UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security	)))	Docket No. RM20-19-000

COMMENTS OF THE ISO/RTO COUNCIL

The ISO/RTO Council ("IRC")[1] submits these comments and responses in reply to the Notice of Inquiry that the Federal Energy Regulatory Commission ("FERC" or "Commission") issued in Docket No. RM20-19-000 on September 17, 2020.[2] In the NOI, the Commission seeks information on the potential risks to the bulk electric system ("BES") posed by using equipment and services produced or provided by entities identified as risks to national security.[3]

I. IRC RESPONSES TO QUESTIONS POSED IN THE NOI

The IRC provides the following responses to certain questions posed in the NOI.

---

[1] The IRC comprises the following independent system operators ("ISOs") and regional transmission organization ("RTOs"): Alberta Electric System Operator ("AESO"); California Independent System Operator ("CAISO"); Electric Reliability Council of Texas, Inc. ("ERCOT"); the Independent Electricity System Operator of Ontario, Inc. ("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. ("SPP").

[2] *Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security*, Notice of Inquiry, 172 FERC ¶ 61,224 (2020) ("NOI").

[3] NOI at P 1.

A. *NOI Question 1(a): What methods could be used to ascertain the extent to which equipment and services provided by Covered Companies is used in the operation of the bulk electric system?*

In many cases, responsible entities[4] do not procure equipment and services directly from Covered Companies.[5] Instead, this equipment is commonly a component or subcomponent of equipment purchased from companies that operate under different names. Responsible entities could attempt to ascertain the extent of their use of equipment provided by Covered Companies by inquiring with vendors and resellers on their use of telecommunications and video surveillance services from specific Covered Companies at the component level. However, most often, there is no practical method of ascertaining the use of components from Covered Companies within products under different brand names because the necessary transparency in the supply chain does not exist today.

Although responsible entities may try to probe their suppliers for information regarding the use of equipment and components from the Covered Companies in their respective supply chains, at the end of the day, because the federal government has access to classified information, the federal government is best positioned to provide the industry with the most useful information on potential threats through processes established for communicating such information.

---

[4] *See id.* at P 15 (explaining that responsible entities include reliability coordinators, balancing authorities, and transmission operators).

[5] *See id.* at PP 11, 19 (defining Covered Companies as companies that produce or provide "covered telecommunications equipment or services" as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3) (2018) ("2019 NDAA"); citing the definition of "covered telecommunications equipment or services" ("Covered Equipment") in the 2019 NDAA as: "…(1) telecommunications equipment produced by Huawei or ZTE or any subsidiary or affiliate of such entities; (2) video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company or any subsidiary or affiliate of such entities; (3) telecommunications or video surveillance services provided by such entities or using such equipment; or (4) telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense . . . reasonably believes to be an entity owned or controlled by, or otherwise connected to, the . . . People's Republic of China.").

Information technology ("IT") network discovery tools could potentially be used to identify and inventory the use of components within equipment for some Covered Companies. Although these tools may identify some equipment components that reveal the manufacturer using the media access control ("MAC") address, this approach would be insufficient to determine all component manufacturers.

B. NOI Question 1(b): Describe any potential complications to system operations that may result from implementing such methods (e.g., need to shut down certain activities to perform testing).

The processes described in the IRC's response to Question 1(a) are non-intrusive evaluation and network discovery processes that will have minimal impact on operations.

C. NOI Question 2(a): Describe the range of potential security impacts to bulk electric system reliability that could occur if a responsible entity uses the equipment and services provided by the Covered Companies within its real-time operations infrastructure and the equipment was compromised.

At the lowest level of security impact, a responsible entity's use of equipment from Covered Companies may not be accessible for exploitation by Covered Companies because of network segmentation that prevents direct and indirect access to installed components. At a moderate level of security impact, Covered Companies may be able to eavesdrop on the responsible entity's communications equipment and video surveillance equipment, which would provide information about internal operations as well as other sensitive information. At a high level of security impact, Covered Companies may be able to modify or disrupt the responsible entity's telecommunications equipment and the communications it supports. Where the impact would fall in the range depends on hostile intent. Any of these is possible, depending on what an adversary intends to do with the components. As noted below, RTOs and ISOs have defense in depth processes to identify and address any such intended intrusions.

D. NOI Question 2(b): If equipment and services provided by Covered Companies is installed in a responsible entity's real-time operations infrastructure, what controls are in place to prevent or detect compromise? What controls are in place to mitigate the potential effects of compromise?

The following controls are in place to mitigate the potential effects:

- Pursuant to the North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") Reliability Standards, high and medium impact BES Cyber Systems[6] are identified and subject to mandatory security standards, including configuration management and network segmentation.
- Security event monitoring detects and enables response to suspicious events.
- Vulnerability assessments and patch management reduce the attack surface to the IT and operational technology ("OT") networks and reduce the risk of lateral movement.
- United States government monitoring services are available in several instances to detect vulnerabilities or signs of potential compromises, including the Department of Homeland Security Cyber Hygiene program and the Electricity Information Sharing and Analysis Center ("E-ISAC") Cyber Risk Information Sharing Program ("CRISP").
- Commercial monitoring services are used by some entities to identify vulnerabilities or signs of potential compromises.
- Responsible entities have deployed intrusion detection and prevention systems that monitor the internet boundary of responsible entities and/or communication through electronic security perimeters ("ESP").

[6] *See* NERC, *Glossary of Terms Used in NERC Reliability Standards*, p. 4 (Oct. 8, 2020) (defining BES Cyber System).

E. *NOI Question 2(c): Describe the range of potential security impacts to bulk electric system reliability from a compromise of a responsible entity's systems related to nonreal time bulk electric system operations (e.g., operations planning) resulting from the use of equipment and services provided by Covered Companies.*

See the response to NOI Question 2(a) above.

F. *NOI Question 2(d): If equipment and services provided by Covered Companies is installed in a non-real time environment (e.g. operations planning), what controls are in place to prevent or detect compromise? What controls are in place to mitigate the potential effects of compromise?*

See the response to NOI Question 2(b) above.

G. *NOI Question 2(e): Describe the potential range of security impacts to bulk electric system reliability from a compromise of responsible entity's systems related to nonbulk electric system communications and operations (e.g., business networks and systems not directly related to bulk electric system operations) resulting from the use of equipment and services provided by Covered Companies.*

See the response to NOI Question 2(a) above.

H. *NOI Question 2(f): If equipment and services provided by Covered Companies is installed in a non-bulk electric system communications and operations environment (e.g., business networks and systems not directly related to bulk electric system operations), what controls are in place to prevent or detect compromise? What controls are in place to mitigate the potential effects of compromise? What controls are in place to prevent compromise of business network or systems from migrating and impacting bulk electric system operations?*

See the response to NOI Question 2(b) above.

I. *NOI Question 3(a): Which requirements of the CIP Reliability Standards, including complementary requirements across the CIP Reliability Standards, require entities to take actions that detect and mitigate the risks associated with the use of equipment and services provided by Covered Companies?*

The following CIP Reliability Standards require entities to take actions that detect and mitigate the risks associated with the use of equipment and services provided by Covered Companies:

- CIP-002, Requirement R1, BES Cyber System Categorization, is designed to identify critical systems and protect them commensurate with their risk level.
- CIP-003, Requirement R1, Cyber Security Policy, is designed so that security practices are in place to protect the overall environment from attack.
- CIP-003, Requirement R2, Cyber Security Plans for Low Impact BES Cyber Systems, requires security plans for all systems, including low impact systems, in order to protect the overall environment from attack.
- CIP-004, Requirement R4, Access Management Program, requires appropriate access management, which can prevent lateral movement of adversaries.
- CIP-004, Requirement R5, Access Revocation, is designed to promptly remove access that is no longer needed thereby preventing malicious use of dormant accounts.
- CIP-005, Requirement R1, Electronic Security Perimeter, segments the network to protect the most critical sections of the network from attacks that may emanate from compromised components.
- CIP-005, Requirement R2, Interactive Remote Access Management, is designed so that network segmentation does not have exposures that may allow attacks from compromised components to propagate through electronic security perimeters.

- CIP-006, Requirement R1, Physical Security Plan, requires that compensating controls, such as access logging, be put in place as a supplement to video surveillance.
- CIP-007, Requirements R1 – R5, Systems Security Management, are designed to harden systems against attacks, which can prevent lateral movement emanating from compromised components. In addition, security event monitoring detects attacks to enable rapid response.
- CIP-008, Requirements R1 – R3, Incident Reporting and Response Planning, require cyber incident response activities to be planned in advance and exercised, which reduces the potential impact of a compromised component by reducing the dwell time of an attack.
- CIP-010, Configuration Change Management and Vulnerability Assessments, requires the components of CIP cyber assets to be identified, documented, and monitored as part of configuration baselines. In addition, vulnerability assessments help reduce the risk of lateral movement, in the event of a malicious component from Covered Companies, by reducing the attack surface of the computers on the network.
- CIP-011, Information Protection, provides security for BES Cyber System Information[7] ("BCSI") to prevent unauthorized access to sensitive information if malicious activity occurs resulting from deployed equipment from a Covered Company.

[7] *See* NERC, *Glossary of Terms Used in NERC Reliability Standards*, p. 4 (Oct. 8, 2020) (defining BES Cyber System Information).

- CIP-013, Supply Chain Risk Management, requires responsible entities to use a cybersecurity risk-based procurement process in the procurement of cyber systems to identify and reduce security risks that may be introduced by equipment and services from Covered Companies.

The breadth of cybersecurity requirements in the NERC CIP Reliability Standards helps mitigate supply chain risks, and NERC has two additional CIP projects underway that will further address supply chain risks.[8] However, the NERC CIP Reliability Standards only apply to responsible entities. Further mitigating supply chain risks requires partnerships with other government and industry entities, which are not subject to the NERC CIP Reliability Standards. Such partnerships will be needed to address supply chain provenance.

J. NOI Question 3(b): What modifications to the CIP Standards would minimize risks associated with equipment and services provided by the Covered Companies?

As described above, the current CIP Reliability Standards reduce the supply chain risks associated with the procurement of equipment and services provided by Covered Companies. The recent addition of CIP-013, Supply Chain Risk Management, has provided additional requirements for responsible entities to address supply chain cybersecurity risk management. One addition to the CIP-013 standard that may be beneficial would be to require responsible entities to verify that suppliers are not on federal blacklists of vendors when making purchases and/or updating risk assessments.

[8] *See* NERC, *Project 2019-03 Cyber Security Supply Chain Risks*, NERC.COM, https://www.nerc.com/pa/Stand/Pages/Project2019-03CyberSecuritySupplyChain-Risks.aspx (last visited Nov. 23, 2020); *see also* NERC, *Project 2020-03 Supply Chain Low Impact Revisions*, NERC.COM, https://www.nerc.com/pa/Stand/Pages/Project_2020-03_Supply_Chain_Low_Impact_Revisions.aspx (last visited Nov. 23, 2020).

Verification of the appearance of a supplier on a federal blacklist would require that that the federal government identify, assess, and communicate these blacklists with responsible entities because responsible entities will not have access to this information without such information sharing.

K. NOI Question 4: Describe any strategies, in addition to compliance with the CIP Reliability Standards, entities have implemented or plan to implement to mitigate the risks associated with use of equipment and services provided by Covered Companies.

Many responsible entities rely on penetration tests and compromise assessment from third parties to help assess whether there are signs of network exploitation. This strategy helps to identify risks associated with compromised equipment from Covered Companies. Many responsible entities also rely on federally-supported security event monitoring and threat information sharing sources that help to spot signs of command and control activity. Command and control activity may be a strong indicator of malicious equipment from Covered Companies.

Technology-based practices for mitigating these risks are generally part of provenance,[9] which may rely on newer technologies that have not matured. Some responsible entities have been following the potential for enabling technologies such as blockchain to help support provenance assessment. In the absence of technology and standard practices to address this risk, responsible entities would need access to procurement channels that are generally open only to federal government programs to clear equipment before procurement.

[9] Provenance is a record that describes entities and processes involved in producing and delivering or otherwise influencing data. Provenance enables businesses to verify and authenticate data and information.

L. NOI Question 5(a): Describe how your organization is informed of the risks to bulk electric system reliability and security posed by the use of equipment and services provided by Covered Companies and what could be done to improve this process.

The members of the IRC are generally informed about risks associated with equipment and services provided by Covered Companies through the E-ISAC, the Department of Homeland Security, the Department of Energy, and public announcements from the executive branch. This information is generally available after equipment is purchased and deployed, and requires investigation to assess the risk and develop mitigation strategies. No information is provided to members of the IRC prior to an equipment purchase to inform the decision with respect to risks related to the Covered Companies. The Commission should work to provide more transparency into supply chain threats during the procurement phase, especially for products produced by Covered Companies.

M. NOI Question 5(b): What actions has your organization taken to address these risks and what impediments exist to do so (i.e., such as procurement process requirements)?

Because the information about these risks is not provided in advance of purchasing decisions, responsible entities are forced to utilize their own individual supply chain controls to assess the risk and respond accordingly. The members of the IRC have responded to NERC alerts to support industry-wide initiatives to reduce this supply chain risk. Members of the IRC are also helping to advance best practices through collaboration with the North American Transmission Forum ("NATF") and the Department of Energy. Some IRC member companies are working with commercial third-party assessors of supply chain risk to leverage the best practices and specialization supported by these

assessors. Furthermore, industries outside Commission authority need to work in concert with NERC to identify risks and solutions.

Since the federal government often classifies supply chain threats, the IRC would value assistance from the Commission in accessing information about these risks either through more private industry access to classified intelligence or through more effective downgrading of classified information to support the procurement process.

N. NOI Question 5(c): What challenges does your organization face when identifying, containing or removing equipment that presents supply chain threats from Covered Companies?

Identification of supply chain threats is challenging because the supply chain is not transparent. Transparency gaps exist between customers, resellers, manufacturers, and component suppliers. Transparency gaps also exist between the federal government, which may be aware of threats, and responsible entities, which are not provided information about these threats during the procurement process and often during operations. Containing and removing deployed equipment is challenging because it takes time to evaluate alternative product offerings, secure funding, procure new equipment, deploy and integrate new equipment, and test the changes. Managing supply chain threats results in additional costs to suppliers, responsible entities, and ratepayers. As a result, it is important to identify supply chain threats before purchasing equipment, avoid false alarms, and maintain the reliability of the BES at an effective price. In summary, the IRC would value assistance from the Commission in identifying supply chain threats early in the system development lifecycle in order to limit the exposure time of malevolent products and components, and reduce the cost of rework.

II. CONCLUSION

The IRC respectfully requests that the Commission accept these comments.

Respectfully submitted,

/s/ Margoth Caley
Maria Gulluni
Vice President & General Counsel
Margoth Caley
Senior Regulatory Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
mcaley@iso-ne.com

/s/ James M. Burlew
Craig Glazer
Vice President-Federal Government Policy
James M. Burlew
Senior Counsel
PJM Interconnection, L.L.C.
2750 Monroe Boulevard
Audubon, Pennsylvania 19403
james.burlew@pjm.com

/s/ Andrew Ulmer
Roger E. Collanton, General Counsel
Anthony Ivancovich, Deputy General Counsel, Regulatory
Andrew Ulmer Director, Federal Regulatory Affairs
California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
aulmer@caiso.com

/s/ Carl F. Patka
Robert E. Fernandez, General Counsel
Raymond Stalter
Director of Regulatory Affairs
Carl F. Patka
Assistant General Counsel
Christopher R. Sharp
Senior Compliance Attorney
New York Independent System Operator, Inc.
10 Krey Boulevard
Rensselaer, NY 12144
cpatka@nyiso.com

/s/ Andre T. Porter
Andre T. Porter
Vice President, General Counsel & Secretary
Mary-James Young
Senior Corporate Counsel
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, Indiana 46032
aporter@misoenergy.org

/s/ Paul Suskie
Paul Suskie
Executive Vice President & General Counsel
Mike Riley
Associate General Counsel
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

/s/ Devon Huber
Devon Huber
Senior Manager, Regulatory Affairs
Independent Electricity System Operator
1600-120 Adelaide Street West
Toronto, Ontario M5H1T1
Canada
devon.huber@ieso.ca

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

/s/ Diana Wilson
Diana Wilson
Director Enterprise Risk Management and Compliance
Alberta Electric System Operator
#2500, 330 — 5 Avenue SW
Calgary, Alberta T2P 0L4
Diana.wilson@aeso.ca

November 23, 2020