



Owl Perimeter Defense Solution (OPDS) Regulatory Compliance Security Feature Map to NERC CIP V3 and NEI-08-09 Appendices D, E

Introduction

The emergence of cyber threats to the US electrical power generation infrastructure has led to rapid adoption of secure inter-network communication systems, originally developed to meet requirements of the Department of Defense to share information across isolated network domains. This document describes how such communication systems may be used to secure network communications in the nuclear power industry while simultaneously mitigating cyber attack threats.

One-way data transfer products created by Owl Computing Technologies, called Owl Perimeter Defense Solutions (OPDS), are used in the nuclear power industry to provide remote monitoring of control system data while denying access to control networks from external locations.

Recent data on cybersecurity penetration testing posted by IBM Internet Security Systems indicate that roughly 25 percent of vulnerabilities are in the Access category. Half of vulnerabilities are related to OS hardening (or lack thereof). OPDS products from Owl Computing Technologies prevent external access to Critical Digital Assets (CDA), and present hardened operating systems for self-protection.

Federal Standards Overview

The following Guidance for Securing Federal Information Systems is composed largely of text excerpts from NIST and CNSS websites. The Federal Information Security Management Act of 2002 (FISMA) recognizes the importance of information security to the economic and national security interests of the United States. FISMA also delegates specific duties and responsibilities to the Computer Security division of the National Institute for Science and Technology (NIST) to provide guidance in securing Federal information systems.

NIST published an Information Technology Laboratory (ITL) Computer Security Bulletin in November 2004, providing an introduction to emerging standards and guidelines for Federal information system security.

FIPS

Federal Information Processing Standards (FIPS) publications from NIST provide a specification for minimum security requirements for Federal information and information systems using a standardized, risk-based approach. FIPS publications of particular interest include the following:

- FIPS 199 -- Standards for Security Categorization of Federal Information and Information Systems (issued February 2004)
- FIPS 200 -- Minimum Security Requirements for Federal Information and Information Systems (issued March 2006).

NIST

NIST Special Publications in the 800 series present documents of general interest to the computer security community. NIST SP 800 publication numbers of particular interest include the following:

- NIST SP 800-18 Revision 1 -- Guide for Developing Security Plans for Federal Information Systems (issued February 2006)
- NIST SP 800-30 -- Risk Management Guide for Information Technology Systems (issued July 2002)
- NIST SP 800-37 Revision 1 -- Guide for Applying the Risk Management Framework to Federal Information Systems (issued February 2010)
- NIST SP 800-53 Revision 2 -- Recommended Security Controls for Federal Information Systems (issued December 2007)
- NIST SP 800-53A -- Guide for Assessing the Security Controls in Federal Information Systems (issued July 2008)
- NIST SP 800-82 -- Guide to Industrial Control Systems (ICS) Security (draft, September 2008).

National institute of science and technology (NIST) Special publications websites:

<http://csrc.nist.gov/publications/PubsSPs.html>

<http://csrc.nist.gov/publications/PubsFIPS.html>

The National Institute of Standards (NIST) defines a Cyber Incident as:

"An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional."

NIST documents have become the standard for virtually all cybersecurity programs at the federal level.

NIAP

NIST and the National Security Agency (NSA) established a program under the National Information Assurance Partnership (NIAP) to evaluate IT products usable by the Federal government. The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) helps consumers select commercial off-the-shelf information technology (IT) products that meet their security requirements and issues product certifications to help manufacturers of those products gain acceptance in the global marketplace.

<http://www.niap-ccevs.org/>

CNSS

The Committee on National Security Systems (CNSS) provides further guidance for the security of national security systems. National security systems are information systems operated by the U.S. Government, its contractors or agents that contain classified information or:

1. involve intelligence activities
2. involve cryptographic activities related to national security
3. involve command and control of military forces
4. involve equipment that is an integral part of a weapon or weapons system(s)
5. are critical to the direct fulfillment of military or intelligence missions (not including routine administrative and business applications).

CNSS Instruction (document) numbers of particular interest include the following:

- CNSSI-4009 -- National Information Assurance (IA) Glossary (revised June 2006)
- CNSSI-1253 Version 1 -- Security Categorization and Control Selection for National Security Systems (issued October 2009).

Committee on National Security Systems (CNSS) Publications web site:

<http://www.cnss.gov/full-index.html>

The US Committee on National Security Systems (CNSS) Instruction No. 4009 (CNSSI-4009), "National Information Assurance Glossary" defines the term "critical infrastructure" as follows:

"System and assets, whether physical or virtual, so vital to the U.S. 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." (Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c[e])

NERC

The North American Electric Reliability Corporation (NERC), an industry sponsored, industry-led, and industry-funded organization, created standards for Critical Infrastructure Protection (CIP). At time of writing, the newest (version 3) are called CIP-002-3 through CIP-009-3. These standards are used to secure bulk electric systems; providing network security administration while still supporting best practice industry processes.

The following NERC website provides access to NERC CIP regulations: <http://www.nerc.com/page.php?cid=2|20>

NERC CIP-002-3 provides definitions of Cyber Assets and Critical Cyber Assets, including the following:

- Control centers & backup control centers performing the functions of the entities listed in the Applicability section of this standard
- Transmission substations that support the reliable operation of the Bulk Electric System
- Generation resources that support the reliable operation of the Bulk Electric System
- Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration
- Systems and 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 Electric System
- Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

Note that the following are exempt from compliance with NERC CIP regulations:

- Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission. More notes on this provided below.
- Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

FERC

The Federal Energy Regulatory Commission, or FERC, is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. FERC also reviews proposals to build liquefied natural gas (LNG) terminals and interstate natural gas pipelines as well as licensing hydropower projects. The Energy Policy Act of 2005 gave FERC additional responsibilities as outlined in FERC's Top Initiatives and updated Strategic Plan.

By 2008, cybersecurity standards developed by the North American Electric Reliability Corporation were approved by FERC for implementation at the power plants. Systems providing System Security Emergency Preparedness (SSEP) functions will be excluded from the FERC/NERC standards, while systems not providing SSEP functions (specifically those that could affect reliable electricity generation) still need to comply with the FERC/NERC requirements.

FERC responsibilities include:

- Regulation of activities of the municipal power systems, federal power marketing agencies like the Tennessee Valley Authority, and most rural electric cooperatives;
- Regulation of nuclear power plants by the Nuclear Regulatory Commission (NRC).

NRC

In March 2009, a new federal security rule (10 CFR 73.54) went into effect requiring commercial nuclear power plants licensed to operate in the United States to submit cybersecurity plans to the Nuclear Regulatory Commission (NRC) for review and approval. In January 2010, the Nuclear Regulatory Commission issued NRC 5.71 Cybersecurity Program for Nuclear Facilities. This requirement led to adoption of NIST guidance publications SP-800-53, and SP- 800-82. Note that nuclear power generation facilities are subject to regulations from multiple organizations. NRC regulations arise from concerns about safety of radioactive materials and their handling. NERC regulations arise from concerns about the reliability of electrical power availability. Both sets of regulations converge under FERC, as described above.

NRC regulations apply to any part of the plant associated with fissile material and its handling, while NERC regulations apply to the "rest of plant". NRC and NERC are currently co-developing a Memorandum of Understanding "between the two organizations to establish formal protocols associated with information sharing, license 'exception request' reviews, on-site compliance inspections, and incident/event response."

NEI

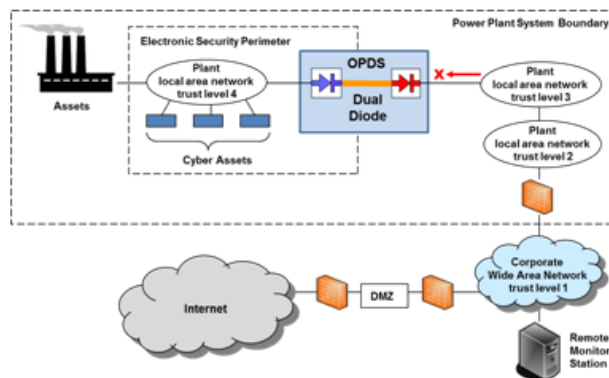
In response to NRC-5.71, the Nuclear Energy Institute (NEI, a nuclear power industry organization) with input and guidance from the United States Nuclear Regulatory Commission, created the NEI 08-09 "Cybersecurity Plan for Nuclear Power Reactors" document. The purpose of the NEI 08-09 Cybersecurity Plan is to provide a description of how the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks" (Rule) are implemented. The intent of the Plan is to protect the health and safety of the public from radiological sabotage as a result of a cyber attack as described in 10 CFR 73.1. 10 CFR 50.34(c), "Physical Security Plan," requires the inclusion of a physical security plan.

NEI 08-09 describes a defensive strategy that consists of a defensive architecture and set of security controls that are based on the NIST SP 800-82, Final Public Draft, dated September 29, 2008, "Guide to Industrial Control System Security," and NIST SP 800-53, Revision 2, "Recommended Security Controls for Federal Information Systems." The security controls contained in NEI 08-09 Appendices D and E are tailored for use in nuclear facilities and are based on NIST SP 800-82 and NIST SP 800-53.

OPDS Description

The Owl Perimeter Defense Solution is a one-way data transfer product based on DualDiode® Technology from Owl Computing Technologies, Inc. OPDS is designed for deployment at the perimeter of isolated plant processing control networks to transfer control system state information from inside the isolated network to monitoring stations outside the network, while denying any form of access from the outside.

A typical deployment is shown in the diagram below.



Note that critical cyber assets are located on the isolated network, that data only flows from the isolated network outward, and all forms of access to the isolated network from external locations are denied. When all external network access to critical cyber assets is denied, the same critical cyber assets are protected from threat of cyber attack from external network locations.

OPDS functions like an appliance that is highly automated (i.e. a network service). Data flows in one direction only, on demand; initiated by automated equipment within the protected network. Human interaction is not required to trigger data flow, but limited human interaction is required to execute a small number of tasks associated with normal operation and routine maintenance; such as power-on, shutdown, and offloading of audit logs.

About Owl Computing Technologies, Inc.

Owl Computing Technologies, Inc. is a privately owned and funded US company. Owl delivers NIAP Common Criteria EAL-4 certified one-way cross domain systems & electronic perimeter defense solutions to transport and protect an organization's most sensitive data between discrete domains of varying security levels and policies. Information sharing Secured by Owl® is enforced with Owl Computing proprietary DualDiode® technology. DualDiode one-way transfer systems guards against data leakage and protects networks from unauthorized access. Owl systems meet the highest levels of information protection within the US Department of Defense, the Intelligence community, & the Power Generation industry, delivering secure, reliable, information transfer of multiple data sources and types across single DualDiode systems -- any file size or data type. www.owlcti.com