

Statement for the Record  
July 21, 2009 Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and  
Science and Technology  
Brian M. Ahern – President & CEO  
Industrial Defender, Inc.

Thank you for the opportunity to submit written testimony regarding efforts to secure the modern electric grid from physical and cyber attacks. I appreciate the Subcommittee examining these important issues and am grateful for your willingness to consider my views.

I am the President and CEO of Industrial Defender, Inc., a provider of cyber risk protection with over 18 years of industrial control system and SCADA industry experience and more than seven years of industrial cyber security experience. Industrial Defender has completed more than 100 process control/SCADA cyber security assessments, more than 10,000 global technology deployments in securing critical infrastructure systems, more than 3,000 mission critical SCADA deployments and provides managed security services for 170 process control plants in 21 countries. My comments on the Subcommittee's hearing topic follow.

Protecting the U.S. Electric Power Infrastructure from Physical and Cyber Attacks

The Federal government has a responsibility to protect our nation's electric power infrastructure from physical or cyber attacks to ensure the social, economic, health and safety of our citizens. There has been a significant increase in malicious cyber attack attempts on critical infrastructure electric power entities from suspected terrorists and even adversarial nations and more action is needed to fortify our nation's electric power cyber defenses in order to combat the potentially dangerous threats. A recent coordinated cyber attack on the United States and South Korea, which may have originated in North Korea, involved the malicious use of more than 100,000 computers. Though this particular attack was not targeted at U.S. electric power interests, it does suggest that more needs to be done in order to improve our nation's cyber defenses.

The majority of electric power assets in the U.S. are owned and operated by private sector entities. Based upon private sector contracts executed by Industrial Defender over the past seven years to assess and mitigate cyber-risk specific to critical infrastructure industries, including electric power, oil and gas, water, transportation and chemical sectors, we have found that industries with cyber security regulatory mandates in place, including the Chemical and Electric Power sectors, are industries taking a leadership role in protecting their digital infrastructure assets. Having regulations in place, however, does not guarantee 100 percent compliance or protection. There have been significant challenges within industries for which mandatory compliance standards have been implemented. A recent letter to electricity industry stakeholders from Michael Assante, the Chief Security Officer for the North American Electric Reliability Corporation (NERC) dated April 7, 2009, raised concern over the identification of Critical Assets and Critical Cyber Assets (NERC CIP-002), which are defined as those "facilities, systems and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." Results from a survey published for the July 1 – December 31, 2008 period suggest that certain qualifying assets may not have been identified as "Critical". Of particular concern were qualifying assets owned and operated by electric power generation owners and operators, of which only 29 percent reported identifying at least one critical asset, and transmission owners, fewer than 63 percent of which identified at least one critical asset. This inaction by electricity asset owners and operators regarding mandatory compliance requirements gives rise to great concern over the ability of any voluntary private sector compliance program to be effective. There is a risk that industries that do not have compliance mandates may be willing to play the percentages that a critical infrastructure incident will not happen at their company, rather than spend thousands or even millions of dollars to mitigate any known risks and vulnerabilities.

Statement for the Record  
July 21, 2009 Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and  
Science and Technology  
Brian M. Ahern – President & CEO  
Industrial Defender, Inc.

Ensuring the reliability and security of the bulk electric system must be a cooperative and shared responsibility between private sector organizations and the Federal government. This should include the Federal government overseeing a coordinated effort between public sector and private sector entities to enhance and enforce the NERC CIP standards; drive cyber security awareness and education within the public and private sector; require vendor commercial information security credentials; provide crucial sharing of information regarding cyber incidents, vulnerabilities and best practices; provide a cyber-security implementation funding incentive; and, offer “Safe Harbor Protection” for private sector companies, ensuring the elevation of threat and vulnerability information to the Federal government while at the same time increasing public awareness and protection.

Industry Compliance with NERC Standards

In addition to the North American Electric Reliability (NERC) survey, which raises concerns over the inaction of bulk electricity asset owners and operators, some bulk electricity providers may be taking a “defensible audit position” in lieu of a well designed cyber-risk mitigation strategy. It is our opinion that this behavior is the result of non-descriptive and prescriptive requirements in the current NERC-CIP standards that leave determination of a risk-mitigation strategy solely to the discretion of industry. Additionally, it is important to note that up to the latest revision of the NERC CIP standards, asset owners and operators were permitted to apply “reasonable business judgment” in determining risk-mitigation strategy for critical assets.

The current industry spread relative to interpretation and action around the current NERC CIP standards is extremely broad. Based upon experience, significant action was taken by industry in assessing cyber-risk through contracting third parties to provide independent NERC CIP gap analysis, network design reviews, vulnerability assessments, penetration testing, and NERC CIP compliance training. Much of this work was done in advance of the December 31, 2008 deadline; however, many utilities remain very active in performing this work relative to their operational assets. What is more concerning, regarding NERC CIP compliance, is the slow pace at which industry is adopting technology required to meet NERC CIP-005 and NERC CIP-007 compliance, specifically, establishing Electronic Security Perimeter and System Security management for all Critical Cyber-Assets. It is evident, as represented in Mr. Assante’s April 7, 2009 letter to Industry Stakeholders, that the definition of a “Critical Asset”, and associated “Critical Cyber-Asset”, has been viewed differently between the private sector and NERC. The private sector’s interpretation, and hence subsequent identification of critical assets, has resulted in actions that seem contrary to the defined objectives of securing the nation’s critical infrastructure.

In one example, a major U.S. electric power provider considered implementing intrusion detection monitoring technology to mitigate cyber security risks and vulnerabilities in order to secure its substations and meet the required NERC-CIP compliance standards. Currently, the NERC-CIP compliance standards focus on “routable communication protocols” and exclude “non-routable communication protocols” and “communication links”. The electric power entity eventually made a cost conscious decision to convert all of its substations to a non-routable communication protocol SCADA network. As a result, it did not move forward with the substation equipment upgrade, resulting in a move backwards instead of using technology to enhance cyber-security, workplace efficiency and productivity.

With over 150 investor owned utilities, government owned and operated utilities and a number of smaller municipal electric entities falling under the jurisdiction of the NERC CIP standards, there should be significant demand for monitoring technology to support NERC CIP requirements. Unfortunately, the purchasing

Statement for the Record  
July 21, 2009 Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and  
Science and Technology  
Brian M. Ahern – President & CEO  
Industrial Defender, Inc.

behavior of bulk electricity providers does not match the number of monitoring sensors needed to support the NERC CIP standards.

Government Efforts to Secure Control Systems and the Electric Industry From Physical and Cyber Attacks

Escalation of threats and exposure of incidences are essential components of successfully thwarting cyber attacks against the nation's critical infrastructure. With 85 percent of the nation's critical infrastructure owned and operated by the private sector, the public and private sectors must work collaboratively, with trusted and open lines of communication, to ensure the timeliest communication of critical cyber-security information. Relying solely on Federal government intelligence agencies to identify the threat is a shortsighted strategy. The private sector represents the most valuable source of operational intelligence, which must be harnessed in order to effectively communicate and drive action to reduce the consequences of pending attacks.

Operational systems (SCADA/Process Control Systems) used to safely and reliably operate critical infrastructure in electric power, water, energy, chemicals and transportation sectors lack the necessary security technology to escalate cyber-threats and expose cyber-incidences in real-time so that appropriate action (communication, emergency orders/actions, etc) can be taken to minimize the impact on national security, public safety, and economic interests.

Greater investments in "Defense in Depth Sensor Technology," including electronic security perimeter, remote access and authentication, network intrusion detection, host intrusion detection, and patch monitoring and management, will enable real-time aggregation of threats and incidences for real-time reporting. FERC Order 706 also calls for "defense-in-depth" subject to technical feasibility considerations with NERC oversight.

Through the deployment of Defense in Depth Sensor Technology, the U.S. Department of Homeland Security (DHS) should assume the role of "Critical Infrastructure Threat Clearing House." The goal of the Critical Infrastructure Threat Clearing House is to establish lines of communication between asset owners and operators and DHS to warn the public of potentially dangerous, malicious, and non-malicious cyber security incidents. It is recommended that DHS establish a "cyber heat map," populated with intelligence by Defense in Depth Sensor Technology, which would provide transparency into the current cyber security threats facing the nation, as well as supply access to detailed information on each specific threat occurrence. However, for this to be effective, safe harbor protection should be afforded to the private sector reporting party (see below).

Pending Legislation and Coverage of the Electric Sector

Cooperation between private sector organizations and the Federal government will need to be achieved to enable increased cyber security protection as well as flexibility to expand these infrastructure platforms to support future needs. To this end, legislation pending before Congress could be strengthened to better achieve the separate goals of the private and public sectors as well as increased public safety. Important issues that are not currently part of the legislative proposals are outlined below.

- A distinct lack of threat visibility due to the slow adoption of technology designed to both detect and protect against cyber security threats.

Statement for the Record  
July 21, 2009 Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and  
Science and Technology  
Brian M. Ahern – President & CEO  
Industrial Defender, Inc.

- Inclusion of safe harbor protection for private sector companies, ensuring the elevation of threats and vulnerabilities to the Federal government, resulting in increased public awareness and protection.
- An absence of specific descriptive and prescription recommendations for critical infrastructure systems and requirements.
- Mechanisms to enable a more efficient and timely means of issuing standards through granting FERC “authorship” responsibility. Presently the NERC Standards processes are largely created and approved by industry and hence are somewhat self-policing.
- Require any full- or part-time contractor with privileged access to critical infrastructure control related information system to obtain commercial cyber security credentials.
- Provision to increase availability of funds for cyber security related equipment and staffing.

Any final legislation promoting public and private sector collaboration should include the following recommendations.

- More Descriptive Definition of Critical Cyber-Assets: It is essential that any final legislation specifically identify which critical cyber-assets need to be secured. As it relates to SCADA/Process Control System security requirements, all computer or microprocessor-based operational devices used to monitor, control, or analyze the critical infrastructure where accurate timing has been deemed necessary must be included to ensure the integrity of the critical infrastructure. These devices include, but are not limited to: Power Plant Automation Systems; Substation Automation Systems; Programmable Logic Controllers (PLC); Intelligent Electronic Devices (IED); sequence of event recorders; digital fault recorders; intelligent protective relay devices; Energy Management Systems (EMS); Supervisory Control and Data Acquisition (SCADA) Systems; Plant Control Systems; routers; firewalls; Intrusion Detection Systems (IDS); remote access systems; physical security access control systems; telephone and voice recording systems; video surveillance systems; and, log collection and analysis systems.
- Remove the Exclusion of “Non-routable Protocols” and “Communication Links”: This exclusion is being used as a work-around to avoid implementation costs. FERC Order 706 includes comments from the ISA99 Industrial Automation and Control Systems Security Team objecting to the exclusion of communication links from CIP-002-1 and non-routable protocols from critical cyber assets. The comments argue that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable – through testing and experience.
- Bolster Public/Private Clearing House: It is increasingly essential that private sector asset owners and operators work collaboratively with the government to warn the public of potentially dangerous malicious and non-malicious cyber security incidents. Through the deployment of Defense-in-Depth Sensor Technology, the U.S. Department of Homeland Security (DHS) should assume the role of “Critical Infrastructure Threat Clearing House.” The goal of the Critical Infrastructure Threat Clearing

Statement for the Record  
July 21, 2009 Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and  
Science and Technology  
Brian M. Ahern – President & CEO  
Industrial Defender, Inc.

House is to establish lines of communication between asset owners and operators and DHS to warn the public of potentially dangerous, malicious, and non-malicious cyber security incidents. It is recommended that DHS establish a “cyber heat map” populated with intelligence by Defense in Depth Sensor Technology, which would provide transparency into the current cyber security threats the nation faces, as well as supply access to detailed information on each specific threat occurrence. In order for this to be effective, safe harbor protection should be afforded to the private sector reporting party (see below).

- Include Recommendation of Descriptive and Prescriptive Solutions: Any final legislation should require the deployment of Defense-in-Depth Sensor Technology throughout the entire SCADA/Process Control System network environment. Defense-in-Depth Sensor Technology includes electronic security perimeter, remote access and authentication, network intrusion detection, host intrusion detection, and patch monitoring and management. Equipping critical infrastructure systems with the appropriate security sensor technology enables real-time aggregation of threats and incidences for real-time reporting to the appropriate authorities.
- Provide “Safe Harbor Protection”: Presently there is no “Safe Harbor Protection” afforded to the private sector for open “escalation of threats, exposure of incidences” with the Federal government. Without these protections in place, private sector companies will be less inclined to share the information and risk potential negative public exposure. Legislation pending before Congress attempts to address this issue by providing protection to disclosed cyber-security data; however, the proposals do not provide a similar protection to the disclosing entity. In order to ensure open communication from the private sector, it is essential to provide privacy protection for both the disclosing entity and the disclosed cyber security data. As a means of bridging the communication gap between public sector and private sector, safe harbor protection should be provided to private sector companies escalating threats and/or exposing incidences with the Federal government. This protection is not intended to provide a safe harbor from accountability, but instead to provide protection to share information with the appropriate authorities. The U.S. Department of Defense’s (DOD) Defense Industrial Base Cyber Security and Information Assurance (CS/IA) pilot program initiative, launched in early 2008, offers a potential model on this issue. The DIB/CSIA has five major components: (1) a binding bilateral DOD-DIB company framework agreement to facilitate CS/IA cooperation; (2) threat and vulnerability information sharing; (3) DIB network incident reporting; (4) damage assessments; and (5) DOD acquisition and contract changes. Some of these components might be relevant to establishing a similar relationship between the Federal government and private sector critical infrastructure companies.
- Grant FERC Authorship Responsibility: Presently, the NERC Critical Infrastructure Protection (CIP) standards [CIP-002 – CIP-009] provide electric utility private sector guidance on the subject of cyber security. Pending legislation would provide FERC with emergency authorities to issue actions/orders in the event of a known cyber-security threat to the electric utility infrastructure. These actions/orders would remain in effect over a defined period of time until they are incorporated into a standard, and/or the threat is mitigated, or the order/action expires.

The NERC CIP standards are self-policing in that they are created and approved by industry. According to FERC Chairman Jon Wellinghoff in his April 28, 2009 letter to U.S. Representative Edward J. Markey, “The commission is committed to exercising all of the authority that Congress has

Statement for the Record  
July 21, 2009 Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and  
Science and Technology  
Brian M. Ahern – President & CEO  
Industrial Defender, Inc.

given it to help protect the power grid. However, Congress needs to be aware that the Commission's current authority is not sufficient to ensure the cyber security of the grid. The existing process is based on industry consensus and is, therefore, too slow, subject to disclosure to potential attackers, and not responsive enough to adequately address matters that affect national security."

Granting FERC emergency authorities to act in the event of a threat or incident is the reactive element of protecting our nation's critical infrastructure. Who is responsible for the proactive element of mitigating our risks, escalating the threats and exposing our incidences?

In addition to having emergency authorities, FERC should be granted authorship responsibilities for future cyber-security standards to ensure the protection and integrity of the nation's electric utility infrastructure. FERC can continue to leverage NERC for the creation of the standards; however, in the interest of ensuring timely, descriptive and prescriptive cyber-security standards, FERC must have the authority to author and issue such standards. Industry input is important to drive public sector-private sector collaboration; however, the present self-policing standards leave the nation's ability to secure the electric utility infrastructure in a timely manner vulnerable.

- Require a Commercial Cyber Security Credential: Any full- or part-time contractor with privileged access to a critical infrastructure control information system, regardless of job or occupational series, would need to obtain a commercial cyber security credential accredited by ANSI or an equivalent authorized body. The credential would also require maintaining certified status with a certain number of hours of continuing professional education each year. This program would be phased in and have a similar framework as DOD Directive 8570.1 Information Assurance Training, Certification, and Workforce Program.
- Cyber Security Implementation Monetary Incentives: This could be similar in concept and scope to the renewable energy incentives passed in the Emergency Economic Stabilization Act of 2008 and/or the smart grid incentives of the American Recovery and Reinvestment Act of 2009 (ARRA).

#### Intrusion Detection Technology and Identification of Cyber Attacks

Industrial networks, while sharing many of the same technologies as business networks, differ enough from business networks to make many conventional threat management approaches ineffective. Industrial networks tend to be more static and predictable than business networks. Safety and effectiveness testing costs for industrial networks are very high, and the effects of technologies like anti-virus scanning and even security patch management on these computers is unpredictable enough that no such technologies can be used safely without incurring very high costs. Industrial networks tend to be tightly controlled – generally conventional office tools such as word processors, presentation tools and email clients are not found on legacy industrial networks. However, modern industrial leverage base Internet protocols like TCP and HTTP layer on top of these base protocols a large variety of control-system-custom protocols like Modbus, DNP3, ICCP and IEC 61850, which are never seen on business networks.

The present lack of investment in equipping industrial network systems with real-time security sensors to provide visibility into the current cyber-security threats, vulnerabilities and incidences plaguing them has emerged as both a necessary and dangerous initiative in terms of cyber security protection. Based on historical risk and vulnerability assessment data captured from Industrial Defender professional services field

Statement for the Record  
July 21, 2009 Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and  
Science and Technology  
Brian M. Ahern – President & CEO  
Industrial Defender, Inc.

teams, most SCADA environments contain latent vulnerabilities, likely with compiled exploits, and are not discovered, on average, until almost a year later (331 days).

As a result, it is necessary to carefully evaluate security technologies and techniques before deploying them on industrial networks and computers. Through the evaluation of many technologies over the last five years, Industrial Defender has found results that span the entire spectrum from security technologies and procedures that actively impair the effectiveness of industrial networks and control systems, through technologies that do not impair networks, but add no value either, to technologies and approaches that are, in fact, effective and worthwhile at securing industrial networks.

Network intrusion detection systems (NIDS) are an essential component of a defense-in-depth strategy, and there are real benefits in the form of specialized expertise when an outsourced managed service provider manages NIDS sensors. NIDS sensors developed for industrial control systems need to be customized with knowledge of industrial network protocols and systems. The sensors are routinely deployed *inside* the security perimeter of the industrial network, monitoring traffic exchanged between the industrial computers and between those computers and the business network.

Conventional NIDS technologies are “signature-based.” That is, much like the well-known anti-virus (AV) products used on PC workstations, signature-based NIDS use a large set of rules called “signatures” to scan network traffic. Any traffic that matches the signature triggers an alert and may trigger corrective action, as well. A key limitation of conventional signature-based NIDS is that like signature-based AV, signature-based NIDS can only detect attacks that it has a signature for. As new vulnerabilities are found in common computer and network components, new signatures are written to identify communications patterns of attackers trying to take advantage of those vulnerabilities. If an attacker discovers a vulnerability or somehow manages to create an attack vector for a vulnerability before a patch/fix or signature for the vulnerability is available, that attack is called a “zero day” attack. Signature-based NIDS are by definition unable to detect zero-day attacks, because those attacks occur before signatures are available to detect the attacks.

Host intrusion detection systems (HIDS) monitor the operation of computer systems and alert when suspicious activity is detected. The archetypical example of HIDS is an anti-virus system. With NIDS, it is generally possible to monitor networks in a completely passive way, receiving a copy of every message exchanged on a switch, for example, without impairing the communications on the switch in any way. This is important because of the prohibitive cost of re-testing an industrial solution for safety and effectiveness if an after-the-fact security monitoring solution changes the behavior of the network significantly.

Control system HIDS have the same imperative – first do no harm. After-market HIDS must not interfere with the operation of the control system and must not reduce confidence in the correctness of a control system to the point where a prohibitively expensive re-test is required. An industrial HIDS solution must be designed with exactly this criterion in mind. Most enterprise class HIDS interfere with the operation of the host, either by accident or by design, or they insert themselves so deeply into the operating system and kernel of the host computer, that they destroy all confidence in the continued correct and safe operation of the control system.

#### Government Investment in Control Systems R&D

One area of focus should be a centralized clearing house for the correlation of alerts and traffic statistics.

Statement for the Record  
July 21, 2009 Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and  
Science and Technology  
Brian M. Ahern – President & CEO  
Industrial Defender, Inc.

Such central oversight would provide intelligence regarding widespread information gathering and other attacks. For the central correlation to work, cooperation of large, managed service providers and large, self-managed networks is needed, in order to send the necessary standardized alerts, and traffic statistics to the U.S. government. If a central agency was the real-time clearing house for conclusions about traffic patterns and the correlation of such conclusions, that agency would be able to correlate suspicious activities across many industrial networks. Such correlation, especially correlation of traffic profiling results, might allow the central monitoring agency to identify widespread information gathering activities targeted at critical infrastructure networks. Such activity is a logical precursor to a widespread attack on infrastructure. It would also allow a central clearing house to draw conclusions about widespread infections calling out to the internet for instructions from time to time, which might be a sign of a coordinated attack on many sites.

Industrial Defender recommends that the Federal government investigate establishing a program, correlation infrastructures and technologies, and the necessary data exchange standards to permit real-time alerts and traffic statistics to be aggregated centrally. Individually managed security service providers and large industrial security/network control centers would be encouraged – or required – to participate in the program and provide the central authority with the statistics and other information that the agency requires to calculate high level correlations. Such a program could provide government and intelligence agencies with important insights into the health of industrial networks overall, and with insight into sudden changes or widespread patterns indicative of preparations for a large-scale attack.

A second area of focus is to strongly encourage control system vendor partnerships with the U.S. Department of Energy's National Supervisory Control and Data Acquisition (SCADA) Test Bed programs at Idaho National Laboratory and Sandia National Laboratory. There needs to be a continued and raised emphasis on control system security product and technology assessments to identify vulnerabilities and corresponding mitigation approaches when systems are being designed and built.