Prepared Remarks by

Bryan S. Owen, Principal Cyber Security Manager, OSIsoft LLC

Federal Energy Regulatory Commission Technical Conference on

Critical Infrastructure Protection Supply Chain Risk Management Issues Identified in Notice of Proposed Rulemaking Docket RM15-14-000

Discussion Panel 2: Scope and Implementation of a New or Modified Standard

January 28, 2016

Introduction

Good afternoon. Certainty of energy delivery is tied to prosperity in practically all walks of life. Addressing threats to reliable energy delivery is well deserving of a collective approach and the commission is to be applauded for holding this technical conference on the subject of supply chain risk management issues as related to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. I am pleased to appear here today with my esteemed industry colleagues to discuss matters important to managing supply chain risk.

My name is Bryan Owen. I am the Principal Cyber Security Manager at OSIsoft LLC, a family owned and operated software company headquartered in San Leandro, California. From a supply chain perspective, OSIsoft products and services are delivered as, and depend on, commercial off-the-shelf (COTS) technology infrastructure. OSIsoft is also a global supplier with offices around the world and is a Presidential "E" Award recipient for Exports by U.S. Department of Commerce.

My pledge as a Professional Engineer is to apply knowledge and skill to the betterment of human welfare above all other considerations. The views I express today are based on over 10 years active engagement with the industrial cyber security community, 15 years of field experience with industrial control systems, and 20 years serving OSIsoft customers - many of which are responsible for reliable delivery of electricity in North America (with many others operating major electrical loads). My views are also shaped personally, by smart grid innovations ranging from distributed generation in my home, to the yet to be realized vision for smart cities. I appreciate this opportunity to contribute observations and views on managing supply chain risk – especially software based risks.

Scope of Standards to Manage ICS Supply Chain Software Risks

Supply chains for Information and Communications Technology (ICT) and Industrial Control Systems (ICS) are complex, globally distributed and interconnected systems. Utilization is pervasive with hardware, software, and computing and networking services provided throughout national infrastructures as well as private enterprises. Direct and indirect obligations imposed on suppliers and vendors have significant potential for unintended consequence and market disruption.

In that Information and Communications Technology and Industrial Control Systems are so deeply entrenched in the bulk electric system, inclusive of upstream suppliers and downstream loads, it may be necessary to approach standards for supply chain security as a shared responsibility model.

For example, 'Fit for Use' in context of industrial safety hazards has been addressed using a shared responsibility model. Standards are defined for Safety Integrity Levels (SIL) and suppliers develop products for the most relevant use cases. Standards bodies are currently working to define Security Assurance Levels that could be used to develop new and modified ICS components with 'Fit for Use' specifications.

Until such time as ICS components build in security and reliability 'Fit for Use' with high impact Bulk Electric System (BES) cyber systems, the scope of new or modified CIP standards to manage supply chain risk should be kept to a minimum and voluntary. Imposing mandatory supply chain risk management beyond the most essential controls, over a foundation of legacy ICS devices, would likely exist only as '*security theater*'. It should remain a high priority to enable, rather than impede, ICS supply chain resources in delivery of 'Fit for Use' solutions.

Computing and networking services offered by Information and Communications Technology (ICT) providers further highlights the necessity of approaching standards for supply chain security as a shared responsibility model. The existing CIP Reliability Standards are unable to keep pace with rapid innovation of computing and networking services because current compliance audit approaches are not technically feasible for providers of modern computing and networking services. Thus, compliance implementation is a regressive force with respect to best available technology for reliability and security.

For instance, I frequently observe entities struggling to manage hundreds and even thousands of point to point VPN connections with external entities, whereas computing and network service providers offer alternatives with innovative reliability and security features. Such solutions are often dismissed out of hand due to compliance risk.

A shared responsibility model for supply chain security should be developed. The scope of new or modified CIP Reliability Standards should be voluntary and minimal at this time. Development of 'Fit for Use' specifications are proposed as the basis for a shared responsibility model addressing supply chain risks.

Essentials for Standards to Manage ICS Supply Chain Software Risks

The essentials for a new or modified standard to manage ICS supply chain cyber risks should focus on the identity of software publishers and associated incident response procedures.

As credit to the current CIP-004 Reliability Standards addressing personnel and training, in my experience these requirements have already permeated throughout the ICS supply chain. Modifications to this standard would likely be disruptive and of diminishing risk reduction.

However, identity of software publishers is a different story. The capability to identity software publishers represents a potential demarcation of responsibility to defend important threats within the ICS supply chain. Digital signatures offer a technical method to identify software publishers as well as providing for code authentication. Digital signatures could be a keystone for enabling ICS supply chain security controls for software, especially where control enforcement is already built into underlying runtime platforms.

The NIST 800-161 standard includes related guidance: 'organizations should ensure that code authentication mechanisms such as digital signatures are implemented to assure the integrity of software, firmware, and information of the ICT supply chain infrastructure and information system' and; 'consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions'.

Code signing with digital signatures is widely accepted as good practice in the software profession. There are few implementation barriers related to code signing although exceptions exist at scale and with technology (eg Javascript). Alternative mechanisms such as the NIST National Software Reference Library could be applied to identify ICS software and potentially the publisher. Commercial security services using binary analysis techniques are also emerging to fingerprint software, enumerate embedded third party libraries, and the associated known vulnerabilities. As such it seems well advised for any new or modified CIP Reliability Standard to prioritize the advancement of mechanisms used to identify ICS software publishers.

Identity of software publishers within the ICS supply chain is important to incident response. In practice, ICS supply chain entities are not necessarily notified about security issues discovered in their software. This communication issue is bi-directional. Security issues tend to be fixed silently by ICS suppliers and vendors without disclosure to responsible entities or industry coordination teams. A new or modified standard to drive improvements in communication and collaboration related to incident response is needed.

Under CIP-008-5, there is little if any incentive for reporting incidents. One idea is to revise the implementation and violation threshold to award an offset credit for reporting incidents. Reports including near misses, such as discovery of a vulnerability, could generate a dramatic uptick of communication about security issues across the supply chain. Alternately, a new or modified CIP Reliability Standard for improving security related communication across the ICS supply chain could be modeled after the voluntary Aviation Safety Reporting System.

Closing

Changes in the threat environment signal the need for increased vigilance and defensive agility throughout ICT and ICS supply chains. Supply chain complexity merits a shared responsibility model based on standards developed as 'fit for use' products and services. High impact Bulk Electric Systems should be the initial focus of 'fit for use' standards.

As an urgent priority, responsible entities need a good mechanism to assure Bulk Electric Systems operate with ICS software from their approved publishers.

Incentives for reporting supply chain security issues should be addressed in new or modified CIP Reliability Standards as a catalyst for better communication and incident response capability.

Finally, voluntary CIP Reliability Standards for managing supply chain security risk should explicitly advance best available technology. Let's not let compliance get in the way of innovation.

Thank you again for your time and I look forward to further discussion.