SIEMENS

October 8, 2014
Response to Request for Information
Experience with the Framework for Improving Critical Infrastructure Cybersecurity
Docket Number 140721609-4609-01

Thank you for this opportunity to respond to the above-referenced request for information (RFI). The Digital Factory Division of Siemens makes industrial control systems (ICS) – the computer systems that control and automate machines and infrastructure. ICS products are used in many physical assets that qualify as critical infrastructure.

As the RFI mentions, NIST published a *Roadmap for Improving Critical Infrastructure Cybersecurity* alongside the *Framework for Improving Critical Infrastructure Cybersecurity* in February 2014. The *Roadmap* "discusses NIST's next steps with the *Framework* and identifies key areas of development, alignment, and collaboration."[1] The RFI asks whether there have been "significant developments – in the United States or elsewhere – in any of these areas since the *Roadmap* was published that NIST should be aware of and take into account as it works to advance the usefulness of the *Framework*."[2]

Siemens would like to ensure that NIST and its partners in the *Framework* process are aware of an important effort that is relevant to both "Conformity Assessment" and "International Aspects, Impacts, and Alignment," two of the "areas for improvement" identified in the *Roadmap*.[3] Specifically, Siemens would like to make sure that U.S. stakeholders inside and outside of government appreciate the work that is now underway at the International Electrotechnical Commission (IEC) to incorporate cybersecurity into a globally recognized system for testing and certifying the safety and security of ICS products and other electrical components. That overall system, known as the IECEE CB Scheme, is explained briefly in the following excerpt from an IECEE Secretariat document:

> The IECEE CB Scheme is the world's first truly international system for mutual acceptance of test reports and certificates dealing with the safety of electrical and electronic components, equipment and products. It is a multilateral agreement among participating countries and certification organizations. A manufacturer utilizing a CB test certificate issued by one of the accepted National Certification Bodies (NCBs) can obtain certification marks of the latter, within their scope of adherence, in the countries where the accepted NCBs are located. . . . The main objective of the Scheme is to facilitate trade by promoting harmonization of the national standards with international standards and cooperation among accepted NCBs worldwide in order to bring product manufacturers a step closer to the ideal concept of "one product, one test, one mark, where applicable."[4]

Siemens greatly appreciates NIST's commitment to "help ensure that private and public sector conformity assessment needs are met by leveraging existing conformity assessment programs and other activities that produce evidence of conformity."[5] We also applaud NIST's recognition that "[d]iverse or

---

[1] *Roadmap* at 1 (http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf).
[2] 79 Fed. Reg. 50891, 50894 (Aug. 26, 2014).
[3] *See Roadmap* at 4-5 and 7-8.
[4] *About the CB Scheme* at 1 (http://www.iecee.org/cbscheme/pdf/cbfunct.pdf).
[5] *Roadmap* at 4 (emphasis added).

specialized requirements [as between different national jurisdictions] can impede interoperability, result in duplication, harm cybersecurity, and hinder innovation."[6] We respectfully suggest that NIST continue to act on those sound principles by encouraging private- and public-sector stakeholders in the U.S. to channel their interest in conformity assessment into participation in, and support for, the international IEC effort described above.

ICS products and services are sold globally, by global corporations. So the scope of the effort to improve and demonstrate the security of ICS products and services must also be global. Achieving the widespread adoption of high-quality conformity assessments for the security of ICS products and services depends, in no small part, on stakeholders around the world trusting that the assessment tools reflect only the agenda of improving security for all users. Vetting conformity assessment systems through the IECEE CB can be an effective means of imbuing those systems with global credibility and ensuring that they remain harmonized.

Siemens believes that the IECEE CB would be a worthy topic for discussion at NIST's upcoming stakeholder workshops, and Siemens would look forward to participating in those sessions. Thank you again for this opportunity to inform NIST's continuing work to improve the cybersecurity of critical infrastructure.

[6] *Id.* at 7.