UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF HOMELAND SECURITY

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements	**:** **:** **:**	**Docket No. CISA-2022-0010**

COMMENTS OF THE ISO/RTO COUNCIL

The ISO/RTO Council ("IRC")[1] respectfully submits these comments in response to the Cybersecurity and Infrastructure Security Agency's ("CISA") Notice of Proposed Rulemaking regarding Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"[2]) reporting requirements.[3]

The IRC recognizes CIRCIA's and any final rule's potential impact on the ISOs/RTOs, other public utilities, generators, gas pipelines, and other stakeholders and critical infrastructure. The IRC emphasizes that – like the statutory aims of CIRCIA itself[4] – the ISOs/RTOs' priorities remain reliable and secure system operations, transparency about critical security threats, and the maintenance of effective and compliant crisis management and emergency response plans in the

[1] The IRC comprises the following independent system operators ("ISOs") and regional transmission organizations ("RTOs"): Alberta Electric System Operator ("AESO"); California Independent System Operator ("CAISO"); Electric Reliability Council of Texas, Inc. ("ERCOT"); the Independent Electricity System Operator ("IESO") of Ontario; 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"). AESO and IESO are not subject to the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") reporting requirements and therefore do not join this filing.

[2] 6 U.S.C. §§ 681-681g.

[3] *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements,* 89 Fed. Reg. 23,644-01 (April 4, 2024) ("NPRM"). Citations to the NPRM will include a pinpoint citation to the printed page in the Federal Register.

[4] 6 U.S.C. § 681b(c)(1)(C) (noting covered entities should include entities for which "accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure").

event of a Covered Cyber Incident[5] (or any Cyber Incident) or Ransom Payment scenario. The IRC anticipates continuing to comply with existing regulatory regimes and to work with their stakeholders to encourage proactive engagement by any stakeholder impacted by a cyber incident, regardless of whether such an incident is covered by CIRCIA or any final rule issued in this proceeding. Such proactive engagement and collaboration is essential to the collective efforts shared by the ISOs/RTOs and their stakeholders in ensuring safe and reliable system operations.

As CISA prepares to finalize issuance of a final rule in this proceeding, the IRC urges the agency to consider the following comments.

I. CISA Should Continue Collaboration with Other Agencies.

The NPRM appropriately recognizes the existence of the current cyber incident reporting landscape for highly-regulated public utilities, and the IRC appreciates the NPRM's signaling of ongoing efforts to promote intra-agency coordination to potentially streamline reporting requirements for Covered Entities confronting a potential crisis.[6] CISA should continue its education, outreach, and collaboration efforts with its sister agencies (including, but not limited to, the Department of Energy and the Federal Energy Regulatory Commission), other related entities (like the North American Electric Reliability Corporation and its Electric Information Sharing and Analysis Center), and the ISOs and RTOs. To that end, the IRC urges CISA and

[5] Unless otherwise defined, capitalized terms shall have the definition given to them in CIRCIA or the NPRM.

[6] *See* NPRM at 23,650 (discussing, among other things, the Department of Energy (DOE) DOE-417 reporting requirements and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard CIP-008-6: Cyber Security—Incident Reporting and Response Planning).

other agencies to promptly solicit input from stakeholders on potential CIRCIA Agreements and enter into, and post in a central location on the CISA website, all such agreements once executed.

II. CISA Should Also Engage with Stakeholders Through a Technical Conference to Streamline Reporting Requirements.

The IRC encourages CISA to engage with the ISOs/RTOs and other stakeholders – ideally through a technical conference – on provisions of CIRCIA Agreements and the design of any web-based reporting forms. Such efforts will promote industry understanding about the contents of CIRCIA Agreements and CIRCIA Reports, and they will realize efficiencies in the submission of required reporting. Among other things, such efforts should identify opportunities to flag in any web-based forms what portion(s) of those forms must be protected from disclosure because they contain confidential information, including but not limited to commercial, financial, and proprietary information, market sensitive information, and/or other Bulk Electric System information. In addition, those forms and any final rule issued in this proceeding should emphasize that the perfect should not be the enemy of the good when it comes to the submission of initial reports required by CIRCIA or any final rule in this proceeding. While good faith efforts should be made to submit fulsome reports, the statute and regulations appropriately recognize a role for supplemental reports to update or augment previously submitted reports.

The IRC also encourages efforts to harmonize and streamline reporting requirements by Covered Entities subject to multiple reporting requirements to yield efficiencies for any Covered Entities that may be forced to respond to crisis and emergency situations while maintaining reliable access to critical infrastructure. On this subject, CISA should clarify the extent to which any existing Cyber Information Sharing and Collaboration Agreements ("CISCAs") or Cooperative Research and Development Agreements ("CRADAs") between CISA and Covered Entities may implicate the reporting requirements in any final rule issued in this proceeding.

III. To Avoid Unintended Consequences, CISA Should Engage in a Case-By-Case Review of the Appropriate Treatment of Information Produced in Response to a Subpoena.

Given the potential national security, privacy, and civil liberty implications of the NPRM's proposal set forth in 6 C.F.R. § 226.14(d)(6), the IRC urges CISA to eschew a rigid proposed approach for the treatment of information received in response to a subpoena, and instead adopt a case-by-case approach to determine the appropriate treatment of such information.[7] Absent a fact-specific review of the appropriate information protection treatment in particular circumstances, CISA's desire to incent compliance[8] could have the unintended and unnecessary consequence of automatically compounding the impacts of Substantial Cyber Incidents, including for entities that have no culpability for a failure to comply with a duly-issued subpoena. A case-specific approach to information treatment would mitigate such unintended and unnecessary consequences, without undermining CISA's enforcement powers given the other enforcement tools available to the agency.

IV. A Final Rule in this Proceeding Should Re-Emphasize the Case-Specific Nature of a "Reasonable Belief" Inquiry.

The IRC observes that both CIRCIA and the NPRM trigger a reporting requirement when a Covered Entity "reasonably believes that the covered cyber incident has occurred."[9] The NPRM correctly describes this finding as <u>not</u> prescriptive given the case-specific and fact-intensive nature of the inquiry. The IRC agrees with CISA that it would be inaccurate to assume such a finding could be rendered "immediately upon occurrence of the incident[.]"[10] Further, the

[7] *See* NPRM at 23,737 (Request for Comment 63, seeking comment on "the treatment of information received in response to a subpoena").

[8] NPRM at 23,735-23,736.

[9] 6 U.S.C. § 681b(a)(1)(A); 6 C.F.R. § 226.5(a).

[10] *See* NPRM at 23,725

NPRM correctly recognizes that a promptly-convened preliminary analysis will likely be required before a "reasonable belief" can be obtained.

However, the IRC observes that the NPRM's "belief" that a "preliminary analysis should be relatively short in duration (i.e., hours, not days)" before the finding is rendered may in many instances understate the complexity of the required analysis given the particular circumstances and the implicated entity or entities. While time is certainly of the essence, it is unclear what record evidence exists to support the assertion that the finding should be rendered in "hours not days." There is also a risk that with such an expectation stated in the record, a sprint for compliance may unintentionally divert resources and focus away from effective crisis management and emergency response at a critical juncture in a preliminary analysis. The IRC urges that any final rule in this proceeding simply re-emphasize the case-specific nature of the "reasonable belief" inquiry following a promptly-convened preliminary analysis without suggesting a specific time table in hours for rendering the determination.

V. Any Final Rule in this Proceeding Should Confirm that an Inadvertent Disclosure of Confidential Information that Does Not Impact an Information System is not a Substantial Cyber Incident.

Any final rule in this proceeding should confirm that, consistent with CIRCIA's intent and statutory text, a Substantial Cyber Incident will not arise in the case of an inadvertent disclosure of confidential information by a Covered Entity that does not impact other information on an information system or the information system itself. Such a fact pattern does not fit within the statutory definition of a Cyber Incident,[11] and thus cannot be a Covered Cyber Incident or a Substantial Cyber Incident.[12]

[11] 6 U.S.C. § 681(5).

[12] In both CIRCIA and the proposed rule, defined terms relying on the term "Incident" appear in the following permutations: Incident, Cyber Incident, Covered Cyber Incident, and Substantial Cyber

The statute makes plain that the meaning of Incident is defined to mean "an occurrence that actually . . . jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information **on an information system**, or actually . . . jeopardizes, without lawful authority, **an information system**."[13] As such, only occurrences that actually impact other information on an information system or impact the information system itself can give rise to a Cyber Incident under CIRCIA or any final rule. To read the statute otherwise would also have unintended consequences, transmuting any inadvertent disclosure of confidential information into a Cyber Incident simply because that piece of information may reside on an information system. In addition, the inadvertent disclosure of confidential information that resides on an information system should not, in and of itself, give rise to a "covered cyber incident" under the statute[14] because such an incident is neither "substantial"[15] nor does such an

Incident. The IRC notes the importance that such terms be clearly distinguished and defined, and that the appropriate terms be employed consistently throughout the NPRM in a manner consistent with CIRCIA.

[13] 6 U.S.C. § 650(12); *see* NPRM at n.135 (explaining that CIRCIA's reference to 6 U.S.C. § 659 should be construed as Section 2200 of the Homeland Security Act, 6 U.S.C. § 650(12) due to subsequent changes in law). In defining Cyber Incident, Congress has struck the requirement that an Incident "imminently . . . jeopardize" information on information systems, or information systems. 6 U.S.C. § 681(5)(B).

[14] 6 U.S.C. § 681(3).

[15] *See* NPRM at 23,668 (describing examples of Incidents that likely would not qualify as Substantial Cyber Incidents as including "The compromise of a single user's credential, such as through a phishing attempt, where compensating controls (such as enforced multifactor authentication) are in place to preclude use of those credentials to gain unauthorized access to a covered entity's systems."); *see also* n.20, *infra*.

Interpreting the application of CIRCIA and the proposed rule to an inadvertent disclosure in the manner suggested in these Comments also appears consistent with the "good faith" exception to Substantial Cyber Incident set forth in the NPRM. *See* 6 C.F.R. § 226.1 (definition of "substantial cyber incident" does not include "Any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system").

event fall within the enumerated elements set forth at 6 U.S.C. § 681b(c)(2).[16] An inadvertent disclosure of confidential information also does not generally appear to implicate the core purposes of CIRCIA and the CIRCIA Regulation as described in the NPRM.[17]

Relatedly, any final rule should clarify that an information technology ("IT") operational event (like a bug in source code or a hardware system failure) would not be an Incident within the statutory meaning of the term unless such a bug or failure was perpetrated "without lawful authority."[18] Thus, where an IT operational event results from lawful activity (for example, contracting with a third party or internally-designed software), such events would not qualify as

---

[16] Requiring that the implementing regulations set forth:

> [a] clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall –
> (A) at a minimum, require the occurrence of--
> (i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;
> (ii) a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability, against
> (I) an information system or network; or
> (II) an operational technology system or process; or
> (iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;
> (B) consider--
> (i) the sophistication or novelty of the tactics used to perpetrate such a cyber incident, as well as the type, volume, and sensitivity of the data at issue;
> (ii) the number of individuals directly or indirectly affected or potentially affected by such a cyber incident; and
> (iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and
> (C) exclude--
> (i) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; and
> (ii) the threat of disruption as extortion, as described in section 681(14)(A) of this title.

6 U.S.C. § 681b(c)(2).

[17] NPRM at 23,651-2.

[18] A bug or hardware system failure also does not appear to generally implicate the core purposes of CIRCIA and the CIRCIA Regulation. *See* n.17, *supra*.

an Incident. Further, the IRC agrees that the NPRM correctly avoids setting a default reporting requirement when the cause of an IT operational event is uncertain. The NPRM appropriately holds fast to the statutory requirement that there be a "reasonable belief" that an event occurred without lawful authority before a reporting obligation is triggered.[19]

VI. Any Final Rule in this Proceeding Should Confirm that Events that Have a De Minimis Impact on an Information System are Not Substantial Cyber Incidents.

Any final rule in this proceeding should also confirm that, in the general run of cases where there is only a *de minimis* disruption to information systems that have no impact on reliable grid operations, there would be no reportable Substantial Cyber Incident under CIRCIA and the proposed rule. This general proposition appears consistent with the NPRM's discussion of incidents that likely would not qualify as Substantial Cyber Incidents, and the specific examples provided like: "[a] denial-of-service attack or other incident that only results in a brief period of unavailability of a covered entity's public-facing website that does not provide critical functions or services to customers or the public" and "[c]yber incidents that result in minor disruptions, such as short-term unavailability of a business system or a temporary need to reroute network traffic."[20]

* * *

The IRC respectfully requests that CISA consider these comments in developing any final rule in this docket.

---

[19] NPRM at 23,665 ("[A]n incident whose cause is undetermined, but for which the covered entity has a reasonable belief that the incident may have been perpetrated without lawful authority, must be reported if the incident otherwise meets the reporting criteria. If, however, the covered entity knows with certainty the cause of the incident, then the covered entity only needs to report the incident if the incident was perpetrated without lawful authority.").

[20] NPRM at 23,668.

Respectfully submitted,

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

/s/ Mark J. Stanisz
Craig Glazer
Vice President-Federal Government Policy
Mark J. Stanisz
Associate General Counsel
PJM Interconnection, L.L.C.
2750 Monroe Blvd.
Audubon, PA 19403
mark.stanisz@pjm.com

/s/ Andrew Ulmer
Roger E. Collanton
General Counsel
Andrew Ulmer
Assistant General Counsel
California Independent System Operator Corporation
250 Outcropping Way
Folsom, CA 95630
aulmer@caiso.com

/s/ Raymond Stalter
Robert E. Fernandez
Executive Vice President and General Counsel
Raymond Stalter
Director of Regulatory Affairs
New York Independent System Operator, Inc.
10 Krey Boulevard
Rensselaer, NY 12144
rstalter@nyiso.com

/s/ Eric Miller
Vice President and Chief Information Security Officer
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, IN 46032
EMiller@misoenergy.org

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

/s/ Chad V. Seely
Chad V. Seely
Senior Vice President & General Counsel
Nathan Bigbee
Deputy General Counsel
Doug Fohn
Assistant General Counsel
Electric Reliability Council of Texas, Inc.
8000 Metropolis Drive, Bldg. E, Suite 100
Austin, Texas 78744
chad.seely@ercot.com

Dated: July 3, 2024