SGIP 2.0, Inc.
401 Edgewater Place, Suite 600,
Wakefield, MA 01880
sgip.org

SGIP's Response to Request for Comment
Department of Commerce, National Telecommunications and Information Administration
Docket No. 170105023-7023-01
RIN 0660-XC033

The Benefits, Challenges, and Potential Roles for Government in Fostering the Advancement of the Internet of Things

I. Introduction

SGIP ("Smart Grid Interoperability Panel") appreciates the opportunity to provide comments to the U.S. Department of Commerce ("Commerce") and specifically the National Telecommunications and Information Administration ("NTIA") in response to its request for comments on the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things ("IoT").

SGIP is an industry consortium representing a cross-section of the energy ecosystem focusing on accelerating grid modernization and the energy Internet of Things through policy, education, and promotion of interoperability and standards to empower customers and enable a sustainable energy future. Our members are utilities, vendors, investment institutions, industry associations, regulators, government entities, national labs, services providers, and universities. A nonprofit organization, we drive change through a consensus process.

The approach, processes, and roles of government outlined represent a consistent and balanced approach to building a national IoT vision and sustainable strategic framework to unlock the value that IoT promises. The comments contained herein are intended to shed additional light on high priority areas and help identify potential high-impact activities for Commerce.

The focus of our comments addresses the following two questions:

a. Are there specific tasks that the Department should engage in that are not covered by the approach?
b. What should the next steps be for the Department in fostering the advancement of IoT?

II. General Comments

SGIP was created in 2009 by Commerce to assist NIST in executing its responsibilities as defined within the "Energy Independence and Security Act of 2007, Title XIII"[1]. SGIP has worked closely with NIST and other federal agencies (e.g. Department of Energy (DOE), Department of Defense (DOD)) to identify and address smart grid interoperability and security gaps through industry-wide, open stakeholder collaboration. IoT, within the energy domain, is a primary and integral focus area of this collaboration. SGIP's collaborative model has been very effective and it is recommended that it be extended to include IoT within other domains. Under this model, Commerce would identify a minimal but sufficient set of collaborative domain-specific organizations, like SGIP, that cover the broader IoT landscape. This would enable Commerce to better understand common industry-wide technology, interoperability, and security issues and better position it to maintain multi-sector consistency and coherency.

Temporal phasing and coordination of initiatives and activities needs to be analyzed and understood to prevent premature policy and regulation that would impede growth. It is important to leverage and build upon existing related efforts associated with the Internet, especially concerning interoperability, security and privacy.

The "NIST Framework for Cyber Physical Systems"[2] is a foundational framework for IoT and should be leveraged as a basis for further specialization and refinement.

III. Performance

IoT represents a wave of expansion in wide-area Internet connectivity. The Internet has evolved, and is continuing to evolve, toward higher performance, lower latency data communications at scale. As performance limits are reached, one of the techniques commonly used is payload compression. This often results in non-critical information content, such as contextual metadata, to be reduced. Contextual information is reintroduced implicitly through human interactions and interpretation. Twitter feeds are a typical example of "real-time", compressed data that lacks contextual information so that it can be routed efficiently often leading to semantic misunderstanding. IoT however will require that device information flows contain sufficient metadata for unambiguous interpretation of data semantics in complex business contexts and to engage in more complex real-time negotiation sequences required for automated transactions. Automated transactions will be further amplified through the growth of blockchain-enabled transactive systems that leverage state-machine driven, executable contracts. In general, this will put significantly higher demands on network capacity, bandwidth and latency when compared with human-centric interactions.

[1] https://www.ferc.gov/industries/electric/indus-act/smart-grid/eisa.pdf
[2] https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

Role: Commerce, working with other federal and local agencies, should prioritize removing barriers to infrastructure expansion to make it easier for organizations to site towers, run fiber and acquire spectrum. Commerce should lead IPv6 conversion within the federal government to further identify and remedy roadblocks to commercial deployment.

Time-sensitive networking (TSN) will be critical for high-value IoT applications in energy, manufacturing, and transportation. These require a high degree of determinism and a common sense of high-precision time. TSN standards have been in development within IEEE (e.g. 802.1, 1588)[3] but these standards need to be accelerated and embedded within products for industry deployment.

Task: Commerce should work to prioritize and accelerate the TSN standards development process through industry partners and other agencies, and publish guidelines and best-practices for TSN deployments and system integration. This should include collaboration on system requirements for high priority domains.

IV. Interoperability

The importance of standards has been highlighted but needs to be emphasized. The growth in global connectivity is founded upon industry acceptance of a relatively small number of interlinked interoperability standards. It should be noted however that achieving interoperability is a process and it's common for multiple standards to compete for market share. Industry weed out is a normal phase in the evolution of standards.

Interoperability and security are understood within the context of architecture. Architecture provides the components and structures within which dynamic behaviors and interactions transpire. Common architectural understanding is a critical element for identifying industry-wide interoperability interfaces and the information flow through those interfaces.

As an example, SGIP is working toward convergence within the energy domain which intersects and overlaps with other domains such as industrial. Existing architectural frameworks include the "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0"[4], DOE Grid Modernization Laboratory Consortium (GMLC) Grid Architecture[5], CEN-

[3] http://www.ieee802.org/1/pages/tsn.html
[4] https://www.nist.gov/news-events/news/2014/10/nist-releases-final-version-smart-grid-framework-update-30
[5] https://energy.gov/under-secretary-science-and-energy/doe-grid-modernization-laboratory-consortium-gmlc-awards

CENELEC-ETSI Smart Grid Reference Architecture[6], and Industrial Internet Consortium's "Industrial Internet Reference Architecture"[7].

The broad diversity of IoT stakeholders further increases the complexity of understanding interoperability within the context of common architecture.

Role: Commerce should work closely with other federal agencies and industry partners to collaborate and converge on common conceptual and logical IoT reference architecture models that form the basis for interoperability within a domain and related domains.

Task: Commerce should publish an IoT Interoperability Framework through a consensus-based stakeholder process. The IoT framework should leverage existing industry frameworks, such as the "NIST Framework for Cyber Physical Systems", "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0", and DOE "GWAC Context Setting Interoperability Framework"[8].

The broad diversity of IoT stakeholders and devices requires a common framework for defining and communicating information meaning and structures through information modeling. Cross-industry collaboration on the development of common, neutral entities and concepts will increase reuse and minimize reinventing existing solutions. Some examples of international information models for energy-related IoT device interactions include; 1) IEC 61850[9] and the associated IoT protocols for exchanging the information contained within the model, such as IEC 61850-8-2 and IEC 62541, and 2) the IEC 61968/61970 Common Information Models (CIM) that support control center interactions.

Role: Commerce should promote cross-industry best practices and guidance for IoT semantic frameworks, leveraging existing domestic and international standards.

V. Criticality

As noted, the mission-criticality of IoT devices is rapidly increasing as the impact of system faults and failures result in greater negative impact. Large-scale complex IoT systems are fault-normal and can learn from and leverage fault-detection and recovery techniques that have been used extensively within industry.

As an example, the ubiquitous residential Internet is designed, installed and managed as an embedded communications infrastructure for delivering non-critical entertainment services.

[6] https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf
[7] https://www.iiconsortium.org/IIRA.htm
[8] http://www.gridwiseac.org/pdfs/interopframework_v1_1.pdf
[9] http://www.iec.ch/

Important IoT services are being built upon this infrastructure where network failures are considered a nuisance and time to repair is indeterminate.

IoT will require that many consumer-oriented services, such as Internet and cellular providers, learn from and leverage best practices and techniques from industries that have been providing high reliability solutions for mission-critical applications such as industrial and military control. Concepts such as fault analysis, fault tolerance and graceful degradation have been applied with success in industries where failure can cause human and financial loss. IoT will require that networks evolve forward with similar functional and operational characteristics and resilient system management.

Task: Commerce should participate in the development of consensus-based industry guidelines with general requirements for secure remote IoT support, including security patches that protect privacy. These guidelines would help inform the development and deployment of IoT devices and systems that would benefit many IoT commercial providers.

Task: Commerce should develop consensus-based industry guidelines with general requirements for robust resilient IoT product design and operation.

VI. Cybersecurity

Cybersecurity is critical for IoT. Developing and maintaining trust is a key component for IoT growth. The "NIST Guidelines for Smart Grid Cybersecurity"[10] is an example of domain-specific security guidelines that provide needed level-setting across the smart grid.

One of the high-priority challenges will be to leverage and adapt technologies that were developed within information technology such as public key infrastructure (PKI), to highly-distributed, cost-sensitive, embedded devices "in the wild".

Task: Commerce should collaborate with industry partners to publish consensus-based best practices and guidelines for IoT cybersecurity based upon existing security frameworks and international standards, such as the IEC 62351 series.

Task: Commerce should collaborate with industry partners to publish consensus-based best practices and guidelines for certificate management of embedded IoT devices and systems.

VII. Conclusion

[10] https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

SGIP appreciates the opportunity to provide these comments to assist Commerce and NTIA in considering the benefits, challenges, and potential roles for government in fostering the advancement of the Internet of Things. The Internet, cloud services, and data innovation will drive the U.S. and world economies for years to come. Just as the Department showed global leadership in early Internet policy, it should lead in the Internet of Things. SGIP stands ready to assist the Department in these and any other efforts to help accelerate the use of Internet of Things within the Power Sector.

Sincerely,

Sharon Allan
CEO & President