# Waterfall Security Solutions Prepared Remarks for the FERC 2016 Supply Chain Integrity Technical Conference

*Andrew Ginter, VP Industrial Security*
*January 28, 2016*

My thanks to the commissioners and to everyone present for the opportunity to address you today.

The Bulk Electric System (BES) supply chain provides both physical and cyber products and services to NERC entities. All major industrial vendors have cyber or "cloud" offerings, which are used widely within the BES. Almost all of these cloud products and services demand connections to acquire real-time data from industrial control systems, and sometimes demand remote control, all from vendor control centers on the Internet. Compromise of vendor "cloud" systems can provide an attacker with the means to attack hundreds or thousands of sites in the North American grid, simultaneously.

For example, many entities with large power plants have segmented their plant networks by deploying just a handful of firewalls. When CIP Version 5 takes effect, even the largest of these segmented power plants will have no High-Impact BES Cyber systems, and no Medium-Impact systems. This is because each network segment controls less than 1500 MW of generating capacity. Segmentation is a legitimate security technique when the result is truly independent segments that make it difficult to propagate an attack from one segment to another, and difficult or impossible to attack all segments simultaneously. However, connections to cloud systems and corporate IT systems pass right through firewalls. At Waterfall, we know this as the NERC CIP firewall loophole.

A growing number of forward-thinking entities address this threat by deploying unidirectional security gateway technology to protect important networks, including segmented power plants. The gateways physically prevent any message from a cloud vendor or an IT network from reaching a protected network. Cloud providers can monitor unidirectionally-protected networks, but can neither control those networks nor compromise them. Entities can legitimately deploy fewer security controls to unidirectionally-protected, segmented networks, because such networks are effectively immune from simultaneous attack.

If vendors need to make changes to protected systems, unidirectional remote screen view technology lets the vendors see the screens of BES control systems, and provide advice to local personnel making changes, without risk to control systems. This is in contrast with CIP-compliant interactive remote access systems, which can be breached by attackers of even modest means. Security-bypass technology is another option for unidirectionally-protected networks. Entities activate this technology manually, to provide a vendor with temporary remote control of an otherwise unidirectionally-protected system.

The NERC CIP Version 5 standards encourage use of unidirectional gateways by reducing compliance costs for unidirectionally-protected systems; CIP V5 exempts unidirectionally-protected systems from bi-directional External Routable Connectivity requirements. In other jurisdictions, such as Europe, the Middle East and along the Pacific Rim, electric utilities are also using unidirectional protections to address cyber supply-chain risks. The same is true in other industries, including offshore platforms, petrochemical pipelines, and railway control systems.

The DHS NCCIC recommends unidirectional communications in three of its top seven strategies to defend industrial control systems, including the network segmentation strategy. NIST 800-82 Revision 2 positions unidirectional gateways as stronger than firewalls in defense-in-depth programs for industrial networks. The commission may also wish to examine how cyber-supply-chain risks are addressed by the French ANSSI critical infrastructure standards. The French standards forbid firewalled connections between the most important critical infrastructure networks and any less-critical networks. The standards forbid remote control of the most-critical networks. The standards though, permit unidirectional monitoring of all networks, and recommend unidirectional communications rather than firewalls.

When NERC entities ask industrial vendors for increased security in the form of unidirectional protections, we see an entire spectrum of responses. Some vendors embrace unidirectional technologies, including remote screen view. Others permit unidirectional gateways for continuous monitoring, but demand security bypass technology for occasional remote control. Still others reject unidirectional technology outright, arguing incorrectly that firewalls and encryption provide sufficient security.

To sum up: critical infrastructure sites in many industries and jurisdictions use unidirectional technology to address industrial cyber-supply-chain risks. Increased use of unidirectional security gateways in the Bulk Electric System will dramatically reduce cyber-supply-chain risks, and will measurably improve the security and the reliability of the Bulk Electric System.

Thank you again.

###