

OWL ADVANTAGE

THE GOLD STANDARD IN DATA DIODE TECHNOLOGY

Grid Cybersecurity

Owl's Role in Achieving the 7 Steps

The seven steps recommended by the DHS include specific recommendations on the use of data diodes. As the global leader in data diode technology, with power grid implementations around the world, Owl has a wealth of experience in implementing cybersecurity in grid systems. This document is intended to show how each of the DHS's seven steps can be accomplished through the use of Owl intelligent data diodes to help operators dramatically reduce cyber risk.

1. APPLICATION WHITELISTING

Only allow predesignated applications to run and access data. Owl solutions only accept data from whitelisted data sources, restricted to a unique IP address, port, and protocol. This prevents malware from communicating over the data diode.

2. CONFIGURATION / PATCH MANAGEMENT

Ensure systems are up to date and that a secure method for introducing authenticated software patches is used. Owl solutions authenticate software patches and updates, then securely transfer them into control centers without using potentially contaminated laptops or portable media.

3. REDUCE ATTACK SURFACE AREA

Isolate control system networks from untrusted networks, lockdown unused services and ports, and use a data diode to provide network segmentation. Owl solutions provide hardware-enforced network segmentation and support the DHS recommendations for isolating control networks, reducing the attack surface to zero.

4. BUILD A DEFENDABLE ENVIRONMENT

Segment networks and restrict host-to-host paths to prevent the spread of infection. Owl data diodes are purpose built as the most effective network segmentation devices available.

5. MANAGE AUTHENTICATION

Implement "least privilege", increase password length, change passwords regularly, and require separate credentials for corporate and control network zones. Owl solutions provide an intrinsic separation of corporate and control network zones, as well as authentication on all transfers, and allow for long passwords requiring regular changes.

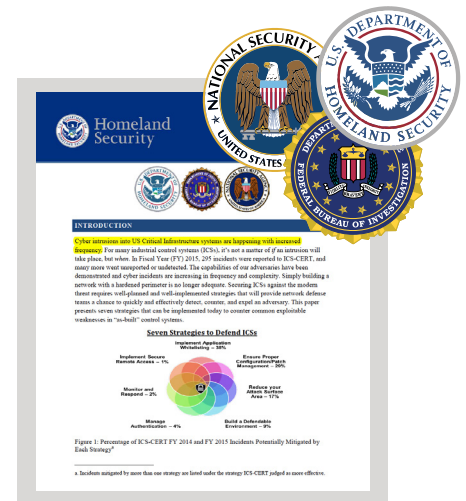
6. IMPLEMENT SECURE REMOTE ACCESS

Implement monitoring-only data access enforced by data diodes, remove backdoors, and any persistent remote connections. Owl data diodes are specifically designed to facilitate secure remote monitoring without enabling remote access or any remote connections.²

7. MONITOR & RESPOND

Monitor traffic at and within control system boundaries, perform login analysis, and watch for access control manipulation. Owl solutions provide real-time monitoring, display & analysis of all connections, and allow offsite auditing of all network activity.

Guidance from the DHS, NSA, and NERC to improve cybersecurity in power substations, microgrids, and transmission infrastructure.



CYBERSECURITY GUIDANCE FOR THE GRID

The power grid and its associated bulk electric systems represent millions of disparate systems connected in networks that range from a single building to thousands of square miles. From substations and transmission equipment, to new microgrids and small scale power generation, these systems all face the growing threat of cyberattack from increasingly sophisticated adversaries.

Beyond the regulations put in place by NERC CIP, the US Department of Homeland Security (DHS), in collaboration with the FBI and the NSA, put together a list of seven concrete steps¹ that grid operators can take to create a layered, defense in depth architecture and mitigate cyber incidents.

NERC CIP COMPLIANCE

Data diodes are used by many critical infrastructure and power grid operators today to achieve compliance with NERC CIP and other regulatory mandates, as well as meeting industry best practices, such as those set forth by the DHS.

Approved by NERC for the use of network segmentation and one-way data transfer, data diodes combine absolute information assurance and unhackable cybersecurity with the ability to share and monitor operational data. As one-way data transfer systems, data diodes isolate and protect networks from external cyber threats, while allowing systems within these networks to transfer data to other networks in a highly controlled, deterministic manner.

With a non-routable, hardware-based platform, data diodes create an absolute electronic security perimeter by physically only permitting data to transfer in one direction, from one network segment to another, across a network security boundary. When utilized effectively, data diodes can help operators achieve NERC CIP compliance, eliminate all external cyber threats, and provide a path to business continuity through remote monitoring and offsite data analytics.

Defense-in-Depth

A “defense in depth” approach prevents a cybersecurity architecture from relying on a single strategy or element to defend a network. Data diodes, a hardware-based network cybersecurity technology designed to protect critical networks while allowing secure, one-way-only data sharing, play an integral part in this layered cybersecurity approach. These multiple layers create a matrix of protection which greatly reduces risk by blocking possible threats across different vectors.

OPDS-100D

Entry level data diode for affordable, effective network confidentiality and assurance.

The OPDS-100D allows operators to deploy more targeted and precise cybersecurity controls at a dramatically lower TCO. The 100D is a highly reliable, single-box data diode solution in a DIN rail form factor which supports multiple data flows and data types, with a maximum throughput of 104 Mbps.

The 100D can be used to create network micro-segments, protecting individual devices (e.g. a PLC), historians, databases, substations, monitoring stations along transmission lines, or any other environment with either one or more data sources and low bandwidth requirements.

KEY FEATURES

- Strongest Network Cybersecurity Available
- Unmatched Functionality and Compatibility
- Competitive Price Point
- Designed for Extreme Environments

OWL DATA DIODE HARDWARE PLATFORMS

- DiOTa – Throughput of 3 Mbps
- OPDS-100D: DIN rail appliance – Throughput from 10 Mbps to 100 Mbps
- OPDS-100: 1U appliance – Throughput from 10 Mbps up to 100 Mbps
- OPDS-1000: 1U appliance – Throughput from 100 Mbps up to 1000 Mbps
- EPDS: Server-based solution – Throughput up to 10 Gbps



OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com