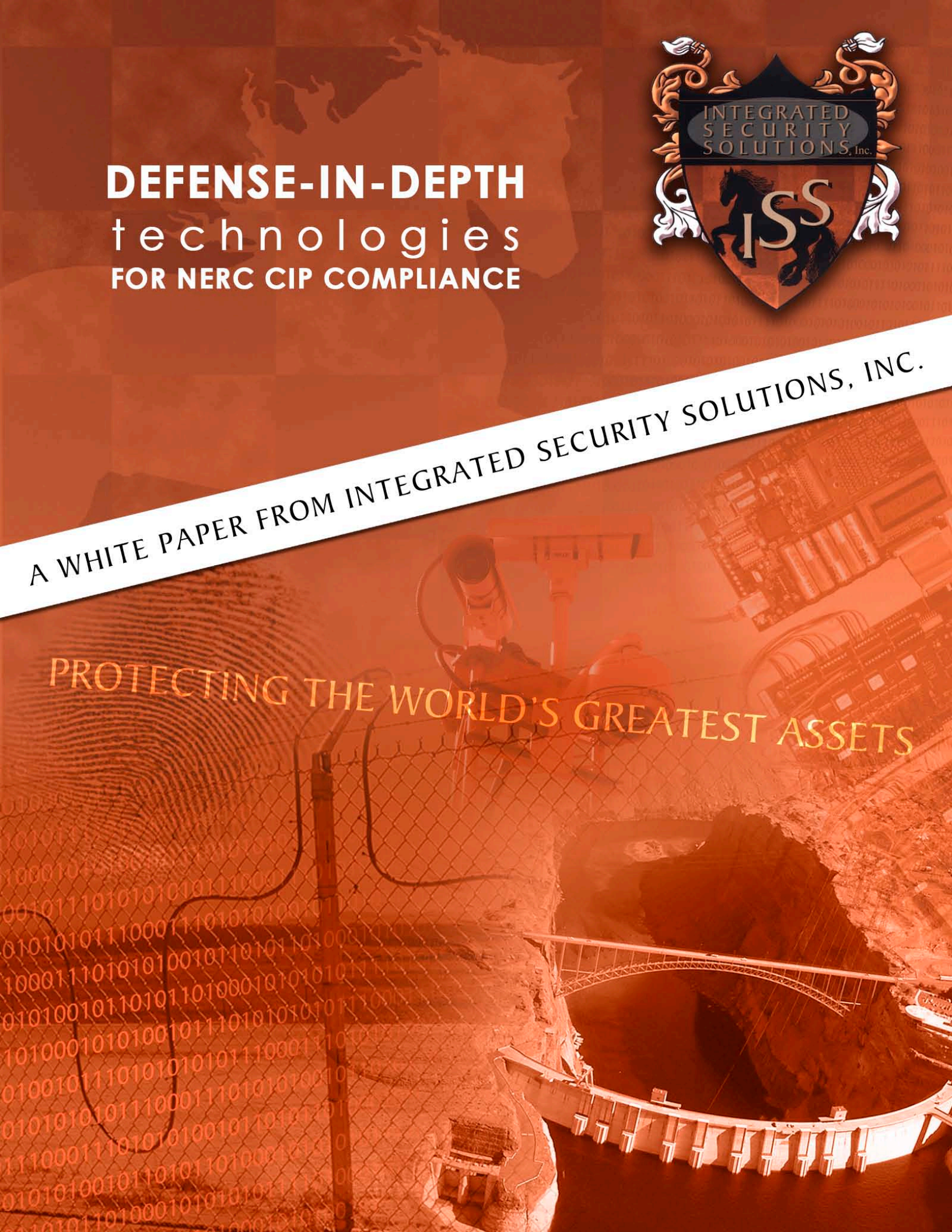
DEFENSE-IN-DEPTH
technologies
FOR NERC CIP COMPLIANCE

A WHITE PAPER FROM INTEGRATED SECURITY SOLUTIONS, INC.

PROTECTING THE WORLD'S GREATEST ASSETS



DEFENSE-IN-DEPTH
t e c h n o l o g i e s
FOR NERC CIP COMPLIANCE

A White Paper

by Integrated Security Solutions, Inc.

THREATS TO CRITICAL INFRASTRUCTURE IN THE UNITED STATES

Stuxnet is the most sophisticated cyber weapon ever deployed, according to present day opinion. Experts who have picked apart the computer worm describe it as far more complex and ingenious than anything imaginable. A sophisticated form of malware, Stuxnet is considered a form of state-sponsored attack or sabotage. Stuxnet infects computer systems by exploiting several vulnerabilities of Microsoft Windows. It targets a specific Siemens SCADA program. It brings a system to a halt and is capable of causing system components to self-destruct while relaying normal operation protocols to monitoring software. Electric utilities, pipelines, railroads and oil companies all use remotely controlled and monitored valves, switches and other mechanisms that are vulnerable to attack.

In April of 2009, the Wall Street Journal published a story entitled “Electricity Grid in U.S. Penetrated By Spies.” The story states that cyber spies penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system. Sources for the story were attributed to current and former national-security officials

> *“The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.’*
>
> *"The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians."*

In 2006, in a project dubbed Aurora, the Department of Homeland Security (DHS) conducted a mock cyber attack on a utility, through Idaho National Labs. The move to SCADA systems, over manually operated systems, boosts efficiency at utilities because it allows workers to operate equipment remotely. But this access to the Internet exposes these once-closed systems to cyber attacks. In project Aurora, the engineers at Idaho National Labs demonstrated this vulnerability by imposing a system exploit to cause any spinning machine connected to the power grid -- such as a generator, pump or turbine -- to self-destruct. These attacks could easily be carried out on vulnerable equipment using the Internet. Video of this dramatized system failure may be viewed at http://www.youtube.com/watch?v=fJyWngDco3g.

Reported intrusions to U.S. Networks include:

- In May 2009, the Department of Transportation (DOT) Inspector General issued the results of an audit of Web applications security and intrusion detection in air traffic control systems at the Federal Aviation Administration (FAA). The Inspector General reported that Web applications used in supporting air traffic control systems operations were not properly secured to prevent attacks or unauthorized access.

- In February 2009, a company based in Cranberry, Pennsylvania, discovered that engineering and communications documents containing key details about the Marine One fleet had been downloaded to an Internet Protocol (IP) address in Iran. The documents were traced back to a defense contractor in Maryland, where an employee most likely downloaded a file-sharing program that inadvertently allowed others to access this information.
- In December 2008, the Federal Emergency Management Administration (FEMA) was alerted to an unauthorized breach of private information when an applicant's personal information pertaining to Hurricane Katrina had been posted on the Internet. The information contained a spreadsheet with 16,857 lines of data that included applicant names, social security numbers, addresses, telephone numbers, e-mail addresses, and other information on disaster applicants who had evacuated to Texas.
- The Government Accountabilities Office (GAO) said in a June 2009 Report to Congressional Committees "the number of incidents [intrusion into the U.S. government networks] reported by federal agencies to US-CERT has risen dramatically over the past 3 years, increasing from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008 (slightly more than 200 percent)."[1]

Primary Infrastructure Targets

Let us focus on one of the primary targets of planned or threatened cyber attacks – The Smart Grid. The Smart Grid is an industry initiative to provide On-Demand electricity to the United States, at present moment market prices. In its utopian state, The Smart Grid encompasses all energy needs for the country, in a seamless and efficient manner, regardless of the source location or type (solar, wind, coal, etc.). This power grid "consists of more than 9,200 electric generating units with more than 1,000,000 megawatts of generating capacity connected to more than 300,000 miles of transmission lines…Because electricity has to be used the moment it is generated, the grid represents the ultimate in just-in-time product delivery. Everything must work almost perfectly, at all times." [2] The system accepts energy from virtually any fuel source, integrating it in a seamless provision of power to the end user.

Attackers have the ability to access SCADA systems and embedded systems, particularly where wireless access points are unguarded. Attackers seek to infiltrate the energy grid to disrupt the American way of life, compromise the U.S. Critical Infrastructures, cripple and weaken U.S. financial markets and other vital business operations, and to distract the public and government from attempts at additional types of attacks. In addition to a denial of service, the most severe threats to energy infrastructure can include the destruction of components through Stuxnet-type invasion.

[1] GAO-09-546 Federal Information Security, INFORMATION SECURITY: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses, Gregory C. Wilshusen, et. al.
[2] The Smart Grid: An Introduction. Prepared for the U.S. Department of Energy by Litos Strategic Communication under Contract No. DE-AC26-04NT41817, Subtask 560.01.04

Let us look at the costs and implications of a large scale attack to the U.S. Smart Grid, by looking at the costs of some outages in our history: [3]

- A rolling blackout across Silicon Valley totaled $75 million in losses.
- In 2000, the one-hour outage that hit the Chicago Board of Trade resulted in $20 trillion in trades delayed.
- Sun Microsystems estimates that a blackout costs the company $1 million every minute.
- The Northeast blackout of 2003 resulted in a $5 billion economic loss to the region.
- The interdependencies of the grid components can bring about a cascading series of failures that could bring our nation's banking, communications, traffic and security systems to a complete standstill.
- The Aurora Project findings by the DHS, project that a successful attack targeted at one third of the North American power grid would cost $700 billion over three months.

In a June 2010 report on High Frequency Low Impact Attacks, the North American Electric Reliability Corporation (NERC) noted "…a single exploitation of a vulnerability can be propagated across a cyber or power system network and potentially affect an entire class of assets at once."

Attack Paths

Embedded Systems

An embedded system contains a computing system that is dedicated to a specific function. Embedded systems in enterprise or industry environments are far more diverse than most people realize. Embedded systems may include refrigerators, thermostats, door locks, handheld devices, smart phones, music players and webcams, in addition to the obvious devices (routers, switches, wireless access points, etc.). These devices have their own IP address and represent as much or more of a security threat than the obvious suspects. These devices must be tracked and secured, maintained and managed just as any other IT system.

Why?

Embedded systems increasingly rely on general-purpose operating systems such as Linux and Microsoft Windows XP Embedded, as these systems are more economical to license and develop, and can leverage open source software. The result – these devices bring to your network, the same vulnerabilities as desktop workstations and servers.

[3] The Smart Grid: An Introduction. Prepared for the U.S. Department of Energy by Litos Strategic Communication under Contract No. DE-AC26-04NT41817, Subtask 560.01.04

Consider this list of embedded devices that can be a threat to the security of a critical facility:[4]

- Checkout or Inventory Wands
- Copiers
- DVRs
- Handheld/Fixed/Portable Medical Devices
- Manufacturing Control Systems
- Multifunction printer/copier/scanner
- Network Music Players
- Networked Medical Devices
- Point of Sale Systems
- Security Cameras
- Security Sensors
- Smart Phones
- Televisions
- Thermostats/Environmental Controls
- Wireless Access Points
- Blue Tooth Technology Devices

Wireless Communication Devices and Access Points

The advent of wireless connectivity and the more recent induction of Cloud computing creates as many potential risks as they eliminate. Every device that offers wireless connectivity also creates an access point to the networks in range of the device. This means that there are potentially unauthorized Wi-Fi networks and access points within a critical infrastructure site. An over reliance on encryption as a defense is a guarantee of defeat – encryption technologies are defeated by technical innovations and human error.

NERC CIP

The reliability standards developed by NERC, based on federal CIP parameters, were put into place and mandated by the inherent risks made apparent by Stuxnet, Aurora and other threats exposed by the implementation of SCADA. The eight CIP standards relating to utilities and cyber protection were meant to ensure that security best practices are being adopted by organizations responsible for systems whose interruption "would have a debilitating impact on security, national economic security, national public health or safety."[5]

[4] *Treat your embedded systems equally*, Q3 2010 Issue of The Barking Seal, a publication of Applied Trust
[5] Presidential Decision Directive PDD-63 of May 1998 - Critical Infrastructure Protection Program (CIP), Patriot Act of 2001 definition of Critical Infrastructure

The Standards and Challenges

NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

CIP-002 Cyber Security - Critical Cyber Asset Identification

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

Two of the defining requirements of note for CIP-002 are:

R3.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter (ESP)

R3.2 The Cyber Asset uses a routable protocol within a control center.

Challenge:

Many utilities routinely permit the operation of cell phones, pagers, wireless bar code readers, and WLAN (Wireless Local Area Network) connections in or near their control centers or substations. CIP compliance is challenged when mobile devices capable of wireless connectivity with wired and wireless interfaces, are able to access a CIP-protected Cyber Asset within the Electronic Security Perimeter (ESP).

CIP-003 Cyber Security - Security Management Controls

Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

Challenge:

If management controls are not monitored for compliance, they are ineffective. Manually managed programs are subject to human error and an inability to follow the lifecycle of authorizations to personnel access, operating system updates and records management. The disparate systems involved in managing full NERC CIP compliance creates a vulnerabilities through a lack of integration of these systems.

CIP-004 Cyber Security - Personnel & Training

Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

Challenge:

The management of records for personnel, including contractors and service vendors must include oversite of the life cycle of background checks, compliance with policy and removal of access upon terminations or non-compliance.

CIP-005 Cyber Security - Electronic Security Perimeter(s)

Standard CIP-005 requires the identification and protection of the ESP(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.

Challenge:

Wireless networking devices introduce the ability to connect control center networking devices within a utility's ESP to other networks inside OR outside the ESP using any computer on the wired control center network. The number of access points is only limited by the number of routable and serial ports that exist on the computing devices within the ESP.[6]

CIP-006 Cyber Security - Physical Security of Critical Cyber Assets

Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

Challenge:

In the context of NERC CIP, the physical security program encompasses the entire Electronic Security System (ESS) and Physical Security Systems (PSS). This includes Access Control Systems (ACS) as in door access, Intrusion Detection Systems (IDS), Closed Circuit Television Systems (CCTV), Data Transmission Media (DTM) and Physical Security Systems (PSS). The devices used in creating these systems may each have their own inherent vulnerabilities by virtue of being controlled by an operating system, and by being communication devices. Additionally, the ESS and PSS should integrate with Cyber Access Controls and personnel records management for full automation of the access system.

[6] Wireless System Considerations When Implementing NERC CIP Standards by Teja Kuruganti, Walter Dykas, Wayne Manges, Paul Ewing, Thomas King (Oak Ridge National Laboratory, Oak Ridge TN 37831), Tom Flowers (Flowers Control Center Solutions, Todd Mission, TX 77363), and Mark Hadley (Pacific Northwest National Laboratory, Richland, WA 99352)

CIP-007 Cyber Security - Systems Security Management

Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).

Challenge:

IT security and governance documents may seem a daunting task of composing legalese.

CIP-008 Cyber Security - Incident Reporting and Response Planning

Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

Challenge:

Multiple system reports may be required to generate and Incident Report. Logs from the ESS and PSS systems, data regarding the network intrusion, access point, data usage may all be required. Additionally, if the incident occurred from an unauthorized personnel event, records pertaining to that employee, contractor or vendor regarding training, background investigations and risk awareness must all be a part of the Incident Report. Follow up procedures must be a part of the response to an event, to include defining practices for access modifications.

CIP 009 Cyber Security - Recovery Plans for Critical Cyber Assets

Standard CIP-009-3 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

Challenge:

Identifying recovery plans for unknown damages can create an endless loop of “what if” scenarios.

COMPLIANCE 101

Integrated Security Solutions, Inc. (ISS) has been protecting some of the world’s most critical assets since forming as an LLC in 2001. ISS provides design, integration, installation, maintenance and value engineering of Electronic Security Systems (ESS) and Physical Security Systems (PSS) around the world. ISS also offers surveys, threat assessments and solutions to mitigate threats and attacks to SCADA and network systems. ISS is currently under contract for a firewall installation in one USACE District infrastructure, and has recently completed the installation and integration of a system for an FAA facility to provide similar network security in addition to the ESS installed. ISS has investigated partners in software and service offerings to include NERC CIP compliance solutions for government customers in the energy sectors.

ISS is considered by the USACE to be an expert in protecting hydro-electric dams and power substations after providing services to more than 80 dams in the United States alone. ISS has continued to be involved in the development of standards, research and development of advanced systems, and value

engineering of technologies to provide the most effective and efficient solutions to protect these critical assets.

NERC CIP compliance begins with applying the CIP standards to a definable set of actions:

1. Identify Assets
2. Identify Vulnerabilities
3. Mitigate

Step 1 – Identify Assets

To effectively block the vulnerable components from cyber attack, for true CIP compliance, we refer to **CIP- 002, Identification of Critical Cyber Assets.** Critical Cyber Assets can be broken down into resources that support the reliable operation and delivery of the bulk power system, and to the critical and essential infrastructure that protects those resources.

Resources may include:[7]

- Transmission Substations that support the reliable operation of the bulk power system
- Generation Resources that support the reliable operation of the bulk power system
- Systems/Facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration
- Systems/Facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more
- Special protection systems that support the reliable operation of the bulk power system
- Any additional assets that support the reliable operation of the bulk power system

Critical and Essential Infrastructure

The foundational networks to be protected are the SCADA LAN, Demilitarized Zone (DMZ) LAN and Corporate LAN servers. There are additional assets within the system that may not be identified. These may be control devices or connected computers not recognized as part of the corporate or critical networks. They may also include environmental controls within the site, or ESS components. All of these are part of the Critical Cyber Asset realm. In an April 2009 message, NERC CSO Michale Assante states "Companies have not identified enough of their assets as critical, thereby requiring additional protection…NERC will broaden the net of assets that would be included under the mandatory standards framework in the future."

[7] McAfee Critical Asset Protection: Meeting and Exceeding the NERC CIP Regulations, White Paper by McAfee Inc., ©2010

Information Assets

In its full context **CIP 3 Cyber Security - Security Management Controls** includes access control of critical assets, and the protection of information regarding the critical asset. The latter will be operation procedures, network topology, incident response plans, security information, data contained in emails, reports, programs and any other information that reveals the critical asset existence, location, operation or protection systems. This includes data pertaining to personnel, visitor and contractor security authorizations, risk assessment and risk management. This information becomes part of the critical asset inventory and should be contained within the ESP and PSS. The CIP requires that the Responsible Entities have provisions for security management controls in place, have cyber security policies readily available to all personnel with access, and provide annual reviews of these policies.

Step 2 - Identify Vulnerabilities

Part of identifying critical assets is to also identify asset weaknesses. This can include a wireless penetration test which may encompass the following:

- Discovery of both known and unauthorized Wi-Fi networks and access points
- Information gathering on network strength, security protocols and connected devices
- Attack and penetration of networks encrypted with WEP, WPA-PSK and WPA2-PSK
- Automated traffic sniffing for finding streams of sensitive data
- Capabilities for joining cracked networks and testing backend systems
- Multi-staged attacks that trace chains of vulnerabilities to sensitive backend data

Routine or continual penetration testing will exceed the requirements of NERC and will help energy providers gain the most realistic vision of the current vulnerability of their IT systems and security controls. The penetration test or Network/Cyber TSCM investigation is conducted within the confines of technologies permitted in the private sector. This investigation can reveal connected IP addresses, operating systems and data flow. Unauthorized IP addresses may come from any device enabled for communication, wired or wireless. Detecting vulnerable access points is critical to the protection of the system.

Additionally, every device containing an operating system should be maintained through software and firmware upgrades. Logging the operating systems for all devices in use will help identify inherent vulnerabilities, as well as provide a basis for alerts when a non-logged system attempts to penetrate the network.

Step 3 – Mitigate (Block, Detect, Workaround, Fix)

Part of the mitigation process to Cyber and Critical Asset security includes the training of all personnel, including contractors and service vendors that have access (**CIP-004**). Training includes security awareness and compliance measures. Additionally, all personnel, including contractors and service

vendors, are required to have an appropriate level of personnel risk assessment on file. This information is part of the information assets.

Network and Physical Security measures to be deployed for NERC CIP Compliance may be broken down into key steps:

Block

Information and Access Controls

Access control pertains to both who has access to assets, and what those individuals are permitted to do with those assets. In addition to the operators' networks and energy management networks, access control will include corporate IT networks, backup networks and quality assurance networks.

Access control is also a part of the site ESS and PSS, controlling the physical access to networks and operating systems. This includes the credentialing of personnel through FIPS 201 compliant access control devices and biometrics.

The standard for the cyber ACS explicitly calls for an access control model that denies access by default. The cyber ACS will only enable required ports and services. This system dictates that only those activities that are specifically defined are permitted – all other activities are denied. The ACS, firewalls and cyber intrusion technologies form, by requirement, an Intrusion Prevention System (IPS).

Electronic Security Perimeter

Referring to **CIP- 005 Cyber Security - Electronic Security Perimeter(s)** requires the identification of the security perimeters. There will be perimeters for each network individually and often for each component. Multiple firewalls will be deployed at the network levels to prevent both outsiders and trusted insiders from gaining unauthorized access to systems. For example, there will be a SCADA firewall as well as a corporate firewall. Cyber intrusion detection technologies can be deployed to defend against attacks from the Internet.

Physical Security Perimeter

The next step in assuring a sufficient perimeter protection refers to **CIP-006 Cyber Security - Physical Security of Critical Cyber Assets**. Having established an ESP, the ESP must be contained within a PSS. This may include all non-cyber related controls such as ACS, IDS, CCTV Systems and any PSS. However, many of these systems are also vulnerable to cyber attack and so they too must become part of the Critical Cyber Asset system. The entire communicative structure that is required to operate and protect the Critical Infrastructure facility may become part of the monitoring and analytic system for immediate reporting of intrusion or threat.

Detect

This action includes CIP-003 and CIP-007.

CIP 007 Systems Security Management includes**,** in requirement 6 **(R.6)**: **Monitor and log all system events related to cyber security.** The system security tool must interface with network programs, including security programs, to produce the most comprehensive forensic analysis of activities which may impact the reliable operation of the critical infrastructure site.

One of the challenges faced by the cyber structure of today's security and operations devices is the unauthorized access to a network system through a wireless access point. Implementing realtime monitoring systems can analyze unauthorized IP addresses and non-standard data usage. The cyber security system may detect the following:

- Unauthorized activity
- Unauthorized operating systems
- IP connections
- Movement of data outside usual or established protocols

This tool is invaluable, as it provides 24/7 coverage of network activity, and will initiate alarms for unauthorized or irregular activity. The monitoring systems are stand alone systems that integrate with the existing security management systems, both physical, electronic and cyber. ISS can work with the appropriate software solution for the installed systems at a given site. For example, the system which monitors an airport infrastructure may not be most appropriate solution for a hydro electric dam environment.

Workaround

CIP- 008 Incident Reporting and Response Planning requires both the reporting of incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), and a plan for responding to access attempts or intrusions.

Response plans may include dynamic changes to the system to block the intrusion, manual or electronic diversion of the intrusion, or an emergency shutdown of a device that has been compromised. Each system requires a solution that is customized for the devices in operation and the systems that control and protect it.

Management of the life-cycle of authorization for access control, whether for electronic security, network permission or metal key distribution, is a key part of CIP 004-3 Personnel Identity, and the mitigation of potential security vulnerabilities.

Fix

CIP 009 Recovery Plans for Critical Assets, requires using best practices in business continuity and disaster recovery techniques. ISS has established relationships with both IT solution providers and SCADA engineers to design critical asset recovery plans for systems in the event of a successful attack. The development of the recovery plan in itself may help identify additional areas needing coverage under the ESP, and avenues to exceed the requirements of NERC CIP standards.

WHAT IS A SOLUTION?

In identifying critical assets and vulnerabilities, and identifying mitigation factors such as firewalls, Network TSCM programs, PSS and ESS, we have identified essentially a list of disparate systems. This list may be composed of the following:

- Personnel Time Logs
- Personnel Security Authorization Database
- Human Resources
- SCADA Control Systems
- Contractor Database
- Risk Management Programs
- Programs that report the results of Criminal Background Checks
- Time Keeping and Payroll Systems
- Corporate Networks and Databases
- DMZ Networks
- Electronic Security System
- Video Management Software
- Access Control Systems

The management of all of these systems and the many others not included in this list raises the corporate responsibility to a cost-defying level. NERC CIP standards require individual sytems to have inherent protection. But a SOLUTION to NERC CIP standards is a program that will encompass all of these systems, and integrate their security dialogue into a cohesive and seamless symphony. The solution will offer an interface through which to define controls, maintain the dialogue of compliance between systems, generate reports for official and internal reporting requirements, and manage the life cycle of access controls. ISS offers NERC CIP solutions that will offer the best value in time management, security management and administrative management of your Defense-In-Depth technologies.

A NERC CIP SOLUTION ILLUSTRATED

Employee X is terminated on Thursday at 5pm. He is escorted from the facility and his Smart Card and metal keys confiscated. The IT Manager will not be informed until 8am on Friday. Neither will the Security Manager, nor Human Resources. Employee X had remote access to the Corporate IT Server and

the Operations Network. He had access to secure areas of the Power Plant and Security Management System. The Security Administrator on duty will enter in a denial of access command to the CIP Solution System. The System will send commands to the Security Management System (for example CCURE), Video Management Software, Network Administration Database, Human Resources, Operations System, etc. Employee X's access to the critical infrastructure is now terminated for all systems in an automated fashion, and records updated for appropriate reporting requirements. This illustration details the Defense-In-Depth layers that make up the full solution, and the benefits of an all encompassing solution that can exceed NERC CIP Standards.

CONCLUSION

The NERC CIP requirements encompass such a vast array of systems and devices that it can seem a daunting task to comply. Compliance is an expensive burden. Organizations that are subject to NERC CIP standards must be "auditably compliant" by 2010 or face penalties of up to $1,000,000 USD per day. ISS views the NERC CIP program to be a part of Defense-In-Depth technologies likened to Disaster Preparedness plans. Disaster Preparedness plans require the inclusion of safety plans, evacuation plans, the plans to mitigate or prevent disaster impacts to human life and critical assets, and the plans for recovery in the event of a disaster.

ISS is capable of being a full solutions provider. In researching this developing field of expertise, ISS finds that some companies may be an expert in the understanding of network security while lacking an understanding of SCADA. Other companies may be an expert in understanding SCADA and Network Security, but lack understanding of ESS and PSS. Still other companies may understand the security of both the cyber asset and the physical assets, but lack understanding of the power generating plants and substations that make up the Smart Grid that NERC CIP seeks to protect.

Through many relationships developed over 30 years of key personnel experience, ISS is adept at bringing together the most knowledgeable and dynamic teams available to develop the most efficient and fully functional solution to meet or exceed NERC CIP requirements. The teams work together to ensure systems will interface with each other. The integrative efforts of both the IT, energy and security industry teams is critical, as much of the solutions today are still in their research and development state in regards to interfacing with operations and security programs.