U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Developing a Framework)
To Improve) **Docket No. 130208119-3119-01**
Critical Infrastructure Cybersecurity)

RESPONSE OF THE ISO/RTO COUNCIL TO NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S OCTOBER 29, 2013 REQUEST FOR COMMENTS

The ISO/RTO Council ("IRC") submits these comments in response to the National Institute of Standards and Technology's ("NIST") October 29, 2013, Request for Comments on the preliminary version of its voluntary Cybersecurity Framework (hereinafter, the "Framework"). The IRC is composed of nine Independent System Operators ("ISOs") and Regional Transmission Organizations ("RTOs") in North America.[1] The following U.S. ISOs and RTOs are providing these comments: the California Independent System Operator ("CAISO"), Electric Reliability Council of Texas ("ERCOT"), 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 ("SPP") (collectively, the "ISOs/RTOs"). These comments address the Framework and its overarching objectives and approach as a whole.

The IRC appreciates the continued opportunity to participate in NIST's work to improve critical infrastructure cybersecurity and applauds the efforts that led to the

[1] The ISOs/RTOs include: Alberta Electric System Operator ("AESO"), the California Independent System Operator ("CAISO"), Electric Reliability Council of Texas ("ERCOT"), the Independent Electric 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 ("SPP"). AESO and IESO are not participating in these comments.

creation of the Framework. We believe that the Framework provides a good foundation for structuring an effective and holistic cybersecurity program.

The IRC observed in its February 26, 2013 "*Response to NIST's Initial Request for Information*" that each ISO/RTO has a risk management program that includes a comprehensive program for addressing cybersecurity risks that draws from both the mandatory and enforceable NERC CIP reliability standards[2] and other industry standards and guidelines. Importantly, each ISO/RTO organizes its program differently based on its specific structure, operating characteristics, responsibilities, and risk assessments. As is noted in Section 1.2 of the Framework, "organizations vary widely in their business models, resources, risk tolerance, approaches to risk management, and effects on security, national economic security, and national public health or safety." For this reason, each organization must employ "a comprehensive risk management approach [that] provides the ability to identify, assess, respond to, and monitor cybersecurity-related risks and provide organizations with the information to make ongoing risk-based decisions." The IRC fully supports this manner of risk-driven cybersecurity. A risk-based methodology—such as Identify, Protect, Detect, Respond, and Recover—provides the best means for organizations to appropriately deploy resources for cybersecurity purposes.

The IRC believes that the Framework's use of the "Identity, Protect, Detect, Respond, and Recover" approach is consistent with and complementary to the best-practices and mandatory standards adopted by the ISOs/RTOs and electricity subsector. This approach is consistent with the increasing emphasis placed by the

[2] The NERC CIP standards include requirements regarding the physical security of critical cyber assets and senior management's roles and responsibilities with regard to cyber security practices.

Federal Energy Regulatory Commission ("FERC") and North American Energy Reliability Corporation ("NERC") on developing cybersecurity programs that identify, manage, and mitigate entity-specific risks.

As is noted in the prior IRC comments on the Framework, the electricity subsector oversees significant critical infrastructure and, for that reason, has been at the forefront of addressing cybersecurity for years. ISOs/RTOs have a long history of developing and complying with reliability standards, including cybersecurity requirements. Given the collective experience of both ISOs/RTOs and the electricity subsector as a whole, the IRC previously encouraged NIST to establish an overarching framework that recognizes, accommodates and complements the extensive cybersecurity standards in use within this and other industry sectors. The IRC believes that the Framework has effectively recognized and responded to that concern by acknowledging that, while the Framework may represent a starting point for some in developing a cybersecurity program, for other industries it will complement, "and does not replace, an organization's existing business or cybersecurity risk management process and cybersecurity program."

To that end, as NIST moves toward finalizing the Framework, the IRC urges that the Framework maintain its current, flexible approach that can be further developed and enhanced, as appropriate, on an entity or sector level. The IRC, for instance, has successfully collaborated with the Department of Energy, its Sector Specific Agency, on initiatives like developing best practices for securing smart grid technologies, participating in federally-funded research projects to develop advanced cybersecurity technologies for the energy sector, and conducting training exercises for advanced techniques in computer network defense. These projects represent a successful sector-specific approach to cybersecurity that NIST should encourage. The Framework, as presently drafted, avoids prescriptive, one-size-fits-all “solutions” to cybersecurity challenges. In this way, the Framework will permit and encourage risk-driven, industry-appropriate cybersecurity that will best enable the efficient use of cybersecurity resources. The IRC urges NIST to maintain this approach as the Framework is finalized, implemented, and reviewed for later updates.

In sum, the IRC believes that the Preliminary Framework provides a strong approach for effective cybersecurity, and—for the electricity subsector—an additional opportunity to, in the Framework’s own words, “use its current processes and leverage the Framework to identify opportunities to improve [ISO/RTO] management of cybersecurity.” The IRC looks forward to additional opportunities to support the development and enactment of the Framework.

Respectfully submitted,

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

/s/ Carl F. Patka
Carl F. Patka
Assistant General Counsel
Christopher Sharp
Compliance Attorney
Raymond Stalter
Director of Regulatory Affairs
New York Independent System
Operator, Inc.
10 Krey Blvd.
Rensselaer, New York
csharp@nyiso.com

/s/ Matthew Morais
Matthew Morais
Assistant General Counsel
Electric Reliability Council of
Texas, Inc.
2705 West Lake Drive
Taylor, Texas 76574
mmorais@ercot.com

/s/ Theodore J. Paradise
Theodore J. Paradise
Assistant General Counsel, Operations
And Planning
John Galloway
Manager, Cybersecurity
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
tparadise@ise-ne.com

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

/s/ Paul Suskie
Paul Suskie
Senior Vice President, Regulatory Policy
and General Counsel
Southwest Power Pool
201 Worthen Drive
Little Rock, Arkansas 72223-4936
(501) 688-2535
psuskie@spp.org

/s/ Stephen G. Kozey
Stephen G. Kozey
Vice President, General Counsel, and
Secretary
Midcontinent Independent
System Operator, Inc.
P.O. Box 4202
Carmel, Indiana 46082-4202
skozey@midwestiso.org