Cybersecurity Concerns

of the U.S. Government

Compiled and Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

Table of Contents

Section	Page Number
About the Editor	2
Introduction	4
NIST Testimony on Computer Security Issues 2000	6
FBI Testimony on the National Infrastructure Protection Center 2002	12
FBI Testimony on Cyber Terrorism 2005	26
FBI Testimony on Cybersecurity Issues 2011	33
DHS Testimony on Understanding Risks and Building Capabilities 2014	45
NIST Testimony on WannaCry 2017	55
Examining DHS's Cybersecurity Mission 2017	64
SEC Statement on Cybersecurity 2017	73

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Threat Level Red: Cybersecurity Research Programs of the U.S. Government (CRC Press)
Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business Privacy Plan (McGraw Hill)

Introduction

The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists. The threat is incredibly serious—and growing. Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. Our nation's critical infrastructure, including both private and public sector networks, are targeted by adversaries. American companies are targeted for trade secrets and other sensitive corporate data, and universities for their cutting-edge research and development. Citizens are targeted by fraudsters and identity thieves, and children are targeted by online predators. Just as the FBI transformed itself to better address the terrorist threat after the 9/11 attacks, it is undertaking a similar transformation to address the pervasive and evolving cyber threat. This means enhancing the Cyber Division's investigative capacity to sharpen its focus on intrusions into government and private computer networks. Key Priorities:

Computer and Network Intrusions

The collective impact is staggering. Billions of dollars are lost every year repairing systems hit by such attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 services around the country.

Who is behind such attacks? It runs the gamut—from computer geeks looking for bragging rights…to businesses trying to gain an upper hand in the marketplace by hacking competitor websites, from rings of criminals wanting to steal your personal information and sell it on black markets…to spies and terrorists looking to rob our nation of vital information or launch cyber strikes.

Today, these computer intrusion cases—counterterrorism, counterintelligence, and criminal—are the paramount priorities of our cyber program because of their potential relationship to national security.

Combating the threat. In recent years, we've built a whole new set of technological and investigative capabilities and partnerships—so we're as comfortable chasing outlaws in cyberspace as we are down back alleys and across continents. That includes:

A Cyber Division at FBI Headquarters "to address cyber crime in a coordinated and cohesive manner";

Specially trained cyber squads at FBI headquarters and in each of our 56 field offices, staffed with "agents and analysts who protect against investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud";

New Cyber Action Teams that "travel around the world on a moment's notice to assist in computer intrusion cases" and that "gather vital intelligence that helps us identify the cyber crimes that are most dangerous to our national security and to our economy;"

Our 93 Computer Crimes Task Forces nationwide that "combine state-of-the-art technology and the resources of our federal, state, and local counterparts";

A growing partnership with other federal agencies, including the Department of Defense, the Department of Homeland Security, and others—which share similar concerns and resolve in combating cyber crime.

Ransomware

Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.

The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation. Home computers are just as susceptible to ransomware and the loss of access to personal and often irreplaceable items— including family photos, videos, and other data—can be devastating for individuals as well.

In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software.

One the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom, usually with bitcoins because of the anonymity this virtual currency provides.

This volume presents important testimony provided by various government agencies addressing threats to computers systems and networks.

NIST Testimony on Computer Security Issues 2000

March 09, 2000

Witness

Karen H. Brown

Deputy Director, National Institute of Standards and Technology

Technology Administration

U.S. Department of Commerce

Venue

Committee on Government Reform

Subcommittee on Government Management, Information, and Technology

Mr. Chairman and members of the subcommittee thank you for the invitation to speak to you today about computer security issues. I am Karen Brown, Deputy Director of the National Institute of Standards and Technology of the Department of Commerce's Technology Administration.

Computer security continues to be an ongoing and challenging problem that demands the attention of the Congress, the Executive Branch, industry, academia, and the public. Computer security is not a narrow, technical concern. The explosive growth in Electronic Commerce highlights the nation's ever increasing dependence upon the secure and reliable operation of our computer systems. Computer security, therefore, has a vital influence on our economic health and our nation's security and we commend the Committee for your focus on security.

Today I would like to address NIST's computer security activities that contribute to improving computer security for the Federal Government and the private sector. I also would like to briefly describe for you our proposed new program activities for next year as requested in the President's budget.

Under NIST's statutory federal responsibilities, we develop standards and guidelines for agencies to help protect their sensitive unclassified information systems. Additionally, we work with the information technology (IT) industry and IT users in the private sector on computer security in support of our broad mission to strengthen the U.S. economy, and especially to improve the competitiveness of the U.S. information technology industry. As awareness of the need for security grows, more secure products will be more competitive in the marketplace. Addressing security will also help ensure that Electronic Commerce growth is not limited because of security concerns.

In meeting the needs of our customers in both the public and private sector, we work closely with industry, Federal agencies, testing organizations, standards groups, academia, and private sector users. Cooperation and collaboration are essential to tackle many common problems facing users throughout the country.

What does NIST do specifically? To meet these responsibilities and customer needs, we first work to improve the awareness of the need for computer security. This helps increase demand for secure and reliable products. Additionally, we research new technologies and their security implications and vulnerabilities and develop guidance to advise users accordingly. We work to develop security standards and specifications to help users specify security needs in their procurements and establish minimum security requirements for Federal systems. We develop and manage security testing programs, in cooperation with private sector testing laboratories, to enable users to have confidence that a product meets a security specification. We also produce security guidance to promote security planning, and secure system operations and administration. I will briefly discuss the need and benefits of each.

First, there is a need for timely, relevant, and easily accessible information to raise awareness about the risks, vulnerabilities and requirements for protection of information systems. This is particularly true for new and rapidly emerging technologies, which are being delivered with such alacrity by our industry. We host and sponsor information sharing among security educators, the Federal Computer Security Program Managers' Forum, and industry. We seek advice from our advisory board of computer experts (Computer System Security and Privacy Advisory Board). We meet regularly with members of the Federal computer security community, including the Chief Information Officers' Security Committee, and the Critical Infrastructure Assurance Office. We actively support information sharing through our conferences, workshops, web

pages, publications, and bulletins. Raising awareness helps ensure appropriate attention is accorded security and helps increase the demand for secure products and security services.

A second need is for research on information technology vulnerabilities and the development of techniques for the cost-effective security. When we identify new technologies that could potentially influence our customers' security practices, we research the technologies and their potential vulnerabilities. We also work to find ways to apply new technologies in a secure manner. The solutions that we develop are made available to both public and private users. Some examples are methods for authorization management and policy management, ways to detect intrusions to systems, and demonstrations of mobile agents. Research helps us find more cost-effective ways to implement and address security requirements.

Third is the need for standards, and for ways to test that standards are properly implemented in products. For example, cryptographic algorithms and techniques are essential for protecting sensitive data and electronic transactions. NIST has long been active in developing Federal cryptographic standards and working in cooperation with private sector voluntary standards organizations in this area. Moreover, in the standards area we have been working with the private sector in preparing for the future. We are leading a public process to develop the Advanced Encryption Standard (AES), which will serve 21st century security needs. Another aspect of our standards activities concerns Public Key and Key Management Infrastructures. The use of cryptographic services across networks requires the use of "certificates" that bind cryptographic keys and other security information to specific users or entities in the network. We have been actively involved in working with industry and the Federal government to promote the security and interoperability of such infrastructures.

Standards help users to know what security specifications may be appropriate for their needs. Testing complements this by helping users have confidence that security standards and specifications are correctly implemented in the products they buy. Testing also helps reduce the potential that products contain vulnerabilities that could be used to attack systems.

For over five years, we have led the Cryptographic Module Validation Program, which has now validated about 90 modules with another 50 expected this year. This successful program utilizes private sector accredited laboratories to conduct security conformance testing of cryptographic modules against a Federal standard we develop and maintain. More recently, we have been working with the international security community to define security criteria in an international

standard that can be used to develop security specifications for products, such as firewalls or operating systems. We are actively working with industry partners in the smart card, health care, and telecommunications fields to accomplish such development of specifications.

Many of these activities are being done in cooperation with the Defense Department's National Security Agency in our National Information Assurance Partnership. Private sector laboratories are being accredited under our National Voluntary Laboratory Accreditation program to conduct such testing. The effort involves developing testing competencies and a process for accrediting testing organizations. The goal is to enable product developers to get their products tested easily and voluntarily, and for users to have access to information about tested products. Under this program we have also led the development of an international mutual recognition arrangement whereby the results of testing in the U.S. are recognized by our international partners, thus reducing the costs to industry.

Advice and technical assistance for both government organizations and private sector users is the fourth need. For example, we have issued guidance including telecommuting and security, security concerns inherent in PBX technology, security requirements in Public Key Infrastructure (PKI) implementation, use of firewalls, and intrusion detection in networks. We also provide program guidance to agencies and are working to complete a document on security program metrics and self-assessment. The information and guidelines that we have developed are available to all users free-of-charge via our web site. We also support agencies on specific security projects on a cost-reimbursable basis when NIST expertise is required.

While I have given you a few examples of NIST's work, I obviously have not covered everything. I want to emphasize that there is still much more to be done to address the continuing challenges of computer security. To put our program in perspective, please keep in mind that approximately $6 million of direct Congressional funding supports both our Federal and industry computer security responsibilities. (In addition, we receive approximately $2 million in outside agency funding to provide technical assistance on particular projects.) This is plainly not enough.

As reflected in the requests made in the President's FY 2001 budget, NIST needs additional resources to help improve the security posture of the Federal government. Looking at the critical information infrastructures of the nation, we also need substantial investments in security research to find ways to protect our infrastructures.

To address the need for additional research to protect our critical infrastructures, the White House has proposed establishing a $50 million Institute for Information Infrastructure Protection (IIIP), which was initially recommended by the President's Committee of Advisors on Science & Technology (PCAST). The IIIP will identify and fill the gaps not being met by private sector market demands or Government agency mission objectives in critical infrastructure protection and provide a strong and secure foundation to protect the various critical infrastructures upon which the Nation's security and economy rely. IIIP's R&D, which will aim to help prevent security problems will include work that can be applied to protect multiple sectors' infrastructures, and thus will complement sector-specific R&D underway elsewhere in the government and private sector. This initiative will help strengthen the focused existing and planned security architectures within the critical infrastructure sectors and help prepare the owners/operators of those infrastructures to survive potential hostile activities. The IIIP will not have any direct role in support of law enforcement or deterring attacks, but will fund R&D to develop new generations of IT security solutions that would be made available for DoJ/FBI, other agencies, and the private sector can use to prevent and respond to future cyber-threats. The IIIP will be a partnership among industry, academia and the government (including both state and local governments). At the core of the partnership is IIIP's selection of information infrastructure protection R&D focus areas, which will rely heavily on advice and guidance obtained from outside experts.

The security of Federal systems must also be improved. These systems contain sensitive information about our citizens and provide services upon which our citizens' safety and well-being depend. The government should exert leadership and set an example for the nation in protecting against risks and vulnerabilities. Two of the budget proposals focus primarily upon the security of Federal systems. Specifically, we propose to establish an Expert Review Team (comprised of eight FTE's) to advise agencies of their vulnerabilities, help prioritize and develop strategies for security fixes, assist agencies in preparing for future security threats, and help agencies plan for security in new system developments. This preventative approach will complement the reporting activities of programs such as FedCIRC. Secondly, we seek a five million dollar increase to enable additional critical activities in the area of cryptography, security management and best practices guidance, and the protection of supervisory control systems.

So let me close by again emphasizing that our national commitment to improve security must be increased. NIST stands ready to play a key role through supporting the proposed Institute, leading the Expert Review Team, and conducting additional work to developing needed security guideline and standards, research in security technology, leading testing programs, and raising

awareness and demand for security products and services. This will augment the already important activities we have underway. We look forward to continuing this work, and believe that your support of the critical new activities would help us to do so.

I will be pleased to answer any questions.

Source: https://www.nist.gov/speech-testimony/computer-security-issues

FBI Testimony on the National Infrastructure Protection Center 2002

Ronald L. Dick

Director, National Infrastructure Protection Center, FBI

Federal Bureau of Investigation

Before the House Committee on Governmental Reform, Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee

Washington, DC

June 24, 2002

Mr. Chairman and members of the Subcommittee, thank you for inviting me here today to testify on the topic, "Cyber Terrorism and Critical Infrastructure Protection." Holding this hearing demonstrates your individual commitment to improving the security of our Nation's critical infrastructures and this Committee's leadership on this issue in Congress. Our work here is vitally important because the stakes involved are enormous. We have seen how a terrorist attack can have immediate simultaneous impact on several interdependent infrastructures. The terrorist attacks in New York directly and seriously affected banking and finance, telecommunications, emergency services, air and rail transportation, energy and water supply. My testimony today will address the improvement of infrastructure protection through two-way information sharing and the challenges we face in the future.

Since our last testimony before this Subcommittee on September 26, 2001, the National Infrastructure Protection Center has seen increases in personnel, funding, and interagency participation, allowing us to make great progress in accomplishing our mission. As set forth in Presidential Decision Directive 63 (PDD-63), the mission of the NIPC is to provide "a national focal point for gathering information on threats to the infrastructures" and to provide "the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts." The Directive defines critical infrastructures to include "those physical and cyber-based systems essential to the minimum operations of the economy and government," to include, without limitation, "telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." Our combined mission supports information and physical security, law enforcement, national security, and the military.

To accomplish this mission, we have had to build a coalition of trust amongst all government agencies, between the government and the private sector, amongst the different business interests within the private sector itself, and in concert with the greater international community. We have begun to earn that trust, and two-way information sharing has increased considerably since our last testimony here.

OUTREACH EFFORTS

To better share information, the NIPC has spearheaded an aggressive outreach effort.

NIPC officials have met with business, government, and community leaders across the United States and around the world to build the trust required for information sharing. Protection of business information and privacy interests are both stressed in NIPC internal deliberations and with business, government and community leaders. Most have been receptive to information sharing and value the information received from the NIPC. Others have expressed reservations due to a lack of understanding or perhaps confidence in the strength of the disclosure exceptions found in the Freedom of Information Act, concerns about whether the Justice Department would pursue prosecutions at the expense of private sector business interests, and simple reluctance to disclose proprietary information to any entity beyond their own control or beyond the direct control of the NIPC.

CRITICAL NEED FOR OUTREACH

The annual Computer Security Institute/FBI Computer Crime and Security Survey, released in April, indicated that 90% of the respondents detected computer security breaches in the last 12 months. Only 34% reported the intrusions to law enforcement. On the positive side, that 34% is more than double the 16% who reported intrusions in 1996. The two primary reasons for not making a report were negative publicity and the recognition that competitors would use the information against them. Many respondents were not aware that they could report intrusions to law enforcement. We have moved aggressively to address these concerns and go out of our way to reassure businesses that their voluntarily provided information will remain secure, and that we are always sensitive to protecting the interests of victims who report crime.

Infragard: The Most Extensive Network of Federal and Private Sector Partners in the World for Protecting the Infrastructure

The InfraGard program is a nationwide initiative that grew out of a pilot program started at the Cleveland FBI field office in 1996. Today, all 56 FBI field offices have active InfraGard chapters. Nationally, InfraGard has over 5000 members. It is the most extensive government-private sector partnership for infrastructure protection in the world, and is a service the FBI provides to InfraGard members free of charge. It particularly benefits small businesses which have nowhere else to turn for assistance. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices. The InfraGard program received the 2001 World Safe Internet Safety Award from the Safe America Foundation for its efforts.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. InfraGard provides a mechanism for the public and private sectors to exchange information pertaining to cyber intrusion matters, computer network vulnerabilities and physical threats on infrastructures. All InfraGard participants are committed to the proposition that the exchange of information about threats on these critical infrastructures is an important element for successful infrastructure protection efforts. The goal of InfraGard is to enable information flow so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.

Private sector members and an FBI field representative form local area chapters. These chapters set up their own boards to govern and share information within the membership. The chapter members include representatives from the FBI, State and local law enforcement agencies, other government entities, private industry and academia. The National Infrastructure Protection Center and the Federal Bureau of Investigation play the part of facilitator by gathering information and distributing it to members, educating the public and members on infrastructure protection, and disseminating information through the InfraGard network.

InfraGard is responsible for providing four basic services to its members: secure and public web sites, an alert and incident reporting network, local chapter activities, and a help desk. Under this program the FBI provides a secure electronic communications capability to all InfraGard members so that the NIPC can provide threat information to private industry owners and operators, and encourage private industry coordination with law enforcement, and each other, on cyber and related physical incidents. This will be accomplished by expanding the established separate website and electronic mail system. The program anticipates approximately 4,000 new members expected in calendar year 2002. A number of the larger field divisions have initiated additional chapters in larger cities located in their respective geographic area of responsibility. The warnings that are provided to our InfraGard members improve the relationship between private industry and the local FBI offices due to the increased level of trust that is often established. It should be noted that the InfraGard program is not responsible for producing NIPC's alerts and warnings. These alerts and warnings are produced and disseminated by NIPC's Analysis and Warning Section.

Information Sharing and Analysis Centers (ISACs)

The NIPC has recently initiated the establishment of an Information Sharing and Analysis Center (ISAC) Support and Development Unit, whose mission is to enhance private sector cooperation and trust, resulting in two-way sharing of information and increased security for the nation's critical infrastructures. The ISAC Development and Support Unit has assigned personnel to each ISAC to serve as NIPC's liaison to that sector. When an ISAC receives information from a member, they forward the information to their NIPC liaison, who then works with NIPC's Analysis and Information Sharing Unit and Watch and Warning Unit to coordinate an appropriate response. The NIPC now has information sharing agreements with nine ISACs, including those representing energy, telecommunications, information technology, banking and finance, emergency law enforcement, emergency fire services, water supply, food, and chemical sectors. Several more agreements are in the final stages, including one to be signed on July 25th with the National Association of State Chief Information Officers. Just as important, the NIPC is receiving reports from member companies of the ISACs. The NIPC has proven to these companies that it can properly safeguard their information and can provide them with useful information. It is because of such reporting that NIPC's products are improving.

Three examples bear discussion. The North American Electric Reliability Council (NERC) serves as the electric power ISAC. The NIPC has developed a program with the NERC for an Indications and Warning System for physical and cyber attacks. Under the program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports

are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the program have stated that the information and analysis provided by the NIPC back to the power companies make this program especially worthwhile. NERC has recently decided to expand this initiative nationwide. This initiative will serve as a good example of government and industry working together to share information and the Electrical Power Indications and Warning System will provide a model for the other critical infrastructures. Additionally, some information available to the NIPC may be classified or law enforcement sensitive and, thus, unavailable to many in the industry. A group of NERC officials have been granted security clearances in order to access classified material on a need-to-know basis. Once the NIPC has determined that a warning should be issued, cleared electric power experts will be available as needed to assist the NIPC in sanitizing and finalizing warning notices so as to provide members of the industry with unclassified, nonproprietary, timely and actionable information to the maximum extent possible.

One of our most recent agreements was with the ISAC for Emergency Services - Fire, the US Fire Administration, an organization which has been a model for the mutual benefits of two-way information sharing. Since that agreement, we have shared intelligence on diver threats to waterfront facilities, suspicious attempts to purchase an ambulance in New York, and the theft of a truck with 10 tons of cyanide in Mexico. In turn, they have told us of suspicious foreign nationals visiting fire stations to gather information and of foreign nationals calling fire and EMS departments and visiting their web sites to gather information on capabilities, watch schedules and manning levels. Such two-way information sharing provides significant safety and infrastructure protection benefits to the public we serve.

The telecommunications ISAC provides a good example of positive, two-way information sharing. In his July 9, 2002 testimony before the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, Bill Smith, Chief Technology Officer, BellSouth Corporation, stated: "With respect to FOIA (Freedom of Information Act), many companies are hesitant to voluntarily share sensitive information with the government because of the possible release of this information to the public." He further noted that BellSouth does share information with the Telecommunications ISAC, but it is "done on a limited basis, within trusted circles, and strictly within a fashion that will eliminate any liability or harm from FOIA requests for BellSouth information." He adds that BellSouth has benefited from advance warnings of worms and viruses. The telecommunications ISAC provided BellSouth with their first notification of the NIMDA worm, resulting in the successful defense of their networks. BellSouth, in turn, was the first to notify the ISAC of problems associated with the simple network management protocol. Although this is an example of two-way information sharing, it is also an example of reluctant sharing resulting from legal, economic and trust barriers. Smith goes on to list BellSouth's

concerns about information sharing, including: "liability under the Freedom of Information Act, third-party liability (e.g., sharing suspected problems about a piece of equipment before thoroughly tested and verified), the lack of a defined antitrust exemption for appropriate information sharing concerning infrastructure vulnerabilities, possible disclosure of information under state sunshine laws, disclosure of sensitive corporate information to competitors, declassification of threat/intelligence information to a level that can be acted upon by company personnel, and the natural inclination of law enforcement, DoD, and intelligence agencies to dissuade the sharing of information related to criminal investigations."

The NIPC routinely shares information with the public and private sectors to help them better protect themselves. That does not mean that information is broadcast across the news media in every instance. While public statements are the best alternative in some cases, in other cases the NIPC has approached victim companies as to a specific investigation, and Information Sharing and Analysis Centers (ISACs) or government agencies privately to help evaluate uncorroborated information in order then to provide public comment. In many cases, a tiered approach is taken so that information with the appropriate level of detail is pushed to the right audiences. If the NIPC finds that despite issuing an advisory, a widespread problem persists or grows, then we will raise the volume, and a more public advisory will be issued to reach a wider audience.

NIPC INFORMATION SHARING PRODUCTS

The NIPC has a variety of information products to inform the private sector and other domestic and foreign government agencies of the threat, including: assessments, advisories and alerts; a Daily Report; biweekly CyberNotes; monthly Highlights; and topical electronic reports. These products are designed for tiered distribution to both government and private sector entities consistent with applicable law and the need to protect intelligence sources and methods, and law enforcement investigations. For example, Highlights is a monthly publication for sharing analysis and information on critical infrastructure issues. It provides analytical insights into major trends and events affecting the nation's critical infrastructures. It is usually published in an unclassified format and reaches national security and civilian government agency officials as well as infrastructure owners. CyberNotes is another NIPC publication designed to provide security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices. It is published twice a month on the NIPC website (www.nipc.gov) and disseminated via e-mail to government and private sector recipients. Although the NIPC can and does issue limited distribution products that are classified or law enforcement sensitive (for