UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cyber Systems in Control Centers	**)**	**Docket No. RM16-18-000**

COMMENTS OF THE THE ISO/RTO COUNCIL

The ISO/RTO Council ("IRC") respectfully submits these comments in response to the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Inquiry ("NOI") for possible modifications to the Critical Infrastructure Protection ("CIP") Reliability Standards regarding the cybersecurity of Control Centers used to monitor and control the Bulk Electric System ("BES") in real time.[1]

The IRC strongly supports measures to enhance cyber security on the nation's bulk power system and in the control rooms that maintain reliable operations on the grid. Nevertheless, after careful review by the IRC members' operations and IT experts, the IRC believes that mandatory Reliability Standards as proposed in the Commission's NOI would not enhance cyber security of the power grid relative to the operational risks, issues, and costs that would result. As described in more detail below, the IRC believes that the logical separation provided under current Reliability Standards and practices results in the same level of protection without the added cost or potential negative impacts that could arise if physical separation of the Internet from BES Cyber Systems in Control Centers and application whitelisting were mandated.

Accordingly, the IRC submits these comments opposing modifications to CIP Reliability Standards that would require separating the Internet from BES Cyber Systems

[1] Notice of Inquiry, *Cyber Systems in Control Centers*, 156 FERC ¶ 61,051 (July 21, 2016).

in Control Centers. Currently effective NERC Reliability Standards already provide mandatory and enforceable controls and protections to prevent adverse impacts on the BES. Additionally, in the new version of CIP Reliability Standards that is currently being developed, NERC is already addressing FERC's directives in Order No. 822.[2] Those directives deal with the concerns described in the NOI. Furthermore, as described below, requiring complete isolation between the Internet and BES Cyber Systems in Control Centers presents potential complications and undesirable consequences. The IRC also opposes modifications to CIP Reliability Standards that would require "application whitelisting" for BES Cyber Systems in Control Centers. CIP Reliability Standards should allow flexibility regarding the technology that is used to comply with their requirements, and "application whitelisting" is a technology that presents many challenges and does not provide the needed flexibility, as described herein.

I. IDENTIFICATION OF FILING PARTY

The IRC is comprised of the following Independent System Operators ("ISOs") and Regional Transmission Organizations ("RTOs"): Alberta Electric System Operator ("AESO"); California Independent System Operator Corporation ("CAISO"); Electric Reliability Council of Texas, Inc. ("ERCOT"); the Independent Electricity System Operator ("IESO"); ISO New England Inc. ("ISO-NE"); Midcontinent Independent System Operator, Inc. ("MISO"); New York Independent System Operator, Inc. ("NYISO"); PJM Interconnection, L.L.C. ("PJM"); and Southwest Power Pool, Inc.

[2] Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards*, 154 FERC ¶ 61,037 (2016). Note that FERC Orders Nos. 706 and 791 also require protections against malware. The Standard Drafting Team that is currently developing the new version of CIP Reliability Standards will address FERC's directives in these three FERC orders.

("SPP"). [3] All IRC members have Control Centers that perform the functions of a transmission operator.

II. COMMENTS

A. FERC SHOULD NOT REQUIRE MODIFICATIONS TO CIP RELIABILITY STANDARDS RELATED TO SEPARATION BETWEEN THE INTERNET AND BES CYBER SYSTEMS IN CONTROL CENTERS

1. *Current Reliability Standards Already Provide for Separation Between the Internet and BES Cyber Systems, And Reliability Standards In Development Will Further Address FERC's Concerns*

The Commission seeks comments on whether CIP Reliability Standards should be modified to require isolation between the Internet and BES Cyber Systems in Control Centers performing the functions of a transmission operator. If isolation is required, the Commission asks whether logical isolation is preferable to physical isolation (or vice versa).[4]

With respect to communications within a transmission operator's Control Center, as the Commission correctly points out in the NOI, logical and physical separation are already addressed in current CIP Reliability Standards. For example, Reliability Standard CIP-005-5, Requirement R1, requires protections for BES Cyber Systems that include segmentation of networks supporting those systems and management of incoming and outgoing traffic for any access point to an Electronic Security Perimeter ("ESP"). Requirement R1 in Reliability Standard CIP-005-5 also requires direct analysis of incoming and outgoing network traffic for known or suspected malicious communication.

[3] The AESO and IESO are not FERC jurisdictional.

[4] NOI at P 11.

Reliability Standard CIP-005-5, Requirement R2, protects against unauthorized interactive remote access (note that this protects against not only Internet traffic but also against any untrusted network traffic). Reliability Standard CIP-006-6, Requirements R1 and R2, protect against unauthorized physical access to BES Cyber Systems and their related network infrastructure components (including Enterprise Access Control and Monitoring Systems - EACMS, Physical Access Control Systems - PACS and Protected Cyber Assets - PCA cases). Reliability Standard CIP-007-6, Requirement R3, requires that a responsible entity arrange to protect against malware using one or more means at the system or via the network layer. This protection can include network isolation techniques as well as Intrusion Detection/Prevention ("IDS/IPS") solutions where such protection is deemed appropriate and effective with regard to compliant operation of reliability functions.[5]

In addition to the current standards, in Project 2016-02, NERC is developing the next version of CIP Reliability Standards to address, among other things, FERC's directives in Order No. 822. Those directives include modifications to CIP Reliability Standards to "require responsible entities to implement controls to protect, at a minimum, communication links and sensitive BES data communicated between BES Control Centers in a manner that is appropriately tailored to address the risks posed to the BES by the assets being protected (*i.e.*, high, medium, or low impact)."[6] The modifications to

[5] *See* Section 3.1 of Reliability Standard CIP-007-6 Guidance and Technical Basis.

[6] Order No. 822 at P 53. FERC made clear that this directive also applies to Control Center communications from facilities at all impact levels, regardless of ownership; the directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications. *Id.* at P 58. FERC also clarified that the reliability gap addressed in Order No. 822 pertains to the lack of mandatory security controls to address how responsible entities should protect sensitive BES communications and data. *Id.* at P 60.

CIP Reliability Standards developed pursuant to this directive will better secure Control Centers from cyberattacks and, as such, will address the Commission's concerns in the NOI.

2. *Complications Would Arise If Complete Isolation Between The Internet And BES Cyber Systems Is Required Within Control Centers*

As stated above, sufficient logical and physical isolation between the Internet and BES Cyber Systems is already in place pursuant to current CIP Reliability Standards. Additional requirements in CIP Reliability Standards for complete isolation between the Internet and BES Cyber Systems within Control Centers would result in several complications for the ISOs/RTOs.

At some ISOs/RTOs, many reliability functions are not connected to the Internet and do not directly use data from the Internet. However, in other ISOs/RTOs' Control Centers, many BES Cyber Systems require the Internet to properly function. For instance, at some ISOs/RTOs, the Internet is used for market services systems, weather forecasting systems, situational awareness systems, and systems that allow information sharing with other parties. All these systems are currently used in control room operator consoles and other BES Cyber Assets within the ESP for economic and efficiency purposes. Consequently, if complete isolation from the Internet is expected, segregating external facing sites such as a market portal from BES Cyber Systems would require a significant amount of re-architecture and re-development. Essentially, the overall market system architecture would need to be redesigned to accommodate a split between the Internet-facing systems and internal systems for those ISOs/RTOs that include market systems in their CIP programs.

In addition to the daily functioning of the above systems, ISOs/RTOs use remote access through intermediate systems for activities such as critical operational support. If remote access through an intermediate system is not allowed due to dependence on the Internet, then ISOs/RTOs would need to provide onsite technical and system support 24 hours a day, seven days a week. Although many regions already have on-site support 24 hours a day, seven days a week, the extent of on-site support would have to be substantially increased. Additionally, this type of isolation from the Internet will make all Internet-based vendor support models inoperable, requiring vendors to provide alternative means to provide needed IT support. Moreover, Requirement R2 in CIP-005-5 already requires that Interactive Remote Access include two-factor separation for accessing BES Cyber Assets.

It is also important to note that many systems within the ESP have connections to non-CIP systems, which in turn connect to the Internet. This is how cyber security updates to operating systems and applications are downloaded and applied as required by CIP Reliability Standards. In addition, the Internet is required for updates to signatures for systems addressing malware, including intrusion detection systems and anti-virus deployments. If Internet use is disallowed and the systems inside the ESP have to be completely self-contained, corporate and market operations support systems would require a massive re-architecture. All back-office systems, as well as downstream consumers of operational data, such as market settlements, would need to be evaluated and likely redesigned or re-implemented to enable full isolation. Thus, the Commission's proposal would sweep away the availability of the array of support tools that have proven

helpful to operators ranging from system support updates to weather updates, as well as future support tools/technologies.

Finally, for some ISOs/RTOs, BES Cyber Systems rely on shared cyber assets, specifically circuits that carry BES and Internet traffic (for example, a market portal). These internet based systems are utilized particularly to accommodate smaller generators and demand response/distributed energy resources that may not have the financial viability to invest in a private network. If this is an issue, then some ISOs/RTOs systems would need to be migrated off the Internet to an alternate solution, such as a private Wide Area Network ("WAN"). This would require every market participant to connect to a highly available private network, which could significantly raise the cost of participation in the wholesale energy markets, thereby creating a potential barrier to entry. Also, shared hardware such as switches, firewalls, routers, and related equipment would need to be remediated. These changes could require substantial financial, resource and time investment for market participants to reengineer their entire market infrastructure.

3. *Complications Would Arise If Complete Physical Isolation Between The Internet And BES Cyber Systems Is Required*

The IRC submits that, with respect to communication between transmission operators, the multiple layers of logical separation that are currently used within shared data paths are considered best practices and are already used between ISOs/RTOs' Control Centers and other transmission operators. Specifically, ISOs/RTOs encrypt communicated data, which can only be decrypted by those who are authorized to receive the data, and telecommunication providers use multi-protocol label switching to tag the

data.[7] Tagged data can only be received by the set of the telecommunication provider's customers that are connected with that particular label. If, notwithstanding these multiple layers of logical separation, the Commission directs that CIP Reliability Standards be modified to require complete physical isolation between the Internet and BES Cyber Systems, complications would arise.

With respect to the cost and resource impact of imposing physically separate networks, the cost will depend on the circumstances of each entity and available existing infrastructure. However, it is plausible that the cost, in terms of dollars and resources, could potentially be significant. The problem is that the corresponding reliability benefits relative to the existing Reliability Standards and business practices will be minimal to null, and, as discussed, could actually create issues that result in circumstances that are less effective than the current paradigm from both a reliability and functional perspective. Thus, there is no rational justification for the change and associated cost/resource impacts. Moreover, even if a transmission operator can physically separate data connections, the separation would not serve to increase system security because those connections will still have to share common physical infrastructure such as telephone poles, power sources, and common data centers. Thus, even if a transmission operator built its own dedicated path, a physical attack to telecommunications infrastructure could still take both the common Internet path and a dedicated data path out of service.

B. APPLICATION WHITELISTING FOR BES CYBER SYSTEMS IN CONTROL CENTERS SHOULD NOT BE REQUIRED

Reliability Standards should establish "what" responsible entities are required to do, but should not be prescriptive with respect to "how" responsible entities should

[7] *See* NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.

comply with the requirements in the standards.[8] More specifically, as the Commission has recently stated, CIP Reliability Standards should be results-based in order to provide flexibility to account for the range of technologies and entities involved in BES communications.[9] Thus, rather than requiring that a specific technology be used to protect BES Cyber Systems, CIP Reliability Standards should establish the goals for protection. Indeed, in keeping with this fundamental principle, Reliability Standard CIP-007-6 already allows the use of "application whitelisting" as one of the methods that can be used to protect BES Cyber Systems from malware. Specifically, the Guidance for Reliability Standard CIP-007-6, Requirement R3 provides as follows (emphasis added):

> 3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, ***white-listing solutions***, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.
>
> 3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the

[8] *See, e.g.,* Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards,* 156 FERC ¶ 61,050 (2016) at P 45.

[9] *Revised Critical Infrastructure Protection Reliability Standards*, 154 FERC ¶ 61,037 (2016) at P 55.

> malicious code. In ***white-listing situations***, ***the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset***. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.
>
> Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

Additionally, Attachment 1 to Reliability Standard CIP-010-2, specifically lists application whitelisting as one of the methods allowed to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset Capability).

Notably, while some ISOs/RTOs have used application whitelisting tools to protect their BES Cyber Assets, requiring application whitelisting in all instances would present several obstacles. For instance, tuning for whitelisting is challenging and implementations could have real-time operational impacts. Not all operating systems work well with whitelisting, as they can cause an accidental Denial of Service ("DoS"). Routine activities, such as operating system patches, cause multiple files to change which can conflict with whitelisting. False positives can prevent systems from functioning properly and application whitelisting can cause additional performance overhead on servers and devices. Additionally, to achieve the desired end result, tuning solutions

requires check-summing or an equivalent to ensure a malicious program is not just renamed to an allowed program.

The most effective "application whitelisting" relies on accurate and well-maintained baselines in line, with the recent implementation of enhanced configuration management controls required under CIP Reliability Standard CIP-010-2. In addition, if "application whitelisting" is not available for a given device or operating system, or could create significant operational impact, other alternatives should be allowed to achieve the same security objective. This would be consistent with the shift in language within Reliability Standard CIP-007-6 Requirement 3, Part 3.1, which now allows entities to select their method to deter, detect, or prevent malicious code, rather than specifically requiring installation of anti-virus/anti-malware, as was the case in Reliability Standard CIP-007-3. Similarly, NERC Reliability Standard CIP-010-2, Requirement R4 requires each responsible entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, to implement one or more documented plans for Transient Cyber Assets and Removable Media that include the sections in Attachment 1 (which, as described above, includes application whitelisting as one of the methods that responsible entities can use).

Therefore, for all the reasons noted, the IRC respectfully submits that additional requirements in CIP Reliability Standards specifically requiring "application whitelisting" are not necessary, and, in fact, may prove to be problematic and counterproductive.

III. CONCLUSION

The IRC requests that the Commission consider these comments on the NOI.

Respectfully submitted,

/s/ *Anna McKenna*
Roger E. Collanton, General Counsel
Anna McKenna
Assistant General Counsel, Regulatory
California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
amckenna@caiso.com

/s/ Carl Patka
Robert E. Fernandez, General Counsel
Raymond Stalter,
Director of Regulatory Affairs
Carl Patka, Assistant General Counsel
New York Independent System Operator, Inc.
10 Krey Boulevard
cpatka@nyiso.com

/s/ Margoth Caley
Raymond W. Hepper
Vice President, General Counsel, and Secretary
Theodore J. Paradise
Assistant General Counsel, Operations and Planning
Margoth Caley
Senior Regulatory Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
mcaley@io-ne.com

/s/ Craig Glazer
Craig Glazer
Vice President-Federal Government Policy
James M. Burlew
Senior Counsel
PJM Interconnection, L.L.C.
Suite 600
1200 G Street, N.W.
Washington, D.C. 20005
202-423-4743
Craig.Glazer@pjm.com
James.Burlew@pjm.com

/s/ Stephen G. Kozey
Stephen G. Kozey
Senior Vice President
Joseph G. Gardner
Vice President & Chief Compliance Officer
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, Indiana 46032
stevekozey@misoenergy.org

/s/ Nathan Bigbee
Chad V. Seely
Vice President and General Counsel
Nathan Bigbee
Assistant General Counsel
Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744
Nathan.bigbee@ercot.com

/s/ Nancy Marconi
Nancy Marconi
Sr. Manager, Regulatory Affairs
Independent Electricity System Operator
1600-120 Adelaide Street West
Toronto Ontario M5H1T1
Canada

/s/ Matt Morais
Paul Suskie
Sr. VP Regulatory Policy
& General Counsel
Matt Morais
Associate General Counsel, Markets and Regulatory Policy
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
mmorais@spp.org

/s/ Diana Pommen
Diana Pommen
Director Interjurisdictional Affairs and Compliance
Alberta Electric System Operator
2500, 330 - 5 Avenue SW
Calgary, Alberta T2P 0L4
Diana.pommen@aeso.ca

Dated: September 26, 2016

CERTIFICATE OF SERVICE

I hereby certify that I have this day served the foregoing document upon each person designated on the official service list compiled by the Secretary in this proceeding.

Dated at Holyoke, Massachusetts this 26th day of September, 2016.

/s/ Julie Horgan
Julie Horgan
eTariff Coordinator
ISO New England Inc.
One Sullivan Road
Holyoke, MA 01040
(413) 540-4683