National Standard of Canada
Standards Proposal

Proposed Standard Title:
Consolidated cybersecurity standard covering Industrial Internet of Things (IIoT) devices and systems

Proposed Scope:
The proposed standard aims to specify minimum requirements for the design and operation of Industrial Internet of Things (IIoT) devices and systems to meet requirements for security, safety, confidentiality, integrity, and availability. The proposed standard is intended to provide a consolidated overview of key security features and practices to meet industry recommended standards and best practices. Where applicable, each requirement will reference industry, regulatory, or best practice standards.

Strategic Need:

Identify the strategic need of key stakeholders and confirmation expressing the need.

This includes consideration for:

a. *The strategic need of key stakeholder (e.g. legislator, industry, government, consumers);*
b. *The type of standard (international, regional, domestic standards and harmonization need);*
c. *Addressing up-to-date vs outdated standard to ensure latest innovative/technology/safety features available for businesses;*
d. *If the standard is intended to support national/regional/international certification programs;*
e. *If there is stakeholder intention to transition to different standard;*
f. *The type of maintenance (periodic, continuous, stabilized, best before date); and*
g. *The use of "CAN" descriptor.*

Cyber security is integral to safeguarding Canada's citizens, information, economy and infrastructure. The need has never been greater as threats evolve and threaten to disrupt our daily lives.

In 2018, there were already more things (8.6B) connected to the Internet than people (5.7B). The number of installed IoT devices is forecast to exceed 22B by 2025. Looking forward, the number of connected devices could reach 200B when 5G is fully deployed

Similarly, the number of Industrial Internet of Things Devices (IIoT) devices installed in industrial and settings is rapidly increasing. IIoT consists of Internet-connected machinery, infrastructure and advanced smart devices that collect, exchange and analyze data to enhance manufacturing, industrial processes and operational efficiencies. They are deployed to improve connectivity, efficiency, scalability as well as time and cost savings for organizations throughout the grid. Grid participants are integrating field devices in enterprise-wide information systems, adding historians, configuration management, event retrieval and remote access.

Many factors are contributing to the increased deployment of IIoT devices, including lower costs of IIoT devices, data transmission and storage; the drive for digitization, secondary uses of data and data

monetarization. The same trends have been observed on electricity generation, distribution, and transmission systems in addition to the need for increased two-way communication between devices as a result of a more distributed and complex grid.

Significant new spend on IIoT devices coupled with a lack of global cybersecurity standards are creating new challenges across systems. IIoT devices can be hacked which can cause major disruptions to operations. The risk for intrusion is higher when devices use the Internet when compared to Supervisory Control and Data Acquisition (SCADA) systems. The Ukraine-Kiev Crash Overide (aka Industroyer) – Malware demonstrated the weakness of IIoT devices and protocols. The number of advisories from the US National Cybersecurity and Communications Integration Center (NCCIC) regarding cyber threats or weaknesses of IIoT devices has been steadily increasing.

New standards and conformity assessment programmes to certify IIoT integrated in systems as cybersafe are urgently needed. Although standards such as ISA/IEC 62443 provide much needed guidance, there are no accepted cybersecurity standards providing detailed performance requirements for the conformance of IIoT devices and their components per se. New global conformance programs for devices supply chains are being launched through organizations such as the Global Cybersecurity Alliance. New standardized approaches to assess the conformance of installed systems using IIoT devices are also being implemented but need to be assessed against Canadian requirements.

Regarding the specific needs of grid operators, the user case may include such as use (e.g. transmission, distribution), function (e.g. relay, feeder, gateway, etc.), communication (e.g. DNP3, cellular, Wi-Fi), deployment context (e.g. substation, power line, control center, cloud), vendors, and existing governing standards (e.g. NERC CIP, IEC 62443), etc.

Developing a consolidated standard requires an understanding of security and threat landscape IIoT devices face, cybersecurity risks driven by these threats, cybersecurity standards applicable to these devices, and the various vendors and their claims of cybersecurity and compliance. Securing IIoT devices individually and connecting them in complex systems will also require a broad consideration about the operation, availability, and safety needs of a distributed integrated network of individual vendor specific and Commercial Off the Shelf (COTS) components.

Need for Availability in Both of Canada's Official Languages: *Do stakeholders need the standard published in both official languages?* *Do users of the standard need the standard published in both official languages?* *Do authorities having jurisdiction need the standard published in both official languages?* *Are there health and safety related needs for the standard to be published in both official languages?* *For adoptions, is there availability of the regional/international standard or other deliverable from the source?* *For adoptions, is there an agreement with the source committee to facilitate official translation?*	YES

Geographical Representation Considerations:

Identify the Canadian geographical representation appropriate to the subject area covered by the standard.

Geographic representation may consider factors such as:

a. *Industry (e.g. petroleum in petroleum producing provinces);*
b. *Reference in regulation (if a regulation exists in a province); or*
c. *Commodity characteristics and social impact (e.g. heating oil for northern climates).*

Industrial sectors of the economy. Critical infrastructure.

Trade:

Identify how the standard meets the needs of the marketplace and contributes to advancing trade in the broadest possible geographical and economic contexts.

For example:

a. *Facilitate Canadian innovation to lead internationally;*
b. *Support the objectives of "One standard, one test, accepted everywhere";*
c. *Support the objectives of "First to Market"; or*
d. *Foster international/ regional/ national alignment of requirements.*

Consumers, businesses across all sectors of the economy and governments have a vested interest in cyber secure IIoT devices. New standards and certification programmes will significantly reduce the risk/severity of cyber attacks through IIoT devices. Through the user case, cybersecure IIoT devices will result in a more reliable grid North American electricity grid.

Canadian organizations will play a leadership role in setting appropriate IIoT cybersecurity standards meeting Canadian requirements in close collaboration with reliable and trusted partners.
By participating in the standards development process, Canadian digital industry players, such as device manufacturers, software developers and testing bodies will be well positioned to become first to market in the commercialization of new cyber safe IIoT products and platforms.

Once developed, the voluntary standard can be adopted by governments and industry through various means. Federal, state and provincial governments routinely adopt thousands of voluntary standards by reference in regulations. Standards are also systematically incorporated by governments and industry as mandatory requirements in procurement documents and supply chain contracts. This will ensure broad compliance to the consolidated standard.

The proposed standard is intended to provide a consolidated overview of key security features and practices to meet industry recommended standards and best practices. Where applicable, each requirement will reference industry, regulatory, or best practice standards from across the globe to foster international, regional and national alignment of requirements.

Relevant existing documents at the international, regional and national level:
NIST Cybersecurity Framework, Framework for Improving Critical Infrastructure Cybersecurity, April 2018 NIST Special Publication, NIST SP 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, May 2013 NIST Special Publication, NIST SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security, May 2015 NIST Special Publication, NIST SP 800-154, DRAFT Guide to Data-Centric System Threat Modeling, March 2016 NIST Special Publication, NIST SP 800-16 Rev. 1, A Role-Based Model for Federal Information Technology / Cyber Security Training, March 2014 NIST Special Publication, NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010 NIST Special Publication, SP 800-52 Rev. 2, DRAFT Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, November 2017 NIST Special Publication, NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization, December 2014 NISTIR 7298r2 Glossary of Key Information Security Terms, May 2013 Federal Information Processing Standards (FIPS), FIPS 140-2, FIPS 140-3 NIST Technical Report, NISTIR 7946, CVSS Implementation Guidance, April 2014 Federal Information Processing Standards (FIPS), FIPS 180-4, Secure Hash Standard, August 2015 Federal Information Processing Standards (FIPS), FIPS 186-4, Digital Signature Standard, July 2013 Federal Information Processing Standards (FIPS), FIPS 140-2, Security Requirements for Cryptographic modules, May 2001 Security Profile for Distribution Management Version 1.0, ASAP-SG February 2012 U.S. Department of Homeland Security. (April 2011). Catalog of Control Systems Security: Recommendations for Standards Developers. Institute of Electrical and Electronics Engineers, Inc. (2003). IEEE STD 1613-2003, Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations, New York, New York.

International Electrotechnical Commission. (2002, January). IEC 61850-3 Communication Networks and Systems in Substations - Part 3: General Requirements

International Electrotechnical Commission, IEC 62351 - Information Security for Power System Control Operations

IEEE C37.231-2006 Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control

DoD Directive 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

NEMA SG-AMI 1 Requirements for Smart Meter Upgradeability Implementing Secure Remote Firmware Updates May 2011 Embedded System Conference Silicon Valley ESC-202

OWASP Internet of Things Project, May 2018

UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, July 2017