Order Code RL31534

Report for Congress
Received through the CRS Web

Critical Infrastructure: Control Systems and the Terrorist Threat

Updated February 21, 2003

Dana A. Shea
Consultant
Resources, Science, and Industry Division

Critical Infrastructure: Control Systems and the Terrorist Threat

Summary

Much of the U.S. critical infrastructure is potentially vulnerable to cyber-attack. Industrial control computer systems involved in this infrastructure are specific points of vulnerability, as cyber-security for these systems has not been perceived as a high priority. Industries potentially affected by a cyber-attack on industrial control systems include the electrical, telephone, water, chemical and energy sectors.

The federal government has issued a warning regarding an increase in terrorist interest in the cyber-security of industrial control systems, citing both interest by international terrorist organizations in critical infrastructure and increases in cyber-attack on critical infrastructure computer systems. The potential consequences of a successful cyber-attack on critical infrastructure industrial control systems could be high, ranging from a temporary loss of service to catastrophic infrastructure failure affecting multiple states for an extended duration.

The National Strategy for Securing Cyberspace was released and contained a number of suggestions regarding security measures for control systems. A focus on the further integration of public/private partnerships and information sharing is described, along with suggestions that standards for securing control systems be developed and implemented.

Possible policy options for congressional consideration include further development of uniform standards for infrastructure cyber-protection, growth in research into encryption methods for industrial control systems, assessing the effectiveness of the new exemptions to the Freedom of Information Act and the integration of previous offices in the new Department of Homeland Security.

Contents

This report was prepared under the general supervision of Glenn McLoughlin, Specialist, Resources, Science and Industry Division, Congressional Research Service.

Critical Infrastructure: Control Systems and the Terrorist Threat

Introduction

This report addresses the cyber-vulnerability of critical infrastructure industries which regularly use industrial control systems. Industrial control systems may be vulnerable to infiltration by different routes, including wireless transmission, direct access to control system computers, exploitation of dial-up modems used for maintenance, or through the Internet. This report will specifically discuss the potential for access to industrial control systems through the Internet.

The vulnerability of U.S. critical infrastructure to cyber-attack and catastrophic failure was brought to light in 1997 in the report of the President's Commission on Critical Infrastructure Protection.[1] Among other concerns, the computer systems used to remotely control process equipment were highlighted as specific points of vulnerability. These systems were updated during the Y2K crisis, but these system's cyber-security has not generally been a high priority. The events of September 11, 2001 have heightened the public awareness of the nation's vulnerability to terrorist attack, and a recent National Research Council report has identified "the potential for attack on control systems" as requiring "urgent attention."[2]

Critical infrastructure is defined in the USA PATRIOT Act as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[3] Several industry sectors considered to be critical infrastructures use industrial control systems in their daily activities. These industries could be significantly affected by a cyber-attack targeting industrial control systems such as supervisory control and data acquisition (SCADA) systems, distributed control systems, and others. The President's Commission on Critical Infrastructure Protection report stated,

> From the cyber perspective, SCADA systems offer some of the most attractive targets to disgruntled insiders and saboteurs intent on triggering a catastrophic event. With the exponential growth of information system networks that interconnect the business, administrative, and operational systems, significant

---

[1]Presidential Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October, 1997.

[2]National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, June, 2002.

[3]United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, P.L. 107-56, Title X, Section 1016.

disruption would result if an intruder were able to access a SCADA system and modify the data used for operational decisions, or modify programs that control critical industry equipment or the data reported to control centers.[4]

Current Industrial Control System Vulnerability

Industrial control systems can include supervisory control and data acquisition systems, distributed control systems (DCS), and programmable logic controllers (PLC). SCADA systems are primarily software toolkits for building industrial control systems. These systems are often used for remote monitoring and sending commands to valves and switches. For example, they can be found in water utilities and oil pipelines, where they monitor flow rates and pressures. Based on the data that these systems provide, computer programs or operators at a central control center balance the flow of material using industrial control systems to activate valves and regulators. Generally, SCADA systems process little data internally, instead performing analysis in a more central location, but are the primary conduits for raw data in and commands out of a control center. They are vulnerable to implantation of faulty data and to remote access through dial-up modems used for maintenance.

Distributed control systems are process control systems where hardware and software components are often provided by a single vendor. These process control systems are commonly deployed in a single manufacturing or production complex, and perform a higher level of internal data processing. DCS generally provide processed information to or a series of commands from a control center. An example might occur within a chemical plant, where a DCS might simultaneously monitor the temperature of a series of reactors and control the rate at which reactants were mixed together, while performing real time process optimization and reporting the progress of the reaction. An attack targeting DCS might cause extensive damage at a single facility, but would be unlikely to affect more than a single site.

Programmable logic controllers are devices used to automate monitoring and control of industrial plants, and are generally used within a manufacturing facility. They tend to provide little external information, and do the majority of their data processing internally. Programmable logic controllers can control as little as a single machine to as much as an entire manufacturing facility. An automated assembly line can be comprised of a series of PLCs, with each machine on the assembly line performing a distinct job. An attack targeting PLCs might cause significant turmoil at a single location, but the extent of the damage would depend on both the PLC's size and connectivity.

These process control systems can be interconnected within a single industry as well. As an example, the oil and gas infrastructures contain both processing and refining sites, as well as holding facilities and distribution systems. Refining and processing sites may utilize DCS, controlling the different refining steps via PLCs. The distribution and holding facilities might be managed by a SCADA system which

---

[4]Presidential Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October, 1997.

collected data from and issued commands to the different sites from a single location.[5]

Industrial control system technologies are often employed in critical infrastructure industries to allow a single control center to manage multiple sites. Industrial control systems were originally implemented as isolated, separate networks. They were viewed as secure systems which protected remote locations from being physically broken into and mistreated. For example, the establishment of remote control systems in dams were believed to protect against unlawful release of the dammed water, as no hand-operable valves and switches were accessible.[6]

Networking industrial control systems on a greater scale has led to increased synergy and efficiency, and, due to utility deregulation, real time information is increasingly important for marketing purposes. Consequently, industrial control systems are becoming linked to corporate computer systems, potentially making them vulnerable to cyber-attack through the Internet. Legacy control systems were originally designed to be free standing networks without Internet access. Therefore, it has been necessary to add network access systems to the original systems to integrate them into the corporate structure. This has created, in the worst cases, a labyrinth of connections which is perhaps not rigorously constructed for cyber-security or well documented.

Some industrial control systems, including legacy systems, are proprietary, and contain non-standard architectures and command syntax. This can be considered both an advantage and a disadvantage. Proprietary systems with esoteric command structures are often non-intuitive, and could be difficult to operate by an untrained individual. Incorrect commands could cause no results, and may increase the probability that the intruder would be noticed and removed from the system. Additionally, different companies may have different command sets, even if they are both members of the same industry, as their proprietary systems may have significantly different structures. Thus, if a hacker or terrorist successfully attacks one company, that experience may not be valuable for use at the next company.

On the other hand, legacy systems may be especially vulnerable due to the ad hoc manner of their integration with the network. This imperfect fit between the different software applications could generate more vulnerable code aspects than would be found in a single piece of software. In a piece of software, it may be possible, for example, through a poorly defined variable, to force the program to behave in a way not expected by the author. When two programs are brought together, the number of these potential weaknesses are multiplied. Thus, legacy systems with network access systems added may be more prone to security flaws and weaknesses than systems which use a single piece of software for both functions.

---

[5]This example was taken from "IT Security for Industrial Control Systems" by Joe Falco, Keith Stouffer, Albert Wavering and Frederick Proctor, Intelligent Systems Division, National Institute of Standards and Technology.

[6]Scott Berinato, "The Truth about Cyberterrorism,"*CIO Magazine*, Vol. 15, No. 11, March 15, 2002.

The degree of integration between control system networks and publicly accessible networks is difficult to judge from the open literature. This makes assessment of the vulnerability of critical infrastructure industries from Internet based attack difficult to know with certainty.[7] Faced with this unclear risk, it is likewise difficult, from an industry perspective, to justify the additional costs of upgrading privately-held industrial control systems to higher security standards.[8] Current off-the-shelf industrial control systems have been designed for operational speed and functionality, rather than for secure operation, and therefore do not have a high degree of operational security.[9] Addition of security requirements can degrade the performance of these components below operating standards. In addition, current off-the-shelf industrial control systems may use open source software, which may impede the use of secure protocols. Open source software is advantageous from the programming perspective, as many users are able to view the code for the software and make improvements on it, but it provides prospective terrorists with source code to discover potential weaknesses.

Given the uncertain vulnerability level and the systemic weaknesses involved in current off-the-shelf technology, there is little incentive to substantially increase the security of industrial control systems from either the market or technological perspective. Therefore the security systems for the corporate network, which block initial intrusion through Web-based servers, may be the sole planned protection for the industrial control systems.

Other security analysts also contend that the obscurity of industrial control systems is less of a defense now than previously. Foreign utility companies increasingly use current off-the-shelf industrial control systems, increasing the international availability of sample systems and their documentation. Due to the similarity between these systems and systems installed domestically, potential terrorists need not break into an American utility to test their plans.[10]

Some security analysts believe that the industrial control system vulnerability should be addressed before potentially catastrophic events occur, and that techniques for reducing the vulnerability are already known. They contend that the majority of attacks on industrial control systems will come through the corporate network,

---

[7]The Department of Energy and the Department of Defense have performed vulnerability assessments, through "red team" exercises, of some individual stakeholders in critical infrastructure industries. (Barton Gellman, "Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say," *Washington Post*, June 27, 2002) These results, while provided to the individual stakeholders, are not widely available. (Joe Weiss, KEMA Consulting, private e-mail communication, September 8, 2002)

[8]Eric Pianin and Bill Miller, "Businesses Draw Line On Security, Firms Resist New Rules For Warding Off Terror," *Washington Post*, September 5, 2002.

[9]Jennifer Alvey, "Digital Terrorism: Holes in the Firewall? Plugging Cyber Security Holes Isn't as Easy as Everyone Wants to Think," *Public Utilities Fortnightly*, March 15, 2002.

[10]Testimony by Timothy G. Belcher, Chief Technology Officer, Riptech, Inc., before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, July 24, 2002.

originating in the Internet. While standard information technology protection methods have not yet been developed specifically for industrial control systems, they contend that if general network benchmark standards were uniformly applied across corporate networks, the corporate network vulnerability to intrusion could be reduced by 80-88%.[11] This would indirectly reduce the industrial control systems vulnerability to intrusion, as routes through the corporate network would no longer be available. These benchmark standards include disabling unneeded server functionality, patching known security flaws, and updating programs to the most recent version.

Other security analysts claim that in addition to general network security, specific protection for industrial control systems must be established. Marc Maifrett, Chief Hacking Officer and Co-Founder of eEye Digital Security, testified that specifications to define a level of security for networked aspects of infrastructure companies and for SCADA control software must be developed and enforced by the federal government.[12] By addressing the vulnerability generated by connecting the corporate network and the control network, in addition to increasing information security between the Internet and the corporate network, a lower control system vulnerability might be achieved.

In contrast, control systems may have vulnerabilities unrelated to those of the corporate network, and may require more specific protection, including against attacks not transiting the corporate network.[13] Protecting the corporate network from intrusion may not address enough of the vulnerable access routes into industrial control systems. Joe Weiss, former technical lead on control system cyber-security for the Electric Power Research Institute (EPRI) and currently a Consultant with KEMA Consulting, asserts that firewalls, intrusion detection, encryption, and other technology needs to be developed specifically for control systems.[14]

Some companies have taken aggressive steps to protect their industrial control systems, and are models for how secure industrial control systems can be established.[15] While most security experts agree that critical infrastructure industries which view secure industrial control systems as a priority can reduce vulnerabilities to a low level, they assert that most critical infrastructure industries are not willing

---

[11]Testimony by Alan Paller, Director of Research, The SANS Institute, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, July 24, 2002.

[12]Testimony by Marc Maifrett, Chief Hacking Officer and Co-Founder, eEye Digital Security, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, July 24, 2002.

[13]Joe Weiss, KEMA Consulting, private e-mail communication, September 8, 2002.

[14]Testimony by Joe Weiss, Consultant, KEMA Consulting, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, July 24, 2002.

[15]For example, see Scott Berinato, "The Truth about Cyberterrorism,"*CIO Magazine*, Vol. 15, No. 11, March 15, 2002.

to voluntarily commit resources, time and effort into reducing their vulnerabilities. Stuart McClure, President and Chief Technical Officer of the security company Foundstone, claims, "[Industries] have fallen into the regulation trap. Unless the government regulates it, they're not yet taking [security] seriously."[16]

The Magnitude of the Terrorist Threat

Some critical infrastructure industry representatives are skeptical that a cyber-terror attack would target industrial control systems.[17] Since there has never been an attack on domestic critical infrastructure industrial control systems which caused intentional damage, even in cases where hackers have successfully broken into these systems, industry representatives believe the cyber-threat to be low. Diane Van de Hei, executive director of the Association of Metropolitan Water Agencies and contact person for the water utility Information Sharing and Analysis Center, was quoted as saying, "If we had so many dollars to spend on a water system, most of it would go to physical security."[18]

Some industry representatives also emphasize that the unfamiliar and uncommon commands used in legacy industrial control systems will continue to provide as high a barrier to future destructive attempts as it has in the past.[19] While utility industry leaders agree that they have been the target of millions of cyber-security incidents, some do not analyze the origin or method of attack. Will Evans, vice president of IT services at People's Energy Corp., reportedly claimed, "[A large utility] could have a million [intrusion] events that need to be analyzed. I don't think anybody has the capability to do that in-house."

Utility industry representatives contend that the vast majority of such intrusions are searches for vulnerable computers in the corporate network by inexperienced hackers, and, of the dangerous minority actually performed by experienced crackers, many are focused on economic aspects of the corporate network rather than the industrial control systems network.[20] From the perspective of critical infrastructure industries, discontented employees who possess inside information about industrial control systems are a greater security risk than external attempts to breach security.

There is evidence that al Qaeda is interested in the vulnerabilities of the U.S. public and private utilities. The discovery in Afghanistan of a computer containing structural analysis programs for dams combined with an increase in Web traffic

---

[16]Robert Vamosi, "Cyberterrorists Don't Care About Your PC," *ZDNet Reviews*, July 10, 2002.

[17]Bill Wallace, "Security Analysts Dismiss Fears of Terrorist Hackers," *San Francisco Chronicle*, June 30, 2002.

[18]Robert Lemos, "What Are the Real Risks of Cyberterrorism?" *ZDNet*, August 26, 2002.

[19]Scott Berinato, "Debunking the Threat to Water Utilities," *CIO Magazine*, Vol. 15, No. 11, March 15, 2002.

[20]Bill Wallace, "Security Analysts Dismiss Fears of Terrorist Hackers," *San Francisco Chronicle*, June 30, 2002.

relating to SCADA systems[21] prompted the National Infrastructure Protection Center to issue a warning information bulletin.[22] A recent analysis of cyber-attack data collected during the second half of 2001 showed that energy industry companies are attacked twice as often as other industries, and that a large number of these attacks originate from the Middle East.[23] Additionally, according to one expert, these statistics do not reflect intrusions directed at control systems which lack firewalls or intrusion detection systems, resulting in an under-reporting of the actual number of attacks.[24]

There have been examples of individuals specifically breaking into utility companies' control systems. The most notable event occurred in Maroochy Shire, Australia, where, in Spring, 2000, a discontented former employee was able to remotely access the controls of a sewage plant and discharge approximately 264,000 gallons of untreated sewage into the local environment.[25] In 1994, a hacker successfully broke into the computer system of the Salt River Project in Arizona.[26] Another example, from March, 1997, occurred when a teenager in Worcester, MA was able to remotely disable part of the public telephone switching network, disabling telephone service for 600 residents, including the fire department, and causing a malfunction at the local regional airport.[27] Reportedly, an intrusion into the SCADA systems of a global chemical company occurred where a former employee attempted to disable chemical operating systems at a production plant.[28]

Often, it is difficult to assess from public reports to what degree a critical infrastructure industry has been breached.[29] For example, a cyber-break-in at the California Independent System Operator (Cal-ISO), California's primary electric power grid operator, went undetected for 17 days in April, 2001. Greg Fishman, a representative of Cal-ISO, reported the intruders "never really got close at all to our operational systems that run the grid."[30] It is not clear what information was

---

[21]Sean Webby, "4 Cities Take Data Off Web; Authorities Remove Info After Hits From Mideast," *San Jose Mercury News*, June 28, 2002.

[22]"Terrorist Interest in Water Supply and SCADA Systems," National Infrastructure Protection Center, Information Bulletin 02-001, January 30, 2002.

[23]Dan Verton, "Vulnerability Assessment Triggers Alarms," *Computerworld*, January 21, 2002.

[24]Joe Weiss, KEMA Consulting, private e-mail communication, September 8, 2002.

[25]A summary of this event can be found in National Infrastructure Protection Center, *Highlights*, 2-03, June 15, 2002.

[26]Robert Lemos, "What are the Real Risks of Cyberterrorism?" *ZDNet*, August 26, 2002 found online at [http://www.msnbc.com/news/799234.asp].

[27]"Juvenile Hacker Charged with Disabling Airport Control Tower Telephones," *Agence France Press*, March 18, 1998.

[28]Esther D'Amico, "Cybersecurity Gains Momentum," *Chemical Week*, August 21, 2002.

[29]*Ibid.*

[30]Dan Verton, "California Hack Points to Possible Surveillance Threat; Power Grid (continued...)

compromised during the intrusion, who the perpetrators were, or what their goal in gaining access was. To date, there has been no indication that the perpetrators of this attack were able to access any sensitive information or systems.

Potential Consequences of a Terrorist Attack

The consequences of an attack on the industrial control systems of critical infrastructure could vary widely. It is commonly assumed that a successful cyber-attack would cause few, if any, casualties, but might result in loss of service while control was wrested from the attacker and any damage repaired. For example, an attack on the public telephone switching network might deprive customers of telephone service for a number of hours while technicians reset and repaired the switching network. An attack on a chemical or liquid natural gas plant facility's control systems might lead to more widespread physical damage.

Lower probability events include catastrophic infrastructure failure, where the failure of one part of the infrastructure leads to the failure of other parts, causing widespread effect. This is due to the synergistic effect of infrastructure industries on each other. A simple example might be an attack on electrical utilities where electricity distribution was disrupted; sewage treatment plants and waterworks could also fail, as perhaps the turbines and other electrical apparatuses in these facilities shut down. On August 5, 2002, the faulty closure of an emergency valve at one of Singapore's two natural gas suppliers blocked the flow of natural gas to seven electrical power plants. The resultant power level dropped 30%, and even after reserve power was employed, there was still a 8% shortfall. The power outage lasted up to 90 minutes.[31] Several chemical production plants were forced to shutdown their facilities during the power outage, and required several days to restore full production.[32]

Some experts warn of a cascade event, where a terrorist is able to manipulate control systems and cause catastrophic failure within an infrastructure. Cascade events can be very damaging, causing widespread utility outages. Twice in 1996, arcing between high voltage transmission lines and trees resulted in widespread power outages. On July 2, 1996, a cascade event left 2 million customers in 11 states and 2 Canadian provinces without power.[33, 34] Most service was restored within 30

---

[30](...continued)
Unaffected; Perps Unidentified," *Computerworld*, June 18, 2001.

[31]Krist Boo and Tan May Ping, "90-Minute Blackout in Several Areas," *The Straits Times (Singapore)*, August 6, 2002, and Krist Boo, "Computer Glitch Behind Worst Blackout in Decade," *The Straits Times (Singapore)*, August 15, 2002.

[32]Sam Cage, "Power Failure Downs Three Singapore Crackers," *Chemical Week*, August 14, 2002.

[33]Susan Reed, "Massive Power Outage in West Still Unexplained," *CNN*, July 3, 1996.

[34]Bonneville Power Administration, "Tree Triggers Power Outage," *Journal*, August, 1996, found online at [http://www.bpa.gov/Corporate/KCC/jl/96jl/jl0896x.shtml].

minutes.[35] On August 10, 1996, a similar event caused 7.5 million customers in seven western states and part of Canada to be without power for up to nine hours.[36]

The scenario which causes the highest degree of concern among experts is the combined use of a cyber-attack on critical infrastructure in conjunction with a physical attack.[37] This use of cyber-terrorism could result in an amplification of the physical attack's effects. An example of this might be a conventional bombing attack on a building combined with a temporary denial of electrical or telephone service. The resulting degradation of emergency response, until back-up electrical or communication systems can be brought into place and used, could increase the number of casualties and public panic.

Others believe that the consequences of a cyber-attack on critical infrastructure would be very limited, and that excessive focus has been given to an unsubstantiated threat.[38] Cyber-security experts who doubt the effectiveness of such an attack range in opinion regarding an attack's impact. Some believe that a cyber-attack on critical infrastructure control systems, while having some effect, would not be devastating, but rather only a minor inconvenience.[39] Other believe that there would be significant impacts from such an attack on control systems, but that such success would be very unlikely.[40]

Current Initiatives

The creation of the Department of Homeland Security has centralized within the Directorate of Information Analysis & Infrastructure Protection a number of offices related to critical infrastructure control system security: the Critical Infrastructure Assurance Office (CIAO), the National Infrastructure Protection Center (NIPC), the National Infrastructure Simulation and Analysis Center (NISAC), and the Department of Energy's Office of Energy Assurance.[41]

---

[35]"Parts of Idaho Darkened by Power Outage, Earlier Western Blackout Traced to Short Circuit," *CNN*, July 3, 1996.

[36]John F. Hauer and Jeff E. Dagle, "Consortium for Electric Reliability Technology Solutions Grid of the Future, White Paper on Review of Recent Reliability Issues and System Events," prepared for Transmission Reliability Program, Office of Power Technologies, Assistant Secretary for Energy Efficiency and Renewable Energy, U.S. Department of Energy, August 30, 1999.

[37]For an overview of this type of scenario, see National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academy Press, Washington, DC, 2002.

[38]Joshua Green, "The Myth of Cyberterrorism," *The Washington Monthly*, November, 2002.

[39]Steve Alexander, "Some Experts Say Cyberterrorism Is Very Unlikely," *Star Tribune* , February 13, 2003.

[40]Mark Harrington, "In Cyber-Attack, The System Bends, Doesn't Break," *Newsday*, February 11, 2003

[41]Homeland Security Act of 2002, P.L. 107-296.

CIAO and NIPC were created in response to Presidential Decision Directive No. 63, issued in 1998.[42] CIAO coordinates the federal government's initiatives on critical infrastructure assurance and promotes national outreach and awareness campaigns about critical infrastructure protection. NIPC is a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response agency. Among other programs, NIPC has developed the InfraGard program, which serves as a clearinghouse for information sharing and analysis for members of critical infrastructure industries.

NISAC was created in 2001 through the passage of the USA PATRIOT Act. It is charged to "serve as a source of national competence to address critical infrastructure protection and continuity through support for activities related to counterterrorism, threat assessment, and risk mitigation."[43] This center is to provide modeling and simulation capabilities for the analysis of critical infrastructures, and is located at Sandia National Laboratories and Los Alamos National Laboratory.

The Department of Energy's Office of Energy Assurance has also been involved in developing techniques to secure energy production and availability.[44] Part of this effort has been the development of "simple, common-sense approaches to improve the overall level of protection in SCADA and digital control networks."[45] A document describing a general approach to improving cyber security in SCADA systems has been released.[46]

Critical infrastructure industries have also developed non-profit organizations called Information Sharing and Analysis Centers (ISACs) to allow industry sector members to share security information in a private forum. Additionally, some critical infrastructure industries have launched initiatives in developing infrastructure security programs.[47] Information sharing, especially regarding the magnitude and nature of observed cyber-attacks, vulnerabilities and their solutions, is seen as an important step in preparing for and protecting against cyber-terror.

There has been limited public/private cooperation on divulging information about and technical solutions to discovered vulnerabilities. Because of perceived limitations in Freedom of Information Act (FOIA) exemptions, industry

---

[42]Presidential Decision Directive No. 63 set as a national goal the ability to protect the nation's critical infrastructure from intentional attacks. For more information regarding this directive and other critical infrastructure policy, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation* by John D. Moteff.

[43]USA PATRIOT Act, P.L. 107-56, Section 1016.

[44]The Department of Energy's Office of Energy Assurance can be found online at [http://oea.dis.anl.gov/oea_home.html].

[45]Remarks of James F. McDonnell, Director of the Office of Energy Assurance, September 19, 2002, found online at [http://oea.dis.anl.gov/mcdonnell_remarks.html].

[46]"21 Steps to Improve Cyber Security of SCADA Networks," Department of Energy, 2002.

[47]The Electric Power Research Institute, for example, has developed a series of primers addressing information security within the energy and power industry. For more information about the Electric Power Research Institute, see [http://www.epri.com].

representatives have generally limited the quantity and quality of information volunteered to the government. Also, the ISAC system has not risen to its full potential in all critical infrastructure areas, due to fears over disclosure of sensitive corporate information to competitors. In testimony before the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, Bill Smith, Chief Technology Officer of the BellSouth Corporation stated,

> With respect to FOIA, many companies are hesitant to voluntarily share sensitive information with the government because of the possible release of this information to the public. BellSouth currently shares cyber-related intrusion information with the Telecom Information Sharing and Analysis Center–the Telecom ISAC–located within the NCC. However, because of the concerns just noted, the information sharing 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. This is neither maximally efficient nor effective.[48]

Partially in an effort to address these concerns, the Homeland Security Act of 2002 created a new FOIA exemption for critical infrastructure information:

> Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement ... shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act).[49]

The breadth of this exemption has caused concern that information showing safety violations or consumer hazards could be hidden through such an exemption.[50] At the confirmation hearing of Homeland Security Secretary Ridge, Senator Levin noted that the exemption language should be clarified:

> The Freedom of Information Act language has got to be clarified. We are denying the public unclassified information in the current law which should not be denied to the public. ... [Y]ou could get information that, for instance, a company is leaking material into a river that you could not turn over to the EPA. If that company was the source of the information, you could not even turn it over to another agency. It means that a member of Congress that finds out about that information through oversight cannot act on that information, even though its unclassified information. We would be stymied from acting on it, making it

---

[48]Testimony of Bill Smith, Chief Technology Officer of the BellSouth Corporation before the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, July 9, 2002.

[49]Homeland Security Act of 2002, P.L. 107-296.

[50]Lauren Weinstein, "Taking Liberties With Our Freedom," *Wired News*, December 2,2002.

> public, for instance, or doing anything else in relation to information which comes to us or comes to you as a result of a voluntary submission.[51]

For more information on this topic, see CRS Report RL31547, *Critical Infrastructure Information Disclosure and Homeland Security*, by John D. Moteff and Gina Marie Stevens.

In another vein, research is currently underway at Department of Energy laboratories to address process control system security. For example, Sandia National Laboratory under the Laboratory Directed Research and Development program has developed secure control systems for the energy industry.[52] Research includes new information architectures, cryptographic methods, and information system security assessments. Much of this work arises from needs discovered through partnerships with systems manufacturers. While a prototype system to demonstrate proof of principle has been implemented at the Sandia National Solar Thermal Test Facility, this system has not been widely implemented in the field.[53] Similar security efforts, though less directly focused on industrial control systems, are being developed at both Lawrence Livermore National Laboratory and Los Alamos National Laboratory. A SCADA testing facility is currently supported by the Idaho National Engineering and Environmental Laboratory, where control system security technologies can be tested.[54]

The National Institute of Standards and Technology has initiatives in industrial control system security. They, in conjunction with a number of industry groups, federal government agencies and professional societies, have created the Process Control Security Requirements Forum to develop process control information security requirements. Through their Critical Infrastructure Protection Grants Program, the National Institute of Standards and Technology provided in fiscal year 2001 roughly $5 million for research in critical infrastructure protection, some of which was focused on industrial control systems.[55] This program has not been further funded.

The President's Critical Infrastructure Protection Board has released *The National Strategy to Secure Cyberspace*, in which a general strategic overview, specific recommendations and policies, and the rationale for these actions are

---

[51]Hearing on the Nomination of Tom Ridge to be Director of Homeland Security, Senate Committee on Government Affairs, January 17, 2003.

[52]Rolf Carlson, "Sandia SCADA Program High-Security SCADA LDRD Final Report," Sandia Report SAND2002-0729, Sandia National Laboratories, April, 2002.

[53]Sandia National Laboratories, "Dish/Sterling Provides Test for Secure Control System," *Sandia Technology*, Vol. 3, No. 1, Spring, 2001.

[54]Testimony of Billy D. Shipp, President and Laboratory Director, Idaho National Engineering and Environmental Laboratory, before the Senate Committee on Energy and Natural Resources, July 10, 2002.

[55]For more information on the Critical Infrastructure Protection Grants Program and the Process Control Security Requirements Forum, see [http://www.mel.nist.gov/proj/cip.htm].

presented.[56] This document addresses concerns regarding digital control systems and SCADA networks, rates SCADA network security as a national priority, and recommends joint public/private efforts in discovering solutions to potential vulnerabilities. This strategy identifies the Department of Homeland Security, in coordination with other federal agencies, as the department responsible for developing best practices and new technologies to increase SCADA security. Some cyber-security experts have criticized this plan, claiming that vulnerabilities will remain because of its lack of enforcement regulations.[57]

Policy Options

Several policy options may decrease the vulnerability of industrial control systems. One option is for the federal government to mandate and enforce a uniform security standard for industrial control systems. Because of the national importance of critical infrastructure systems, a uniform standard might be developed, with the input of advocates, industries and the federal government, which would include the functionality necessary to protect industrial control systems. A voluntary, standards-based approach has been developed for server operating systems with some success, and a similar mechanism could be used to develop standards for commercial off-the-shelf control systems.[58] Alternately, processes and specifications currently being developed through federal programs might be generalized to other critical infrastructure industries and established as a universal standard. Critics of this approach cite the many different uses of industrial control systems in different industry sectors as making such a standard unwieldy. They also contend that a mandated standard would be less effective than a voluntary standard, as solutions to new problems could not be implemented immediately, but would wait for changes to the standard.

Another option would involve supporting encryption research to protect industrial control system data transfer. Encrypting the information transmitted between remote units and their controllers would inhibit inclusion of false information to and from industrial control systems. Current encryption technology is not compatible due to the time required to process the encrypted data. Industrial control systems have stringent timing requirements and tend to be built out of less computationally robust components, which complicate the use of current encryption technologies. While a prototype encryption method for industrial control systems has been developed, it is not widely tested or implemented in industry.[59] Further research into encryption techniques for these processes could provide efficient, market-driven technology for securing industrial control systems information.

---

[56]*The National Strategy to Secure Cyberspace* is available for download at the President's Critical Infrastructure Protection Board website, found online at [http://www.whitehouse.gov/pcipb/].

[57]Robert Lemos, "Bush Unveils Final Cybersecurity Plan," *CNET News*, February 14, 2003.

[58]The Center for Internet Security, a not-for-profit organization, develops consensus security standards for computer systems. They can be found online at [http://www.cisecurity.org/].

[59]Jennifer Alvey, "Digital Terrorism: Holes in the Firewall? Plugging Cyber Security Holes Isn't as Easy as Everyone Wants to Think," *Public Utilities Fortnightly*, March 15, 2002.

The new FOIA exemptions created in the Homeland Security Act of 2002 may provide a higher volume, freer exchange of information between the federal government and industry, as industry may become more forthcoming about potential vulnerabilities. Policymakers may wish to inquire into whether vulnerabilities transmitted to the federal government are eventually reduced, and how the information being provided to the federal government is used.

Policymakers may also wish to assess the effectiveness of the Department of Homeland Security in coordinating security enhancements to control systems, promoting government/industry partnerships, and performing risk and vulnerability assessments. With the concentration of previously existing agencies into the Directorate of Information Analysis and Infrastructure Protection, previous duplication of effort may be removed, but critics have suggested that difficulties in integrating these agencies may lead to a reduction in effectiveness.