mining and physical layer security. The OSTP advises the president on the impacts of science and technology on domestic and international affairs and coordinates research and development to support critical infrastructure protection strategy. In addition, it leads an interagency effort to develop and implement sound science and technology policies and budgets and to work with the private sector, state and local governments, education communities and other nations to this end (http://www.ostp.gov/html/_aboutostp.html). DARPA conducts research and development focused primarily towards military applications and basic computer and network technology, but some of the technologies are applicable to information security. Some examples include information assurance technologies and biometrics.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Then there is NIST, the mother of all research and development agencies. NIST falls in not only the research and development mission area but also in the education and training and information sharing mission areas. According to the NIST web site (http://www.nist.gov/public_affairs/general2.htm), its mission is "to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life." In the specific area of information security, NIST identifies vulnerabilities and cost effective solutions and sets security standards for sensitive federal systems. These standards are often used as a model for private industry systems as well. NIST develops measurement methods, tests and validation programs for information security. It sponsored an international competition on the advanced encryption standard and hosts a web site providing information security advisories, bulletins, standards, guidelines, and announcements. NIST maintains cryptographic standards and validates new ones. It maintains a list of anti-virus resources, vendors and recommendations (http://www.nist.gov/public_affairs/computers.htm). The Computer Security Division of NIST maintains the ICAT Metabase, a vulnerability search engine that links users into a variety of publicly available vulnerability databases and patch sites.

The responsibility of policing the Internet is shared by the FBI, the CIA, the Defense Intelligence Agency, the Secret Service, the National Security Agency, local law enforcement and many other agencies. The list now includes the Department of Homeland Security. The FBI, the Secret Service and the military have publicized special programs to combat cyber crime. The other federal agencies are sure to have similar but more secretive programs. The FBI's special program is called the Computer Analysis Response Team (CART). CART provides assistance to FBI field offices in search & seizure of computer evidence as well as forensic examinations. In 1999 CART conducted 2400 examinations of computer evidence. The CART is now working on a project called the Automated Computer Examination System (ACES). ACES will conduct many routine examinations in a self-documenting, automated method (http://www.fbi.gov/hq/lab/org/cart.htm).

The Secret Service has two special programs called the Electronic Crimes Branch (ECB) and the Electronic Crimes Special Agent Program (ECSAP). The ECB provides forensic analysis of electronic storage devices such as hard drives, provides training for law enforcement and private industry, conducts research and development, and provides technical support to Secret Service investigations. The ECSAP consists of over one hundred and seventy five agents trained in forensic analysis and handling of electronic evidence deployed to Secret Service offices around the country. ECSAP personnel are available to assist local law enforcement personnel in conducting investigations involving all types of electronic evidence.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The DOD has a controversial new program called the Total Information Awareness (TIA) Project. The idea behind TIA is to mine databases and the Internet to detect terrorist plots. It has generated a lot of public concern about privacy rights.

Policing the public networks also requires cooperation with other countries since the Internet has no national boundaries. The Departments of State and Justice are working to establish information sharing and extradition arrangements even as this paper is being written. The Cybercrime Treaty is the current avenue of approach to achieve such arrangements. Under the Cybercrime Treaty member countries must criminalize hacking, production or distribution of hacking tools and child pornography. The treaty also requires expansion of criminal liability for intellectual property violations. It requires that member country Internet service providers preserve Internet usage records and grants power to monitor online activities in real time. In addition, the treaty requires cooperation with mutual assistance requests from other member countries (http://www.ala.org/alaorg/oif/cybercrimetreaty.html). The treaty was opened for signatures in November of 2001. Approximately thirty-three nations including the US have signed so far, but action is required by each national parliament before the respective nation can ratify and be bound by the Treaty. The treaty will go into effect when it is ratified by five nations, three of which must be Council of Europe (COE) members. As of February 2003, two COE members have ratified the treaty. When the treaty goes into effect, the US, a non-COE nation, can apply for admission. (http://www.treatywatch.org/TreatyStatus.html).

Law enforcement is having notable success in policing the networks and apprehending cyber criminals. One example is the recent arrest of virus distributor Simon Vallor in Britain in which the FBI provided information that led to prosecution under British law. Another example is the arrest of software time bomber Tim Lloyd. Then there is the conviction of Kevin Mitnik. The National Association of Defense Lawyers (NADL) has even complained that cyber criminals get stiffer sentences than criminals who commit similar crimes without computers. Since the NADL is making this complaint, law enforcement and the courts must be crimping someone's style. A good place to look at current high profile cases is the NIPC Major Investigations page.

The information sharing mission of the executive branch is split across many offices. This distributed organization is evident in the PDD 63 assignment of responsibilities where eight different executive departments have responsibilities for the eight sectors of critical infrastructure. The eight lead agencies are then responsible to set up Information Sharing and Analysis Centers in each of the infrastructure sectors. Recently this distributed arrangement has been centralized somewhat by establishment of the Department of Homeland Security (DHS). Critical infrastructure protection functions (to include information sharing) of the Departments of Commerce, Justice and Energy have been rolled into DHS. The core reasoning behind the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

establishment of DHS is that combining multiple agencies into one office should improve data sharing and focus the component agencies towards one goal. The DHS works with the other federal agencies, state and local governments and the private sector to harden the critical infrastructure.

Other agencies with primary roles in information sharing include the Department of Justice (DOJ), the General Services Administration GSA) and DoD. The DOJ Computer Crime & Intellectual Property Section provides information on cyber crime legal issues, instructions on how to report and fight cyber crime and training for state and local law enforcement. Through the FBI the DOJ also partners with the SysAdmin, Audit, Networking and Security Institute to present the SANS/FBI Top 20 Vulnerabilities List. This list contains information for fixing the ten most commonly exploited services in Windows and the ten most commonly exploited services in Unix. It is designed primarily to assist organizations without full time computer security professionals. The idea behind the list is that hackers exploit these top twenty vulnerabilities the most, and therefore, eliminating them will solve the majority of computer security breaches. GSA contributes by funding the Common Vulnerabilities and Exposures (CVE) Dictionary, a dictionary that points to other vulnerability databases. The CVE Dictionary provides industry standard names for vulnerabilities and exposures. The DoD contributes to the information sharing mission by funding the CERT Coordination Center (CERT/CC) and the Networked System Survivability Program (NSSP). CERT/CC publishes security alerts and research and development information, handles computer security incidents and develops training to improve information security (http://www.cert.org). Like CERT/CC, NSSP is a branch of the Carnegie Mellon Software Engineering Institute. NSSP incorporates the experience of CERT/CC to distribute security practices and information security evaluation methods and conduct training (http://www.sei.cmu.edu/programs/nss).

The executive is also making progress on the training and education front of our unfriendly little cyber war. One of the latest developments is the Security Plus Certification Program, an entry level certification program for computer professionals. It could become a minimum standard that would help Government and companies hire proficient network administrators. The Program seems to have its origin in the need for more security training and better ways to certify knowledge presented in the National Plan for Information Systems Protection and the National Strategy to Secure Cyberspace. The Security Plus Program is a product of the Computing Technology Industry Association, which is made up of representatives from the FBI, the Secret Service, NIST, IBM, Microsoft, Sun Microsystems, Verisign, Novell, and other companies (Lemos [2]).

In addition to developing the certification program, the Government is expanding the Scholarship for Service program, which provides scholarships in information security in exchange for one or two years of service in federal agencies upon graduation. The National Science Foundation runs the program,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and the funding comes from the fiscal year 2002 supplemental appropriations bill. Enrollment in the program is expected to double to about three hundred students. The end result will be improved information security in the federal agencies receiving these graduates.

The Congress has done its part towards improved information security by enacting numerous laws relating to cyber crime and cyber terrorism. For example, the Computer Fraud and Abuse Act of 1996 amends the 1986 version of the bill by the same name, which was the legislative branch's first major attempt at cyber crime law. The act prescribes a fine and up to twenty years in jail for unauthorized access to federal government or financial institution computers, unauthorized access to computers used in interstate or foreign commerce or communications and password trafficking that affects interstate commerce. The act gives the Secret Service overall jurisdiction for offenses under the act, but it also gives the FBI jurisdiction in cases of espionage, foreign counterintelligence, national defense or foreign relations. So the Computer Fraud and Abuse Act covers a lot of bases, but what about computers not owned by the Government and not used by a financial institution?

The Economic Espionage Act of 1996 prohibits knowingly taking, concealing, copying, transmitting, altering, destroying, receiving or possessing trade secrets with the intent of benefiting a foreign government. The penalty is up to $500,000 and 15 years in prison or $10,000,000 for an organization. The Act has a similar "trade secret" provision where the offense again includes knowingly taking, concealing, copying, transmitting, altering, destroying, receiving or possessing trade secrets. However, in this case there is not intent to benefit a foreign government and the product must be produced for or placed in interstate commerce. For such theft of trade secrets, the penalty is an unspecified fine and up to 10 years in prison or a $5,000,000 fine for an organization. The sentence under this act may also include criminal forfeiture of the property used in or derived from the violation. These two acts together represent most of the legislation used to prosecute cyber criminals in the United States.

Another piece of proposed legislation that seeks to define cyber crime and impose penalties is the Cyber Security Enhancement Act. The act has been approved by the House, but it still needs to be passed in the Senate. The act would direct the US Sentencing Commission to review and possibly amend federal sentencing guidelines with respect to computer crimes involving national security, critical infrastructure or public health and safety concerns. It also seeks to prohibit advertising of illegal interception devices through the Internet or other media, increase penalties when the offender knowingly causes or attempts to cause death or serious bodily injury and broaden the offence and stiffen the penalty for invading the privacy of the stored communications of other people (Sinrod). One provision of the bill, to allow Internet service providers to share customer records and communications with law enforcement agencies in emergency situations, has already been enacted within the Patriot Act.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Rather than laying out additional infractions and penalties for the black hats, the Gramm-Leach-Bliley Act of 1999 focuses on enhancing information security by ensuring that financial institutions have security plans and basic security features for their computer networks. The Act requires a written security program with a risk analysis and response program for each information system and mandates board of directors involvement in the security program. It requires user authentication for system access, encryption of electronic information while data is in transit and storage and unauthorized individuals may have access, and protection against loss due to environmental hazards. The act also requires monitoring systems and procedures, training procedures, and periodic testing. It went into effect in July 2001.

The Millennium Digital Commerce Act became law in October of 2000. The Act gives digital signatures the same contractual binding force as pen and ink signatures. The important thing to information security, though, is that the Act enables and encourages the use of biometric dynamic signature verification. Cyber-SIGN (http://www.cybersign.com/news_news.htm) describes the dynamic signature verification process by saying, "We analyze the shape, speed, stroke order, off-tablet motion, pen pressure and timing information captured during the act of signing." Thus, the integrity of the data received along with the signature is assured. However, the Act falls short of addressing the possibility of digital signature theft. If digital signatures can be stolen, are they of any value?

Then there is a series of bills and acts that grants additional powers to law enforcement to identify and monitor cyber criminals. This approach will have the desired effect of securing the Internet. The USA Patriot Act is probably the most well known example. The Patriot Act is primarily focused on preventing and combating terrorism, but many of the provisions affect information security because cyber terrorism and terrorist use of our information networks are considered in the act. Some of the most relevant provisions are as follows. Section 105 of the act directs the Secret Service to establish a national network of electronic crime task forces. Section 202 grants authority for wiretaps involving computer fraud and abuse. Section 206 grants roving wiretap authority, a tool needed where the bad guy often switches telephones or computers. Section 207 extends the duration of surveillance on non-citizens who are agents of a foreign power. Section 210 expands the electronic records information the Government may seek with a subpoena. Section 212 allows Internet service providers to voluntarily provide customer records and communications to law enforcement in an emergency situation. Section 216 expands law enforcement's authority to monitor what phone numbers or IP addresses a particular subject calls or visits. Section 217 allows the interception of electronic communications of a computer trespasser accessing a Government or financial institution computer. Law enforcement must have the computer owner's permission.
Section 814 deals directly with the deterrence and prevention of cyber terrorism. Section 816 directs the Attorney General to beef up existing federal computer forensics laboratories.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Another bill that would grant additional powers to law enforcement to identify and monitor cyber criminals is the Cyberspace Electronic Security Act (CESA) of 1999. Although this bill apparently died in Congress due to privacy concerns, it shows that Congress is dedicating much thought and taking positive steps to improve the state of information security. Also, it is highly likely that we have not seen the last of this issue. CESA deals with recovery information, algorithms or back doors used to decrypt encrypted electronic communications. The idea behind the proposal is that law enforcement must be able to interpret electronic communications when it has a valid court order. If criminals use strong encryption, then law enforcement will not be able to interpret the data in a timely manner and sooner or later lives will be lost. The compromise between privacy and need to know would be to let a third party, the recovery agent, hold the recovery information until law enforcement needs it. The bill states that no unauthorized person shall seek to obtain recovery information and that recovery agents shall not use recovery information except as authorized by the act. CESA would require that communication owner permission or a court order is obtained for the release of recovery information. It lists the requirements for law enforcement access and addresses the usage, disclosure and destruction of recovery information obtained by law enforcement. The act would also prevent the recovery agent from revealing sensitive law enforcement techniques. It would authorize funding for the FBI technical support center through FY03 and direct the sentencing commission to review penalties for violating CESA or using encryption to conceal criminal acts.

The Congress has also passed or is considering laws that fund and support information security research and training information technology professionals. Some examples are the Cyber Security Research and Development Act (CSRDA), the Computer Security Enhancement Act (CSEA) and the Networking and Information Technology Research Advancement Act (NITRAA). The main provision of CSEA is to strengthen the role of the National Institute of Standards and Technology (NIST) in evaluating encryption technologies and how they could be used to protect Government systems (http://www.cdt.org/legislation/107th/encryption). CSEA has passed in the House but not in the senate to date. The CSRDA was signed into law in November 2002, and provides nine hundred million dollars in grants through NIST and the National Science Foundation (NSF). The funding to NSF supports undergraduate and graduate degree programs and fellowships to students pursuing doctoral degrees in computer and network security. The funding to NIST will provide grants for partnerships between universities and the private sector to establish computer security research centers. CSRDA also charges NIST to develop checklists for use by federal agencies in selecting security settings on federally procured hardware and software.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The NITRAA amends the responsibilities of NSF to include generating fundamental scientific and technical knowledge with the potential of advancing networking and information technology. It also tasks NSF to provide computing and networking infrastructure support for all science and engineering disciplines and support basic research and human resource development in networking and information technology. The NITRAA authorizes stepped appropriations (704 million in FY03 to 1030 million for FY07) for NSF. The act directs NASA, DOE, and EPA to conduct basic and applied research in networking and information technology in specialized areas and authorizes funding for these research activities. NITRAA tasks NIST with conducting basic and applied measurement research needed to support computing systems and networks; developing voluntary standards and guidelines, measurement techniques and test methods for interoperability of networks; developing benchmark tests for computing systems and software; and encouraging the development, deployment and implementation of voluntary guidelines and standards for robust security technology and best practices and interoperability relating to network security. The act then authorizes stepped appropriations (24 million in FY03 to 35 million in FY07) for these NIST projects. Finally, it tasks NSF with a 2 year study on the state of research on networking and information technology in the US and directs NSF to maintain a database on the information technology work force. NITRAA has not yet left the House.

The Government believes that market forces should be the primary driver for computer security and that the Government should work cooperatively with industry towards computer security. The Cyber Security Information Act of 2001 seeks to establish such a partnership between the federal government and industry. To that end, it authorizes the President to establish working groups of federal employees to engage in discussions on cyber security with outside organizations and share related information. In reality these working groups, Information Sharing and Analysis Centers (ISACS), have already been established by presidential decision directive 63. This legislation formalizes the process and would allow the President to add more federal employees to the ISACs. The act grants antitrust law exemptions to organizations cooperating with the Government and states that information provided to the Government will be protected from disclosure. This bill was introduced in the House in 2001 and has not yet been passed.

The proposed National Cyber Security Defense Team Authorization Act of 2002 would establish a Cyber Security Defense Team composed of representatives from the Departments of Defense, Justice, State, Commerce and Treasury and the CIA. The team would identify areas in which our government and economy's information infrastructure in exposed, identify locations of key hardware, and recommend to federal agencies ways to eliminate vulnerabilities.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

So the Congress and the executive branch have taken many steps to improve the state of information security, but there are some problems. For one thing, Congress has been slow in approving the fiscal year 2003 budget. The delay means that federal agencies can buy only a fraction of the tools and services needed to secure federal information systems. It also has a damaging affect to the information security contractors who work on Government systems. Secondly, many federal agencies are not turning out to be good information security role models as PDD 63 and the derivative policy documents set forth. US representative Steve Horn, chair of the Subcommittee on Government Management, Information and Technology recently released a report card on Government security. Fourteen out of twenty four federal agencies failed. Also, a House report released in October 2002 noted that federal agencies are not conducting periodic risk assessments, have failed to identify critical systems, have inadequate security controls, rely on flawed commercial software and have not built information technology security into capital planning (Jackson). Third, the Government must find a way to increase salaries for information technology professionals if it wants to have some of the best and the brightest. The Government has tried the short term solution of hiring contractors to fill in the gaps, but this tactic is not cost effective over the long term and contract employees are not as likely to stay in Government employment for as long as federal employees. Richard Forno of Security Focus Online suggests that the Government should hold producers of security products accountable for the failures of their products. This strategy would almost certainly reduce the number of vulnerabilities in releases of security products, but it conflicts with the current policy statement that information security should be controlled by market forces.

In conclusion, the Congress has done a thorough job in considering legislation. It may need to get some of the bills stuck in committees moving and grant additional tools and privileges to law enforcement if it intends to effectively curtail cyber crime and prevent cyber terrorism. Presidents Clinton and Bush and the President's Critical Infrastructure Protection Board have done an excellent job on establishing goals and setting policy towards protecting the critical infrastructure and improving the state of information security. President Bush has made budget requests very favorable to cyber security. The executive agencies have done well in the mission areas of managing critical infrastructure protection, research and development, policing the public networks, education and training and information sharing. However, the Congress needs to get its act together in providing timely appropriations, and many federal agencies need information security overhauls.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

"White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." 22 May 1998. URL: http://www.terrorism.com/homeland/pdd63.htm (14 Feb. 2003).

Allor, Peter. "White Paper: IT-ISAC Defined." 10 Jan 2000. URL: http://www.it-isac.org/isacinfowhtppr.php (14 Feb. 2003).

"National Plan for Information Systems Protection: An Invitation to Dialogue." Version 1.0. URL: http://www.ciao.gov/publicaffairs/np1final.pdf (14 Feb. 2003).

Bush, George W. "Executive Order 13231 of October 16, 2001." 16 Oct. 2001. URL: http://www.ncs.gov/ncs/html/eo-13231.htm (14 Feb. 2003).

"National Policy to Secure Cyberspace." Feb. 2003. URL: http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (18 Feb. 2003).

Miller, Jason. "2004 IT budget request focuses on homeland defense, cybersecurity." Government Computer News, Volume 1, No. 1. 20 Jan. 2003. URL: http://www.gcn.com/vol1_no1/daily-updates/20903-1.html (14 Feb. 2003).

URL: http://www.whitehouse.gov/deptofhomeland/bill/title2.html#202 (20 Feb. 2003).

Plehal, Jim. "A Message from Rear Admiral Jim Plehal, Acting Director of the National Infrastructure Protection Center." URL: http://www.nipc.gov/about/about.htm (14 Feb. 2003).

"National Infrastructure Protection Center." URL: http://www.nipc.gov (14 Feb. 2003).

Nowell, Paul. "Taking a Byte out of Crime: New Public-Private Venture Meant to Combat Cybercrime." The Associated Press. 08 August 2000. URL: http://www.abcnews.go.com/sections/tech/dailynews/cybercrime000811.html (14 Feb 2003).

"National Communications System Services." 19 Dec. 2002. URL: http://www.ncs.gov/NCS/HTML/NCSProjects.html (12 Feb. 2003).

"Critical Infrastructure Assurance Office: About Us." URL: http://www.ciao.gov/publicaffairs/about.html (12 Feb. 2003).

"National Infrastructure Simulation and Analysis Center." Jan. 2003. URL: http://www.sandia.gov/CIS/NISAC.htm (12 Feb. 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"About FedCIRC." URL: http://www.fedcirc.gov (12 Feb.2003).

"Overview." URL: http://www.nsf.gov/home/programs (10 Feb. 2003).

"About OSTP." URL: http://www.ostp.gov/html/_aboutostp.html (05 Feb. 2003).

"Defense Advanced Research Projects Agency Technical Offices Programs." 30 June 2002. URL: http://www.darpa.mil/body/off_programs.html (05 Feb 2003).

19 Dec. 2002. URL: http://www.nist.gov/public_affairs/general2.htm (20 Feb. 2003).

"Bits and Chips: NIST Gives U.S. Computer Industry the Advantage." 26 Oct. 2001. URL: http://www.nist.gov/public_affairs/computers.htm (01 Feb. 2003).

"FBI Laboratory Computer Analysis and Response Team." URL: http://www.fbi.gov/hq/lab/org/cart.htm (01 Feb. 2003).

"United States Secret Service Financial Crimes Division Electronic Crimes Branch." URL: http://www.ustreas.gov/usss/fcd_ecb.shtml (01 Feb. 2003).

"Secret Service's Little-Known Role: Protecting Citizens as Well as Leaders." URL: http://www.ectaskforce.org/About_Us.htm (14 Feb. 2003).

Harris, Shane. "FBI, Defense in talks about controversial surveillance technology." 22 Jan. 2002. URL: http://www.govexec.com/dailyfed/0103/012203h1.htm) (14 Feb. 2003).

"Cybercrime Treaty." 26 Sep. 2002. URL: http://www.ala.org/alaorg/oif/cybercrimetreaty.html (01 Feb. 2003).

"Treaty watch: Treaty Status." URL: http://www.treatywatch.org/TreatyStatus.html (01 Feb. 2003).

Leyden, John. "Welsh virus writer Vallor jailed for two years." The Register. 06 Feb. 2003. URL: http://www.theregister.co.uk/content/56/28953.html (06 Feb. 2003).

Lemos, Robert. "Lawyers: Hackers sentenced too harshly." News.com. 20 Feb. 2003. URL: http://www.news.com.com/2100-1001-985407.html (21 Feb. 2003.

Gaudin, Sharon. "Legal system gears up for computer crime cases." 27 June 2000. URL: http://www.cnn.com/2000/TECH/computing/06/27/computer.law.idg/index.html (06 Feb. 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"WWW.CYBERCRIME.GOV: Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. " 14 Feb. 2003. http://www.cybercrime.gov (14 Feb. 2003).

"SANS/FBI Top 20 List." Version 3.21. 17 Oct. 2002. URL: http://www.sans.org/top20 (06 Feb. 2003)

"About CVE." 18 June 2002. URL: http://www.cve.mitre.org/about (06 Feb. 2003)

"Welcome." URL: http://www.cert.org (06 Feb. 2003).

"About the SEI – Welcome." URL: http://www.sei.cmu.edu/programs/nss (06 Feb. 2003).

Lemos, Robert. "Feds, firms unveil test for security pros." News.Com. 27 Nov. 2002. URL: http://www.news.com.com/2100-1001-975556.html (06 Feb. 2003).

O'Hara, Colleen. "Cyber scholarship program expands." Federal Computer Week. 13 Feb. 2003. URL: http://www.fcw.com/fcw/articles/2003/0210/web-schol-02-13-03.asp (21 Feb. 2003).

"18 U.S.C. 1030: Fraud and Related Activity in Connection with Computers." 24 Jan. 2002. URL: http://www.usdoj.gov/criminal/cybercrime/1030_new.html (15 Jan. 2003).

"United States Code Title 18 – Crimes and Criminal Procedures Part II Chapter 90 – Protection of Trade Secrets." URL: http://www.tscm.com/USC18_90.html (15 Jan. 2003).

Sinrod, Eric. "E-Legal: House Seeks to Increase Computer Crime Penalties." 23 July 2002. URL: http://www.law.com/jsp/article.jsp?id=1024079027108 (15 Jan. 2003).

Johnson, Barry. "GLBA: Safety and Soundness Standards. A Financial Institution's Responsibility." URL: http://www.giac.org/practical/Barry_Johnson_GSEC.doc (10 Jan. 2003).

"News and Events." URL: http://www.cybersign.com/news_news.htm (11 Jan. 2003).

URL: http://speakout.com/activism/issue_briefs/1305b-1.html (11 Jan. 2003).

"USA PATRIOT Act as Passed by Congress." 24 Oct. 2001. URL: www.eff.org/Privacy/Surveillance/Terrorism_militias/20011025_hr3162_usa_patriot_bill.html (5 Jan. 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"Cyberspace Electronic Security Act of 1999." URL: http://www.cdt.org/crypto/CESA/CESArevised.shtml (12 Jan. 2003).

"107th Congress 2nd Session S.2182." URL: http://www.theorator.com/bills107/s2182.html (13 Jan. 2003).

"Encryption 107th Congress." URL: http://www.cdt.org/legislation/107th/encryption (14 Jan. 2003).

"107th Congress 1st Session H.R. 3400." URL: http://www.theorator.com/bills107/hr3400.html (14 Jan. 2003).

"107th Congress 1st Session H.R. 2435." URL: http://www.theorator.com/bills107/hr2435.html (14 Jan 2003).

"Press Release: Schumer Introduces Bill to Increase Cyber Security and Protect New York From Terrorist Hacker Attack." 05 Mar. 2002. URL: http://www.senate.gov/~schumer/SchumerWebsite/pressroom/press_releases/PR00874.html (15 Jan. 2003).

Jackson, William. "Make GISRA permanent, House panel tells Congress." Government Computer News. Vol. 21 No. 33. 18 Nov. 2002. URL: http://www.gcn.com/21_33/news/20513-1.html (15 Dec. 2002).

Forno, Richard. "The Curmudgeon's Crystal Ball: Security Predictions for 2003." 15 Jan. 2003. URL: http://online.securityfocus.com/columnists/135 (15 Jan. 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced