

April 17, 2019

Simon Slobodnik
Officer of Electrical Reliability
Federal Energy Regulatory Commission

And

Kevin Ryan
Office of the General Counsel
Federal Energy Regulatory Commission

Ref: “Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security” Document No. 2020-20987, Docket No. RM20-19-000.

Dear Mr. Slobodnik and Mr. Ryan,

The TIC Council Americas is pleased to provide comment on “Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security,” document number 2020-20987, Docket No. RM20-19-000. The TIC Council supports all efforts to address cybersecurity in connected infrastructure, systems, components and devices and looks forward to our ongoing engagement and discussion on this topic.

The use of equipment produced or provided by certain entities identified as risks to national security can introduce cybersecurity risks to safety and security and thoughtful action and safeguards are needed to protect against cyberattack vulnerability.

We believe that a transparent and comprehensive regulatory framework for certification on cybersecurity that makes use of the IEC 62443 series of standards would be beneficial for industry and authorities alike.

Using a combination of cybersecurity standards, evaluation, and certification will improve systems security and risk management, through metrics, measurements, and benchmarks that support acquisition requirements for entities identified as risks to national security. The U.S. EPA Energy Star program is an example of a voluntary public-private partnership that relies on independent third-party certification to help ensure ongoing compliance and the integrity of the Energy Star label. A similar program for cybersecurity of bulk electrical systems and components would benefit the energy industry and ensure compliance with the established framework.

Conformity assessment is a reasonable and responsible model for addressing the challenges of acquisition and cybersecurity and improving cybersecurity posture throughout the product lifecycle. And trusted, independent third-party conformity assessment is a cost-effective policy solution as it provides the highest level of confidence and helps government leverage private-sector resources.

The emerging standards landscape as well as the increasing number of cybersecurity incidents are good indications that such a framework is critically needed to defend the U.S. bulk electric system.

TIC Council is the global trade federation representing the independent third-party Testing, Inspection and Certification (TIC) industry which brings together more than 90-member companies and organizations from around the world to speak with one voice. Its members

provide services across a wide range of sectors: consumer products, medical devices, petroleum, mining and metals, food, and agriculture among others. Through provision of these services, TIC Council members assure that not only regulatory requirements are met, but also that reliability, economic value, and sustainability are enhanced. TIC Council's members are present in more than 160 countries and employ more than 300,000 people across the globe.

We appreciate the opportunity to give feedback on "Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security" document number 2020-20987. Should you have any questions, please don't hesitate to contact Karin Athanas at +1 240 762 8069 / kathanas@tic-council.org.

Sincerely,



Hanane Taidi
Director General
TIC Council



Karin Athanas
Executive Director
TIC Council Americas
kathanas@tic-council.org