Waterfall Security Solutions Ltd.

NERC CIP V5 Standards Position

Unidirectional Security Gateways as Secure Alternatives to Firewalls and Network Intrusion Detection Systems

Stronger Security Simplifies Compliance

Date: September 2014

- Legal Notice & Disclaimer -

Any and all third party intangible and/or proprietary and/or intellectual property rights ("**Third Parties' Rights**"), mentioned herein, whether registered or not, including, without limitation, patents, trademarks, service marks, trade names, copyrights and computer applications, belong to their respective owners. Waterfall Security Solutions Ltd. disclaims any and all interest in all such Third Parties' Rights. It is forbidden to copy, modify, amend, delete, augment, publish, transmit, create derivative works of, create or sell products derived from, display or post, or in any other way exploit or use such Third Parties' Rights without the express authorization of their respective owners.

Except as specified herein, Waterfall Security Solutions Ltd. does not guarantee nor make any representations with regard to any and all third party tangible and/or intangible and/or proprietary and/or intellectual property ("**`Third Party Property`**") mentioned herein. Waterfall Security Solutions Ltd. does not endorse nor makes warranties as to the completeness, accuracy or reliability of such Third Party Property, and all such warranties are hereby expressly and strictly disclaimed.

- Table of Contents –

Summary

The electric power sector leads both North American industry and the world in strong cyber-security standards. Both the NEI and NRC standards in nuclear generation and the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards in the Bulk Electric System[1] (BES) are seen as among the most demanding cyber-security regimes enforced anywhere in the world. The NERC CIP standards in particular are seen as a model of cyber security for other industries and critical infrastructures. The NERC CIP V5 standards are designed specifically to enhance the reliability of the Bulk Electric System through strong security.

The CIP V5 standards recognize that Unidirectional Security Gateways provide security which is stronger than firewalls, and position the gateways as an alternative to firewalls and costly Network Intrusion Detection Systems (NIDS). The V5 CIP standards have 103 requirements overall, and provide exemptions from 37 Medium-Impact requirements, and 5 High-Impact requirements, when Waterfall's Unidirectional Security Gateways are used to protect an Electronic Security Perimeter (ESP) rather than using firewalls and NIDS. Unidirectional Security Gateways increase the security of critical control systems, simplify and reduce the ongoing cost of CIP V5 compliance programs, and eliminate the need to use high-maintenance firewalls and NIDS.

Waterfall's Unidirectional Security Gateways are deployed widely in the BES, especially in power generation applications. The strong security provided by these gateways is recognized by steadily increasing numbers of industry analysts and security experts. For example, while addressing representatives of NERC entities at a recent cyber-security conference, Tim Roxey, the Chief Security Officer of NERC, observed that:

> *"When you are considering security for your control networks, you need to keep in mind innovative security technologies such as unidirectional gateways."*

Frost & Sullivan maintains that Waterfall's gateways provide

> *"… optimum security for networks across user verticals in a more reliable and effective way than do two-way conventional firewalls."*

Dale Peterson, CEO of Digital Bond maintains that

> *"You [Waterfall Security] stop all inbound attacks, firewalls don't. Full stop."*

In short, the Bulk Electric System is becoming measurably safer, more secure and more reliable as a result of the widespread deployment of Unidirectional Security Gateways. The NERC CIP V5 standards recognize this trend. NERC entities who deploy the gateways

[1] This document uses the NERC convention of capitalizing terms defined formally in the NERC glossary.

enjoy dramatically improved security, improved reliability, and find their CIP compliance costs reduced as well.

Unidirectional Security Gateways

Waterfall's Unidirectional Security Gateways use hardware-enforced unidirectional communications. Waterfall's unique Unidirectional Gateways use two network hardware modules: the transmit (TX) module contains a fiber-optic transmitter, but no receiver, and the receive (RX) module contains a fiber-optic receiver, but no transmitter. The two modules are connected by a single fiber-optic cable. This fiber-optic cable is the only connection between the TX and RX modules, and as a result, the TX module can send information to the RX module, but never vice-versa. There is no physical way to enable the RX to emit light into the fiber-optic cable, nor is there any way to enable the TX to receive light or to convert any light back to an electrical signal.

Waterfall's Unidirectional Gateways are a combination of hardware and software. The unidirectional hardware provides security, making it impossible for any system on an external network to launch a network attack the protected systems in a critical network. The Waterfall software replicates industrial servers over the unidirectional medium, making the gateway solution a plug-and-play replacement for firewalls.

IT/OT integration Use Case – Power Plant

Take for example a generating plant using a process historian on the plant network. The historian gathers data from generating unit control systems, archives that data, and make the data available to corporate users. The gateway software consists of a transmit (TX) agent component and a receive (RX) agent component. Each agent runs on a conventional Windows or Linux computer, which can be either a customer-supplied computer, or a Waterfall Linux or Windows Host Module, as shown in Figure (1).

Figure (1): Waterfall's Modular Unidirectional Gateway Hardware Architecture

The TX agent connects to the plant historian and queries the historian for data. The TX agent sends that data to the RX agent via the TX and RX hardware modules, as illustrated in Figure (2).

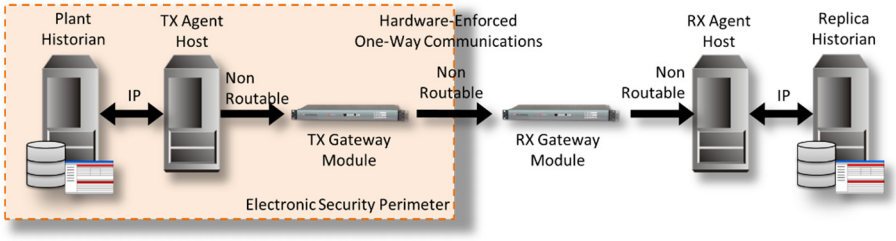

Figure (2): Historian Server Replication

The RX agent, after receiving the data, connects to a historian on the external business network. The RX agent instructs the historian on the business network to store the historical data received from the operations historian, creating a fully updated replica on the business network.

The replica historian is maintained by the gateway solution as a real-time, faithful replica of the plant historian. The replica has all of the historical data, back to "the beginning of time," and it has all of the latest data, updated in real-time by the Waterfall Unidirectional Gateway system. Users on the business network now access and query the replica historian, instead of the operational historian inside the industrial network.

Waterfall's Unidirectional Security Gateways provide absolute protection from attacks originating on external networks. The gateways eliminate the online attack threat vector entirely, so security practitioners no longer need to spend time or mind-share dealing with the risk of network-based attacks from the business network.

NERC CIP V5 and Unidirectional Security Gateways

The NERC CIP Version 5 standards include many advancements from the current CIP V3 standards, including significant changes to the way network perimeter protection is handled. The CIP V5 standards position Unidirectional Security Gateways as an alternative to firewalls and NIDS, and the V5 standards include measures to encourage the deployment of this stronger, unidirectional alternative.

The V5 standards contain 103 requirements, and provide exemptions from 37 Medium-Impact requirements and from 5 High-Impact requirements when Unidirectional Security Gateways, rather than firewalls and NIDS, are used to protect an ESP. With fewer rules to follow, deploying Waterfall Unidirectional Gateways reduces the ongoing cost of V5 CIP compliance programs.

The V5 standards include Unidirectional Security Gateway exemptions due to:

- The definition of External Routable Connectivity,
- The definition of Interactive Remote Access, and
- The definition of Electronic Access Point.

In all these cases, the resulting CIP program simplifications are justified by the stronger-than-firewalls security provided by Unidirectional Security Gateways.

CIP V5 Impact Levels

The majority of the CIP V5 unidirectional exemptions apply to Medium Impact BES Cyber Systems. The CIP V5 standards define a BES Cyber System as a set of BES Cyber Assets. A BES Cyber Asset is a Cyber Asset which, if impaired or mis-used would, within 15 minutes of the asset's required correct operation, affect the reliable operation of the Bulk Electric System. A Cyber Asset is a programmable electronic device, including the hardware, software, and data in the device. Every BES Cyber System must be protected by an Electronic Security Perimeter.

The definitions for High, Medium and Low Impact BES Cyber Systems are detailed and complex. In summary though, NERC entities should expect that:

- **High:** Most computers and networking equipment supporting control rooms in Reliability Coordinators, Balancing authorities and Transmission Operators are High Impact,
- **Medium:** Most e computers and networking equipment supporting control rooms in large generating sites, and in high-voltage substations are Medium Impact, and
- **Low:** Most of the remaining computers and network equipment supporting lower-voltage substations and smaller generators are Low Impact.

Note that the terms *control room* and *Control Center* can be confusing. CIP auditors have ruled that most power plant control rooms are not BES Control Centers, because most such control rooms control generation at only one physical site. This means that the highest-impact systems normally found in power plants are Medium Impact BES Cyber Systems.

External Routable Connectivity and Unidirectional Gateways

The CIP V5 standards define External Routable Connectivity (ERC) as:

> *"The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection."*

When Waterfall Unidirectional Security Gateways are deployed as the sole means of communicating across an ESP, then the only communications through that ESP is hardware-enforced unidirectional communications, not bi-directional communications.

This means the BES Cyber Systems inside of ESPs protected by exclusively by Waterfall's Unidirectional Security Gateways have no External Routable Connectivity. This eliminates 32 of the 103 requirements and sub-requirements in the CIP V5 standard that would otherwise apply to Medium Impact BES Cyber Systems protected by firewalls.

Interactive Remote Access and Unidirectional Gateways

Interactive Remote Access is defined as:

> *"User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications."*

Waterfall's Remote Screen View product uses Unidirectional Security Gateways to replicate a real-time stream of screen images to external networks to make available to remote support personnel. The real-time stream of screen images allows remote personnel to give advice to a site when diagnosing and correcting complex problems.

CIP auditors have ruled that Remote Screen View does not constitute Interactive Remote Access, because the Waterfall Unidirectional Security Gateway hardware absolutely prohibits anyone outside an ESP from "initiating access" to the screens of unidirectionally-protected BES Cyber Systems.

This means that sites deploying Waterfall's Remote Screen View are exempt from all three CIP-005 V5 requirements for interactive remote access.

Electronic Access Points and Unidirectional Gateways

An Electronic Access Point is defined as:

> *"A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter."*

The unique design of the hardware and software in Waterfall's Unidirectional Security Gateways is not routable. This mean Waterfall's Unidirectional Gateways can be deployed to replicate industrial systems such as historians and OPC servers to corporate networks where they are accessible by business users, third parties and even cloud services, without having the gateways designated as EAPs.

Network Intrusion Detection Systems and Unidirectional Security Gateways

In particular, CIP-005 R1.5 requires that a NIDS to be deployed at every EAP for every High Impact BES Cyber System and in every EAP for every Medium Impact BES Cyber System a Control Center. This requirement is a specific response to FERC Order No. 706, which requires multiple layers of defenses for the most important BES Cyber Systems, because of the well-known limitations of firewalls.

Since Waterfall's Unidirectional Security Gateways do not constitute an EAP, the gateways are in effect an alternative to firewalls and NIDS. The V5 standards in this way recognize the stronger-than-firewall protections the gateways provide to protected critical networks, even networks of High Impact BES Cyber Systems.

Table of Exemptions

The table below summarizes which CIP V5 requirements "go away" for BES Cyber Systems protected by Waterfall's Unidirectional Security Gateways. For each exempted requirement, the columns in the table mean:

- **ID**: The CIP standard number and requirement number for the requirement
- **Description**: The full description of the requirement
- **Impact**: which classes of systems are exempt:
  - **High:** High Impact BES Cyber Systems,
  - **Medium:** Medium Impact BES Cyber Systems not at BES Control Centers, and/or
  - **Low:** Low impact BES Cyber Systems,

  and, if applicable, their

  - EACMS – Electronic Access Control or Monitoring Systems,
  - PACS – Physical Access Control Systems, and/or
  - PCA – Protected Cyber Assets, which are Cyber Assets within an ESP which may not themselves be BES Cyber Assets, but which "inherit" the impact level of the highest-impact BES Cyber System inside the ESP.
- **Reason**: The reason the requirement is exempted when BES Cyber Systems are protected by Unidirectional Security Gateways. The reason is one of:
  - **ERC:** exempt because the system has no External Routable Connectivity,
  - **EAP:** exempt because the system has no External Access Point, and/or
  - **IRA:** exempt because the system has no Interactive Remote Access

Note that the table below is only a summary. Security practitioners should consult the full NERC CIP standards to understand details and nuances of the requirements and exemptions summarized here.

Table of Exemptions

ID	Description	Impact	Reason
004-2.1	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Medium + EACMS, PACS	ERC

004-2.2	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Medium + EACMS, PACS	ERC
004-2.3	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Medium + EACMS, PACS	ERC
004-3.1	Process to confirm identity.	Medium + EACMS, PACS	ERC
004-3.2	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	Medium + EACMS, PACS	ERC
004-3.3	Criteria or process to evaluate criminal history records checks for authorizing access.	Medium + EACMS, PACS	ERC
004-3.4	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Medium + EACMS, PACS	ERC
004-3.5	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	Medium + EACMS, PACS	ERC
004-4.1	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	Medium + EACMS, PACS	ERC
004-4.2	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Medium + EACMS, PACS	ERC

004-4.3	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Medium + EACMS, PACS	ERC
004-4.4	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	Medium + EACMS, PACS	ERC
004-5.1	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	Medium + EACMS, PACS	ERC
004-5.2	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Medium + EACMS, PACS	ERC
004-5.3	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	Medium + EACMS, PACS	ERC
005-1.2	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	Medium + PCA	ERC
005-1.3	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	High Medium	EAP
005-1.5	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	High Medium	EAP
005-2.1	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	High + PCA Medium + PCA	IRA

005-2.2	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	High + PCA Medium + PCA	IRA
005-2.3	Require multi-factor authentication for all Interactive Remote Access sessions.	High + PCA Medium + PCA	IRA
006-1.2	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	Medium + EACMS, PCA	ERC
006-1.4	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	Medium + EACMS, PCA	ERC
006-1.5	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	Medium + EACMS, PCA	ERC
006-1.6	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	Medium + PACS	ERC
006-1.7	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	Medium + PACS	ERC
006-1.8	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	Medium + EACMS, PCA	ERC
006-1.9	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	Medium + EACMS, PCA	ERC
006-2.1	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	Medium + EACMS, PCA	ERC
006-2.2	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name,	Medium + EACMS, PCA	ERC

	and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.		
006-2.3	Retain visitor logs for at least ninety calendar days.	Medium + EACMS, PCA	ERC
006-3.1	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	Medium + PACS	ERC
007-1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Medium + EACMS, PACS, PCA	ERC
007-4.2	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure	Medium + EACMS, PACS, PCA	ERC
007-5.1	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	Medium + EACMS, PACS, PCA	ERC
007-5.3	Identify individuals who have authorized access to shared accounts.	Medium + EACMS, PACS, PCA	ERC
007-5.6	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Medium + EACMS, PACS, PCA	ERC

Table (1): Summary of Unidirectional Security Gateway Exemptions

Conclusions

The NERC CIP V5 standards position Unidirectional Security Gateways as a stronger alternative to firewalls and NIDS for protecting ESPs. The standards include measures to encourage the deployment of Unidirectional Gateways by simplifying CIP program requirements for gateway-protected BES Cyber Systems. When an ESP is protected by Waterfall's Unidirectional Security Gateways, Medium Impact BES Cyber Systems are rewarded with exemptions from 37 of the 103 requirements, and High Impact systems are exempted from 5 of the 103 requirements. Both Medium-Impact and High-Impact BES

Cyber systems are exempted from the costly CIP 005 R1.5 requirement for Network Intrusion Detection Systems when Waterfall's Unidirectional Security Gateways are deployed as the sole means of communications through an ESP.

With fewer rules to follow, deploying Waterfall's Unidirectional Gateways to increase the security of critical control systems simplifies and reduce the ongoing cost of V5 CIP compliance programs.

About Waterfall Security Solutions

Waterfall is the leading provider of strong network security products which protect the safety and the reliability of control system networks. Waterfall Security Solutions' mission is to eliminate the use of firewalls in critical infrastructure control systems. The company develops products which provide stronger-than-firewall protections for industrial control networks. Waterfall's products are deployed in utilities and critical national infrastructures throughout North America, Europe, Asia and the Middle-East. Waterfall's innovative products dramatically reduce the cost and complexity of compliance with NERC-CIP, NRC, NIST, CFATS and other regulations, and include support for leading industrial applications, including the OSIsoft PI™ Historian, the GE Proficy™ iHistorian, Siemens SIMATIC™/Spectrum™ solutions and GE OSM™ remote monitoring platforms, as well as OPC, Modbus, DNP3, ICCP and other industrial protocols. Frost & Sullivan describe Waterfall's solutions as ensuring "optimum security for networks across user verticals" and awarded Waterfall the 2012 Network Security Award for Industrial Control Systems Entrepreneurial Company of the Year, the 2013 North America Award for Customer Value Enhancement, and the 2014 Award for Global Oil and Gas Infrastructure Security New Product Innovation. For more information visit: www.waterfall-security.com.

Contact Us

Please contact Waterfall directly for additional information on this topic or on any topic related to Waterfall products.

Waterfall Security Solutions
1133 Broadway, Suite 708
New York, NY 10010
+1 212-714-6058
info@waterfall-security.com