



Independent Assessment of Owl Computing Technologies DualDiode® Technology for FISMA and NIST Compliance

Conducted by:

MBL Technologies, Inc.
1 Research Court, Suite 450
Rockville, MD 20850
www.mbltechnologies.com
ph: 703-732-6419

April 5, 2010



About MBL Technologies, Inc.

MBL Technologies is a service disabled veteran owned small business (SDVOSB) that specializes in providing information security and privacy services to government and commercial entities. Specifically, MBL Technologies and its staff concentrate on information security and privacy program management, Federal Information Security Management Act (FISMA) compliance, system security, and the integration of organizational information technology (IT) and security requirements. Through years of delivering high quality client service and developing sound security and privacy solutions, the members of the MBL Technologies team have forged a reputation in the information assurance industry for excellence and reliability and have excelled at helping private entities comply with FISMA, National Institute of Standards and Technology (NIST) and other federal requirements. MBL Technologies and its staff have performed similar FISMA/NIST compliance activities at various government and commercial organizations including the Nuclear Regulatory Commission (NRC), the Department of Health and Human Services (DHHS) and the Department of Veterans Affairs (VA). MBL Technologies is vendor neutral and thus has no partnerships with Owl Computing Technologies or any other hardware software vendors. This neutrality allows us to provide truly unbiased expertise and service to our clients.

The primary MBL Technologies' contributors to this Owl Computing Technologies DualDiode[®] Technology Assessment, Mr. Eric Hummel and Mr. Ryan Tappis, drew upon applicable experience with the technology under consideration as well as the proposed analytical criteria, NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* and NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security* to complete this task. Mr. Eric Hummel, a Certified SCADA Security Architect (CSSA), Certified Information System Security Professional (CISSP) and Certified Information Security Manager (CISM) with over 15 years of industry experience, has evaluated data diode technology for compartmentalized classified systems in the past, and possesses an innate understanding of the potential associated benefits and risks. Mr. Ryan Tappis, a CISSP, has extensive experience in risk management, security control auditing, and security compliance earned through direct support of agencies such as the NRC and commercial entities. He brought to bear a unique combination of management expertise and technical implementation know-how.

Legal Disclaimer

FISMA compliance and security control satisfaction is ultimately at the discretion of the entity assessing a system's security. Through our extensive experience in the federal sector and with FISMA and NIST compliance in particular - MBL Technologies confirms to the best of its knowledge that the verbiage set out in this document is accurate. However, MBL Technologies cannot guarantee and shall not be held liable should an agency not concur with the findings of this assessment or in the event of a system security failure. Any and all statements concerning and encompassing Owl Computing Technologies DualDiode[®] Technology meeting required security are based exclusively and solely on the predication and presumption that the product is installed correctly and is operated as intended in conformance and in compliance with directions and instructions accompanying the said technology.

Table of Contents

Abstract..... 1

Owl DualDiode® Technology..... 2

NIST SP 800-53, Revision 3 and NIST SP 800-82 Compliance..... 3

Case Study..... 8

Conclusion..... 11

Abstract

This whitepaper documents the security characteristics of Owl Computing Technologies, Inc.'s (Owl) proprietary DualDiode® Technology. The whitepaper describes the use of Owl DualDiode® Technology in enhancing security for organizations that must comply with Federal Information Security Management Act (FISMA) requirements and National Institute of Standards and Technology (NIST) controls. Understanding that federal security requirements are constantly evolving and the rising costs associated with ensuring federal compliance are of utmost concern, this paper details how Owl DualDiode® Technology can save organizations money, enhance operational security, and improve conformity with Federal requirements.

Specifically, this document details the capabilities of Owl DualDiode® Technology, its technical characteristics, and its ability to assist organizations and systems in complying with NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* and NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*. We analyze NIST SP 800-53 and NIST SP 800-82 control by control, and explicitly detail which controls are satisfied simply by implementing Owl DualDiode® Technology. Finally, we explore the implementation of Owl DualDiode® Technology in a hypothetical, "real world" environment, and provide a practical example of how using Owl DualDiode® Technology enhances security and improves compliance.

The findings of this whitepaper illustrate that Owl DualDiode® Technology can enhance organizational compliance with federal regulations and result in an improved security posture. In particular, when implemented correctly, operated as intended and coupled with security policies, Owl DualDiode® Technology can satisfy roughly 20% of the required NIST security controls (SP 800-53 and SP 800-82). In the end, this can save organizations both time and money as a single Owl DualDiode® Technology product can satisfy a large number of the NIST security requirements.

Owl DualDiode® Technology

Owl DualDiode® Technology is a National Information Assurance Partnership (NIAP) Evaluation Assurance Level (EAL) 4-certified boundary protection device that can meet the stringent requirements of well established information security models, such as Biba, Bell-LaPadula and Boebert-Kain to allow data to flow in one direction only, regardless of input, failure or any other condition. Owl core DualDiode® Technology is comprised of two specially configured Asynchronous Transfer Mode (ATM) communication cards and an optical fiber as shown in Figure 1 (see below). The two communication cards fit into standard 32 or 64 bit PCI slots in their respective (typically separate) host machines, and communicate through the optical fiber.

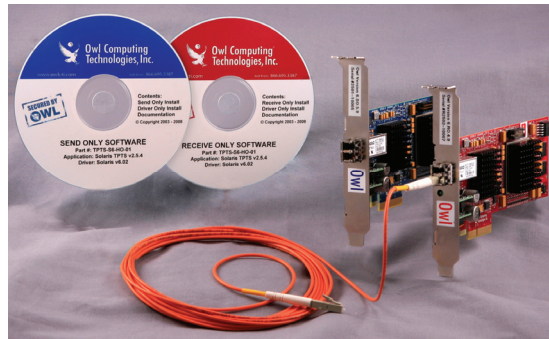


Figure 1 - DualDiode® ATM Communication Cards

All components are color-coded: Blue for Send, and Red for Receive. The Send card resides in a designated Send Server (Blue) on the source network, and is populated only with components for photo transmission. The Receive card resides in a designated Receive Server (Red) on the destination network, and is populated only with components for photo detection. The security of the one-way data transmission is embedded in the circuitry of the communication cards. This enforces the one-way transfer of data at both ends of the fiber optic cable, creating the DualDiode® data transfer system; a secure one-way link between networks as shown below in Figure 2.

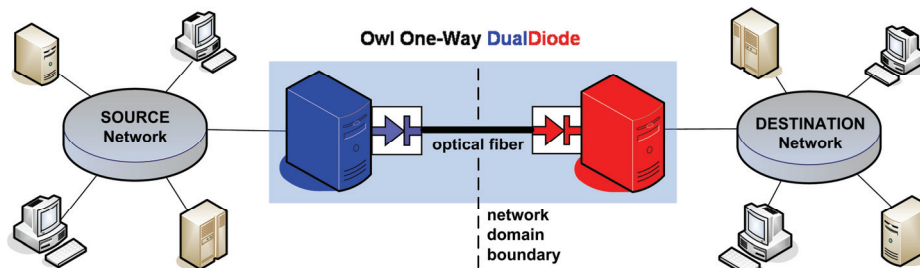


Figure 2 - One-Way Data Transfer

DualDiode® Technology creates a dedicated Send and Receive optical link that uses Owl proprietary protocol across the network boundary. When operated in conjunction with Owl software, it supports the transfer of a variety of data using three forms of transport: (1) files and populated directory structures; (2) UDP packets and (3) TCP streams. For each form of transport, interfacing software from Owl provides a seamless connectivity between edge servers and the networks to which they belong.

NIST SP 800-53, Revision 3 and NIST SP 800-82 Compliance

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* establishes the minimum security controls for systems which store, process or transmit federal information. The controls are organized into 18 families, based on their purpose. In total, there are over 190 controls for systems in the High baseline. As defined in Federal Information Processing Standard (FIPS) 199, the High baseline applies to information systems whose security posture must be protected at the highest level based on the potential severe ramifications of an information security breach. For typical Owl DualDiode® Technology implementation locations - industrial control systems, power plants, other critical infrastructure components, etc. - this High baseline will likely be applicable. Augmenting the High baseline are control enhancements, which mandate additional security granularity for specific controls.

In addition to NIST SP 800-53, NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security* offers specific security control recommendations for Industrial Control Systems. While not required, these recommendations are considered best practice and strongly encouraged in ICS architectures. By meeting these NIST standards, organizations enhance their compliance and adherence to FISMA, as FISMA explicitly mandates NIST Special Publications as the de facto standard for security.

As part of this document, Owl DualDiode® Technology was considered against each control outlined in NIST SP 800-53, Revision 3 and NIST SP 800-82. The controls which are satisfied through the use of OwlDualDiode® Technology, and the method in which Owl DualDiode® Technology satisfies each, are detailed in Table 1 and Table 2 below.

Table 1 - NIST SP 800-53 Controls

NIST SP 800-53, Revision 3 Control	How Owl DualDiode® Technology Can Result in Compliance
AC-4: Information Flow Enforcement	This control requires that information flows are enforced in accordance with prescribed policies. Enhancements (7) and (16) specifically address the value of “One-way flow enforcement”. Utilizing Owl DualDiode® Technology at the system boundary guarantees that data flow is restricted to one direction.
AC-6: Least Privilege	This control requires that users only have access to what they need to in the legitimate exercise of their responsibilities. Enhancement (6) requires the protection of the system from privileged access from outside of the organization. Implementing Owl DualDiode® Technology on the system boundary ensures that privileged access cannot occur from the outside.

Independent Assessment of FISMA and NIST Compliance for
Owl Computing Technologies DualDiode® Technology

NIST SP 800-53, Revision 3 Control	How Owl DualDiode® Technology Can Result in Compliance
AC-17: Remote Access	This control mandates remote access be restricted and secured. Owl DualDiode® Technology enforces this control via the one-way data flow. Remote access into a network can be completely shut down through the implementation of Owl DualDiode® Technology on the network perimeter.
SA-7: User Installed Software	This control protects the network from user downloaded software which can contain malicious code. Owl DualDiode® Technology enforces a one-way “Source to Destination” traffic flow and will block downloads going in the opposite direction.
SC-4: Information in Shared Resources	This control mandates the prevention of data flow from systems with different security levels. Owl DualDiode® Technology can be implemented to ensure that high security level data can move to a low security level system, but not vice versa, thus satisfying this control.
SC-5: Denial of Service Protection	This control requires that systems maintain availability and protection against denial of service attacks. In specific installation instances, Owl DualDiode® Technology can be physically located on the network to mitigate Denial of Service Attacks. By using Owl DualDiode® Technology to enforce a policy of only outbound data transmission, potential hackers outside the network could not flood the protected system with messages.
SC-7: Boundary Protection	This control requires that the perimeter of networks is protected from attacks. Enhancements (1), (2), (4), (5), (10), (16) and (18) specifically dictate requirements for protecting data flow on the network boundary. Owl DualDiode® Technology implemented on the network perimeter can satisfy this control requirement.
SC-15: Collaborative Computing Devices	This control mandates the blocking of collaborative computing devices (network whiteboards, video conference, etc) unless specifically required. These applications require bi-directional communication and cannot function through Owl DualDiode® Technology.

Independent Assessment of FISMA and NIST Compliance for
Owl Computing Technologies DualDiode® Technology

NIST SP 800-53, Revision 3 Control	How Owl DualDiode® Technology Can Result in Compliance
SC-18: Mobile Code Protection	This control, specifically Enhancement (3) requires a policy to restrict the mobile code that can be loaded and executed on the system. Owl DualDiode® Technology will not allow mobile code to be downloaded and prohibits the user from introducing mobile code into the protected network because the one-way data connection runs in the opposite direction. This meets the control requirement in Enhancement (3) which mandates that the system prevent the download and execution of prohibited mobile code.
SC-24: Failure to a Known State	The control requires the system to fail in a consistent and secure state. By design, upon failure, Owl DualDiode® Technology still cannot pass data in the reverse direction.
SC-28: Protection of Data-at-Rest	The control requires the protection of the confidentiality and integrity of data at rest in the system. Owl DualDiode® Technology will not allow access from the external network to change or view the data in the systems it protects (by simply not passing traffic inbound).
SC-32: Information System Partitioning	This control specifies that systems and data be segregated, based on the classification of data being stored. Owl DualDiode® Technology can strictly and reliably enforce data flow from different sensitivity zones.
SI-3: Malicious Code Protection	The control requires both protection and detection mechanisms for anti-virus protection. Owl DualDiode® Technology provides the protection mechanism. By disallowing data flows into a protected network, new viruses or malicious code cannot be introduced via network traffic.
SI-9: Information Input Restrictions	This control mandates that information input is restricted to authorized personnel only. Through the implementation of Owl DualDiode® Technology, an organization can block information from being input from a lower trust level to a higher trust level.

Table 2 - NIST SP 800-82 Controls

NIST SP 800-82 Recommendation	How Owl DualDiode® Technology Can Enhance Security
<p>5.1 Firewalls</p> <p>“In an ICS environment, firewalls are most often deployed between the ICS network and the corporate network. Properly configured, they can greatly restrict undesired access to and from control system host computers and controllers, thereby improving security. They can also potentially improve a control network’s responsiveness by removing non-essential traffic from the network. When properly designed, configured, and maintained, dedicated hardware firewalls can contribute significantly to increasing the security of today’s ICS environments.”</p>	<p>Use of Owl DualDiode® Technology in conjunction with a firewall enforces absolute restrictions for inbound network traffic, while allowing flow of files, streams and syslog data outbound. Due to the specific anti-tampering characteristics of Owl DualDiode® Technology, enforcement of this policy can be guaranteed beyond the assurance that a firewall can provide.</p>
<p>5.2 Logically Separated Control Network</p> <ul style="list-style-type: none"> • “There should be documented and minimal (single if possible) access points between the ICS network and the corporate network. • A stateful firewall between the ICS network and corporate network should be configured to deny all traffic except that which is explicitly authorized.” 	<p>Owl DualDiode® Technology enforces a strict separation between the ICS and other network segments that prohibits inbound data transfer. The effect is that only outbound traffic is authorized. Statefulness of incoming packets is irrelevant and outbound traffic can be explicitly configured to carry only authorized traffic.</p>
<p>5.3 Network Segregation</p> <p>“ICS networks and corporate networks can be segregated to enhance cyber security using different architectures.”</p>	<p>Owl DualDiode® Technology’s ability to restrict dataflow to one-way only can provide logical segregation between control networks and corporate networks.</p>
<p>5.4 Defense in Depth</p>	<p>The implementation of Owl DualDiode® Technology as part of</p>

NIST SP 800-82 Recommendation	How Owl DualDiode® Technology Can Enhance Security
<p>“A single security product, technology or solution cannot adequately protect an ICS by itself...an effective defense-in-depth strategy requires a thorough understanding of possible attack vectors on an ICS. These include:</p> <ul style="list-style-type: none"> • Backdoors and holes in network perimeter • Vulnerabilities in common protocols • Attacks on field devices • Database attacks • Communications hijacking and ‘man-in-the-middle’ attacks” 	<p>a defense- in-depth security posture can protect against each of the attack vectors listed.</p>
<p>5.6 Protocols that are potential security risks:</p> <ul style="list-style-type: none"> • DNS • HTTP • FTP/TFTP • Telnet • SMTP • SNMP • DCOM • SCADA Protocols (Modbus/TCP, EtherNet/IP, DNP3) 	<p>These are all protocols that will be completely blocked inbound by Owl DualDiode® Technology at the boundary of the Level 4 Trust Layer. All of these protocols except SNMP are also blocked outbound. The Level 4 Trust Layer is isolated from external attack via any communication protocol.</p>
<p>6.2.6.2 Intrusion Detection</p> <p>“Current IDS and IPS products are effective in detecting and preventing well-known Internet attacks, but until recently they have not addressed ICS protocol attacks. IDS and IPS vendors are beginning to develop and incorporate attack signatures for various ICS protocols such as Modbus, DNP, and ICCP.”</p>	<p>Both host- and network-based Intrusion Detection Systems complement an Owl DualDiode® Technology implementation. Owl DualDiode® Technology allows syslog data to flow from sensors to aggregators and consoles outside of the Level 4 Trust Layer while at the same time blocking traffic from traversing in the opposite direction.</p>

Case Study

As an example of how this would apply in a real world design, let us examine a representative enterprise computing environment in a power plant. Technically, Owl DualDiode® Technology can be implemented at several points on a network. This example assumes placement of Owl DualDiode® Technology to specifically protect Trust Level 4 data. This example does not illustrate all of the possible placements of Owl DualDiode® Technology nor does it exactly mirror all power plant computing environments, rather it provides a sample framework of how Owl DualDiode® Technology can be utilized.

As illustrated in Figure 3 below, the plant's computing infrastructure consists of the following:

- **Trust Level 1**, which provides access to other power plant sites and access to the public Internet. Systems in this Trust Level (as described below) are separated from Trust Level 2 systems by a firewall.
- **Trust Level 2**, which consists of executive, financial and operations components. Systems in this Trust Level connect to systems in Trust Level 1 to provide internet services, employee email and other common services.
- **Trust Level 3**, which receives data from Trust Level 4 processes and correlates process information from the plant including flows, pressures and temperatures.
- **Trust Level 4**, which contains safety related equipment, control systems and other critical plant infrastructure components.

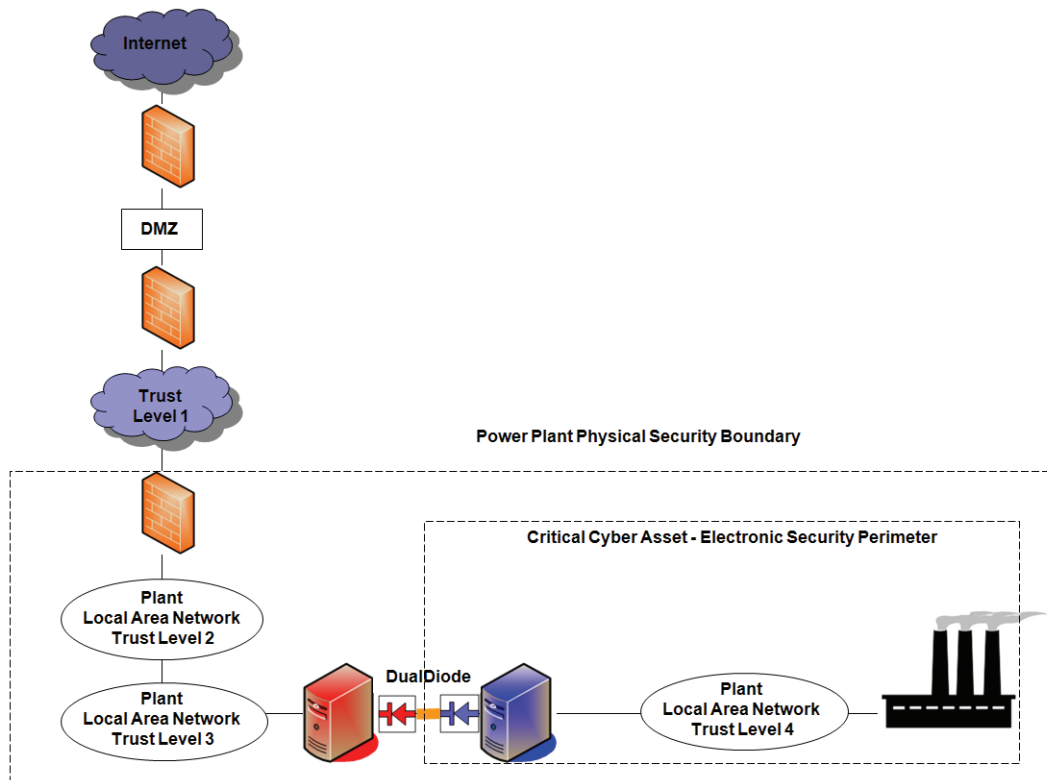


Figure 3 - Case Study Network Diagram

Within the plant's computing infrastructure, as the Trust Level increases, the sensitivity of the data and infrastructure increases, as does the need for protection of the integrity of data and software in order to enhance the reliability of plant operations. Sensitivity of data and trust levels increase from the outside in as illustrated in Figure 4 below.

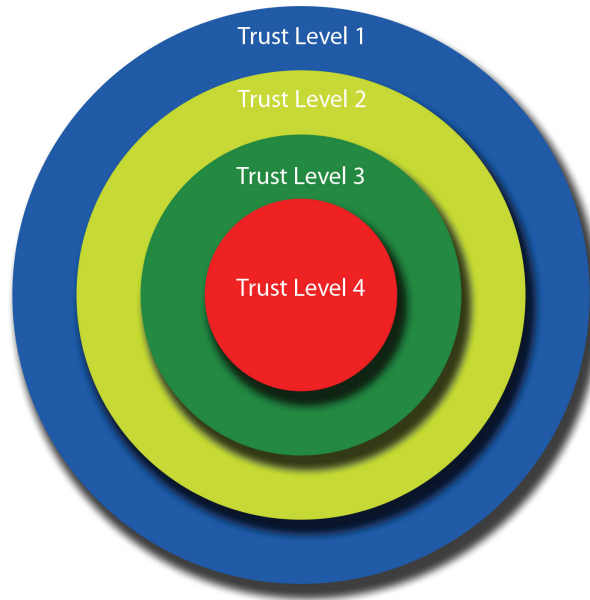


Figure 4 - Trust Levels

In our example, Owl DualDiode® Technology is positioned between Trust Level 4 and Trust Level 3. In this environment, Trust Level 4 will send information across to the LAN in Trust Level 3 about the state of controls, sensors, indicators, command history, logs and security data from devices. This data is transmitted using various protocols. Due to the utilization of Owl DualDiode® Technology, data can only flow in one direction: **FROM Trust Level 4 TO Trust Level 3** and not vice versa. This is illustrated in Figure 5 below.

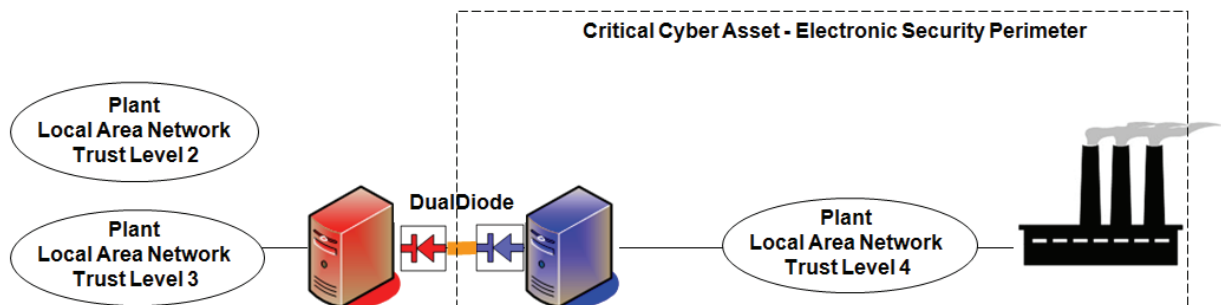


Figure 5 - One-Way Data Transfer

A would-be attacker cannot pass commands from the lower trust level via the Internet, Corporate WAN or Power Plant LAN to attack Trust Level 4. The implementation of Owl DualDiode® Technology in this

instance protects against outside threats (via the Internet) and insider threats (via the Plant Local Area Network in Trust Level 3). Meanwhile, Owl DualDiode® Technology still enables critical measurements, readings, and status messages to pass from Trust Level 4 to Trust Level 3. This one way traffic flow is imperative as Trust Level 3 houses servers that conduct detailed analysis of the plant operations from the raw data transmitted from systems within Trust Level 4.

A protective solution as described above would be accompanied by policies that complement the structural features of the one-way Owl DualDiode® Technology boundary control. These policies, as briefly summarized below, in combination with the successful implementation of Owl DualDiode® Technology, could satisfy almost 20% of the roughly 190 security controls defined in the High Baseline of NIST SP 800-53, Revision 3 in addition to a portion of the security recommendations defined in NIST SP 800-82. A sample of these security policies include:

1. Policies to ensure a well designed and implemented change control process that can detect and prevent malicious logic from being introduced manually into the control system. (To satisfy security controls CM-3 and CM-5)
2. Personnel and visitor policies that ensure that persons with physical access do not have the opportunity to perform malicious activity. (To satisfy security controls AC-2, AC-3, AC-6, PE-2, PE-3, PE-7 and PS-3)
3. A logging and incident response process that takes advantage of the streaming and syslog capabilities of Owl DualDiode® Technology. (To satisfy security controls AU-6, IR-4, IR-5 and IR-6)
4. An effective, periodic training and awareness requirement for all users that describes enterprise risks, roles and responsibilities, and mandated adherence to requirements. (To satisfy security controls AT-2 and AT-3)
5. A defined Certification and Accreditation (C&A) process for assessing system risks and obtaining senior executive acceptance of risks prior to system changes. (To satisfy security controls CA-2, CA-5 and CA-6)
6. Policies requiring continuous monitoring of system security controls throughout the system's operation. (To satisfy security controls CA-7 and RA-5)

The remaining security controls are mainly centered around operational and management security requirements that are satisfied through additional policies, procedures and supplementary security technology solutions.

Conclusion

As illustrated in this whitepaper, Owl DualDiode® Technology can help organizations protect their critical systems, adhere to requirements, and meet federally mandated NIST control requirements. When implemented correctly, Owl DualDiode® Technology can satisfy numerous NIST SP 800-53 and NIST SP 800-82 security controls. When inserted into a defense-in-depth architecture and implemented within an organization with robust security policies and processes, Owl DualDiode® Technology results in increased compliance, decreased costs, and an overall improved security posture.