NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Andy Sharp
Interim Chief Financial Officer and Controller

Date: July 11, 2019

RE: Management Response to 2020 Budget Draft 1 Comments

The deadline for comments on the first draft of NERC's 2020 Business Plan and Budget (BP&B) ended on June 28, 2019. Comments were submitted by six entities and covered a range of topics. Below is a summary of those comments and NERC management's responses as applicable.

Bonneville Power Administration (BPA)
BPA expressed support for the investment and the importance of the Electricity Information Sharing and Analysis Center (E-ISAC) and the Cybersecurity Risk Information Sharing Program (CRISP), and applauded NERC and the industry on the Standards Efficiency Review (SER) project. BPA indicated the need for a better understanding of the E-ISAC and CRISP programs and a higher degree of transparency on the tangible benefits to the industry, as well as assurance that as resources are transferred from other programs to the E-ISAC, that those programs will still be viable to the industry.

NERC Management Response
Under the oversight of the Electricity Subsector Coordination Council's Member Executive Committee, NERC is making ongoing investments into additional resources, including personnel and technology, in support of the *E-ISAC Long-Term Strategic Plan*, while at the same time stabilizing costs in other NERC programs through ongoing effectiveness efforts and efficiency increases. However, NERC remains committed to investing in all NERC programs in support of the strategic focus areas outlined in the broader *ERO Enterprise Long-Term Strategy*.

The benefits for industry that result from investment in the E-ISAC long-term strategy are detailed in the NERC 2020 BP&B, Section A, in the "Stakeholder Engagement and Benefit" portion of the E-ISAC section. These benefits include, but are not limited to, enhancements to the following:

- **E-ISAC Portal, Communications, and Critical Broadcast Program (CBP)** – The E-ISAC Portal includes a user-community capability that allows members with similar security concerns to collaborate directly on a secure platform. In addition to Portal communications, the E-ISAC issues bulletins, develops periodic reports, and holds monthly and dynamic briefings. The E-ISAC also developed the CBP to deliver information rapidly to stakeholders about emerging security threats based on the best analysis available at the time, with follow-on updates as more details emerge.
- **Watch Operations** – Watch Operations is the principal entry and egress point for information sharing between the E-ISAC and its members and partners. Information flows into the organization via E-ISAC Portal postings, emails, phone calls, and other means and receives initial analysis by Watch Officers to determine (1) the severity of the event, (2) if it is part of an ongoing series of

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

related events, and (3) whether it rises to the level that requires a "deeper dive" by cyber and physical security subject matter experts. As part of the long-term strategy, the E-ISAC is transitioning to 24/7 watch operations in support of increased information sharing and analysis objectives. Watch Operations staff and physical and cyber analysts will rotate through an after-hours, on-call schedule on a weekly basis. If escalation is required, a physical and/or cyber analyst will be involved, with further management escalation as needed.

- **Analysis** – As mentioned above, the E-ISAC publishes reports, bulletins, and advisories; conducts webinars; and convenes experts for classified and unclassified briefings for its members. The most valuable content in those activities comes from analysis by E-ISAC cyber security, physical security, and threat intelligence teams. The E-ISAC long-term strategy has guided investments in hiring and training skilled security analysts, identifying and leveraging additional technology, enhancing relationships with government analysis sources, and developing strategic vendor relationships.
- **GridEx and GridSecCon** – The E-ISAC's biennial GridEx is designed to (1) exercise the electricity industry's crisis response to simulated coordinated cyber and physical security threats and incidents, (2) strengthen crisis response functions, and (3) provide input for lessons learned. GridSecCon is the E-ISAC's annual conference that brings together hundreds of subject matter experts on cyber, physical, and operations technology threats and solutions, with training sessions and classified and official use only briefs on topics vital to grid security.
- **CRISP** – CRISP is a unique private-public initiative among the E-ISAC, North American electric utility industry, the U.S. Department of Energy, and the U.S. Intelligence Community. Using passive information sharing devices on CRISP participant networks outside boundary firewalls, participant data is matched against identified threat signatures to examine potential threats and provide participants with recommended mitigation steps. Aggregated indicators of compromise and other relevant security information is shared with all asset owners and operators (AOOs) that are registered with the E-ISAC, regardless of participation in CRISP, through E-ISAC Portal postings.
- **Cyber Automated Information Sharing System (CAISS)** – The E-ISAC has also broadened automated information sharing capabilities beyond CRISP. In 2017 and early 2018, the E-ISAC and several industry partners piloted CAISS. The pilot evaluated technological solutions for bi-directional communication, workflow between participants, the handling and vetting of shared information, and lessons learned from the technology and processes overall. CAISS became operational in 2019 and is available for voluntary participation by industry AOOs.

Additional information is also provided below in response to comments from the Canadian Electricity Association (CEA) and the Independent Electricity System Operator (IESO).

CEA and IESO

CEA and IESO, both Canadian entities, provided similar comments, commending NERC's budget stabilization efforts outside of the E-ISAC through ongoing cost-effectiveness and efficiency increases. However, both organizations expressed concern with the magnitude of E-ISAC budget increases and the corresponding value for stakeholders, including Canadians, urging NERC to continue to seek opportunities to leverage capabilities already available from other agencies and partners.

NERC Management Response

NERC recognizes that Canadian entities have important and experienced industry and governmental resources focused on cyber security. The E-ISAC is an important supplemental resource offering the following unique and complementary attributes:

- **Broad View** – The E-ISAC is positioned to take a broad view of the threat landscape across all of North America. E-ISAC membership includes utilities with interests in Canada, Mexico, and the United States (including Alaska, Hawaii, and its territories) and covers a range of organizations from municipal and cooperative entities to investor-owned entities, including generation, transmission, and distribution functions.
- **Electricity Industry Focus** – The E-ISAC is focused on threats to the electricity industry, and provides industry-specific guidance. At the same time, it maintains relationships with other ISACs that address security issues impacting critical interdependent sectors.
- **Access to the Intelligence Community** – Due to the E-ISAC's partnerships with various government entities, the E-ISAC also has access to the U.S. Intelligence Community and its data and resources. The E-ISAC can use information below the tear line from the Intelligence Community and share it with members subject to the requirements of established information sharing protocols.
- **Member Community** – Because the E-ISAC is focused on the electricity industry, it has a well-defined community of members and offers a range of opportunities for members to interact with each other. Some opportunities include monthly briefings, unclassified threat workshops, and large security training and exercise events like GridSecCon and GridEx. The E-ISAC also maintains close working relationships with Canadian entities, as well as with Natural Resources Canada, Public Safety Canada, the Canadian Centre for Cyber Security, the Canadian Communications Security Establishment, and the Royal Canadian Mounted Police.
- **Physical Security** –The E-ISAC is also a growing source for aggregated physical security information. The E-ISAC works closely with both U.S. and Canadian member organizations and governments to regularly review physical security threat information to track and identify threats.
- **Partnership Outreach** – The E-ISAC has focused on enhancing its partnerships with Canadian industry members and finding collaboration opportunities. The E-ISAC has committed to visiting companies across the provinces. So far, E-ISAC staff members have visited IESO, New Brunswick Power, BC Hydro, Hydro Quebec, and Manitoba Hydro, and are confirming additional meetings over the coming months. The feedback has been positive, the relationships stronger and, most importantly, the E-ISAC is seeing increases in membership, information sharing, and collaboration. In late 2018 through 2019, the E-ISAC had 25 new Canadian AOO user accounts.

In addition, over the past few months, the E-ISAC and IESO have been working in good faith to gain additional insights on their respective capabilities, including the IESO's new and unique role in cyber information sharing and analysis within the Ontario province. These discussions have also focused on the mutual benefits of entering into pilot collaboration agreement, which builds on the strengths of both organizations and improves the overall efficiency and effectiveness in the execution of their common objective of assisting industry with cyber security awareness and reducing cyber security risks.

Edison Electric Institute (EEI)
EEI expressed support for NERC's investment in the E-ISAC. EEI also encouraged NERC to continue enterprise-wide effectiveness and efficiency efforts, and to clearly identify those savings to stakeholders, particularly with respect to meetings and travel expenses in light of efforts to improve productivity and effectiveness of stakeholder engagement activities. Additionally, EEI requested that NERC provide clarity on the drivers for its salary increase, and continue to look for opportunities to reduce medical expenses.

NERC Management Response
As part of the *ERO Enterprise Long-Term Strategy*, NERC is committed to effectiveness and efficiency efforts and reflecting identified cost savings as part of the BP&B process. Meeting and travel expenses are increasing slightly in 2020 mainly due to E-ISAC personnel increases, engagement efforts, and enhanced conference call capabilities. Potential savings from the NERC stakeholder committee restructure will be analyzed and determined once there is more certainty on the outcome of the committee and meeting structures going forward.

Also as part of the ERO Enterprise long-term strategy, NERC is committed to building and maintaining top talent with the required specialized expertise necessary to fulfill the ERO Enterprise's mission-critical roles. Executive and staff compensation and benefits are determined based on guidelines established by the Board of Trustees (Board) Corporate Governance and Human Resources Committee and the results of market compensation and benefit studies. The 2020 budget for base salaries assumes a 3.0% increase over actual 2019 base salaries for merit adjustments and, as requested by the Board, up to 0.5% for equity and market adjustments.

NERC benchmarks benefit costs with industry and similar organizations and works actively with an independent broker to keep costs reasonable to stay competitive for talent acquisition and retention, and increases to medical insurance plan costs were below market for several years. NERC's medical benefits plans have not changed for 2020; however, the past two years have shown higher increases due to recent loss experience and fewer medical insurance provider options in the state of Georgia. NERC continues to negotiate these premiums and will have final amounts for 2020 at the end of 2019.

ISO RTO Council Standards Review Committee (SRC)
The ISO RTO Council SRC expressed the following:

- Following the results of the SER, NERC should make adjustments in the Reliability Standards and compliance program areas to include reduced compliance requirements reflected in NERC's processes;
- Ensure the E-ISAC is able to provide the most relevant and timely actions in response to bulk power system threats and vulnerabilities;
- Following the implementation of the Compliance Monitoring and Enforcement Program (CMEP) tool, Align, and the Centralized Organization Registration ERO System (CORES), NERC should identify and reflect resulting savings in future budget years; and

- NERC committee structure changes in development by the Stakeholder Engagement Team could result in reduced meeting and travel expense projections for future budget years.

NERC Management Response
NERC generally agrees with the statements above, as they are aligned with the goals or potential outcomes of the SER project, the *E-ISAC Long-Term Strategy*, Align and CORES tools, and the effectiveness and efficiency efforts related to stakeholder engagement. With regard to financial savings following the implementation of Align and CORES, savings for application costs (i.e., software licenses, maintenance, and support) will be realized in future Regional Entity budgets as they transition from their legacy CMEP systems to the centralized tools.

National Rural Electric Cooperative Association (NRECA)
NRECA expressed general support for the first draft of NERC's 2020 BP&B and encouraged NERC to continue with its efficiency and effectiveness activities to undertake further cost saving under this 2020 budget and future budget years as well. NRECA noted that this effort should not only be a short-term focus, but should be a long-term focus for NERC.

NERC Management Response
NERC agrees with NRECA and notes that its effectiveness and efficiency efforts are part of the E*RO Enterprise Long-Term Strategy*.

We appreciate the comments received and encourage your continued participation in the BP&B process.

Sincerely,

Andy Sharp

Andy Sharp
Interim Chief Financial Officer and Controller