When completed, email this form to: sarcomm@nerc.com

Note: an Interpretation cannot be used to change a standard.

Interpretation 2014-02: Request for an Interpretation of CIP-007-5 & CIP-007-6, Requirement R2.1, for FoxGuard Solutions
Date submitted: July 8, 2015
Contact information for person requesting the interpretation:
Name: Michele Wright
Organization: FoxGuard Solutions, Inc.
Telephone: 540-382-4234,ext. 244
Email: mwright@foxguardsolutions.com
Identify the standard that needs clarification:
Standard Number (include version number): CIP-007-5 & CIP-007-6 (example: PRC-001-1)
Standard Title: Cyber Security – Systems Security Management
Identify specifically what requirement needs clarification:

Requirement Number and Text of Requirement:

R2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-5 & CIP-007-6 Table R2 – Security Patch Management*.

R2.1: A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a *source or sources* that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.

Clarification Requested:

From the aforementioned language in Requirement 2.1:

"The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists."

The measures section speaks to having a list of sources that are being monitored. In the Guidelines and Technical Basis section of this standard Requirement 2.1 states:

> *"Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates."*

****

Statement 1:
For compliance with these requirements, Responsible Entities are required to document the sources that they actively monitor for the release of cyber security patches. This could be one or multiple sources, often times a considerable number based on environment complexity and asset diversity. For many Responsible Entities, the ongoing monitoring of numerous sources can be a very labor intensive effort.

In 2013, the U.S. Department of Energy (DOE) awarded funding to simplify the efforts associated with patch and update management for energy delivery systems via way of a patch information aggregation portal. Reference U.S. DOE Funding Opportunity Announcement#: DE-FOA-0000797 – "Innovation for Increasing Cybersecurity for Energy Delivery Systems" (Topic 1) and "Patch and Update Management Program for Energy Delivery Systems".

In this scenario pertaining to Question 1 below, information about the release of cyber security patches is available via an aggregation source, while patches themselves are available directly from the "original" and "other" sources (as defined in The Guidelines and Technical Basis section of the standard). The aggregation source is one that may also reference the "original" and "other" sources as part of its content, both to provide additional information on the patch as well as to provide a means by which it can be acquired.

Question:
Can Responsible Entities identify and monitor a source that aggregates information about the release of cyber security patches from multiple "original" and "other" sources (as in defined in Requirement 2.1 of the Guidelines and Technical Basis section of the standard)?

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

Material Impact

Lack of clarity on what constitutes a "source" could cause Responsible Entities to spend unrecoverable person-hours attempting to monitor individual sources of cyber security patches for

hundreds (if not thousands) of operating systems, software applications, network devices and field devices. The possibility of overlooking an available cyber security patch released from the vendor is increased due to the sheer number increased systems / devices now under scope of CIP-007-5 and CIP-007-6 standards. The greatest impact on the Responsible Entity would be for their High and Medium Impact assets.