Open Secure Energy Control Systems, LLC
8070 Georgia Avenue
Silver Spring, MD 20910

Contact: Dr. Stanley A. Klein
Email: stan@osecs.com
Phone: 301-565-4025

Comments to
Sub-Committee on Standards
under the National Science and Technology Council's Committee of Technology

We first present the perspective from which we are commenting and then provide specific comments addressing questions posed in the inquiry.

PERSPECTIVE

The first project for Open Secure Energy Control Systems, LLC (OSECS) was a Phase II Homeland Security Small Business Innovation Research (SBIR) project in which we developed an initial prototype open source toolkit for developing secure applications using IEC-61850. The toolkit provides IEC-61850 client functionality, facilitates integration with conventional open source security tools, and provides other security functions. One area in which we pioneered is the use of World Wide Web Consortium (W3C) web services communications to transmit IEC-61850 objects. Subsequently, we performed a DOE Phase I SBIR focused on extending our efforts to the wind power extension, IEC-61400-25. We contributed to the efforts on IEC-61400-25-4 Annex A, which is provides web services communications for wind power. (That capability has been suggested by ourselves and others as a solution to the “61850-Lite” identified as a discussion issue in the EPRI Report to NIST on the Smart Grid.) We subsequently prepared a report for the Electric Power Research Institute (EPRI) on lessons learned on those projects.

After conclusion of our SBIR efforts, we recognized that our commercialization efforts were intertwined with US acceptance of 61850 and 61400-25, and that the Smart Grid would positively impact that acceptance. Given the importance of the Smart Grid to our commercialization prospects, we became active in Smart Grid activities and have prioritized that over Toolkit improvement and release.

Dr. Stanley Klein, a Managing Principal of OSECS, represents OSECS in Smart Grid efforts and in numerous other standards activities. He is active in SGIP activities including the Cyber Security Working Group (CSWG) and several of its subgroups the Transmission and Distribution Domain Experts Working Group (T&D DEWG), Priority Action Plans PAP-11 (on Common Object Models for Electric Transportation), the Vehicle-to-Grid DEWG, PAP-14 (on T&D Model Mapping), and PAP-16 (on Wind Plant Communications). He is also a member of IEC TC 57 WG-15 on cybersecurity for the IEC standards, was a member of the IEC task group that prepared IEC-61400-25-4 Annex A, has participated in a number of IEEE standards efforts as a member of either a working group or a ballot pool, and is a member of the NERC Control System Security Working Group (that prepares relevant NERC guidelines).

COMMENTS

1. The Federal Government needs a proper definition of "open standard."

ARRA requires use of "open standards" for the Smart Grid. There is no official Federal definition of the term. There are a variety of definitions available in the literature. The relevant Wikipedia article cites definitions, relevant for US purposes, of ITU-T, IETF, Bruce Perens, Ken Krechmer, Microsoft, W3C, the Open Source Initiative, and the Digital Standards Organization. An edition of XML Cover Pages, published by OASIS, summarizes some additional relevant definitions including the Business Software Alliance, the Commonwealth of Massachusetts Information Technology Division, Consortiuminfo.org, the Open Geospatial Consortium, Sun Microsystems, and UN/CEFACT. Among the kinds of provisions in the various definitions are the following:

a. Development of the standard in an open process (such as a voluntary, consensus process defined in OMB Circular A-119). Note that a voluntary, consensus process is a common requirement, but that most definitions of "open standard" apply further requirements.

b. Public access to development process – Several definitions require that during the development process the drafts be posted for public comment and that the comments be considered.

c. Public availability – All definitions require at least reasonable and non-discriminatory pricing. Several require availability at no cost on stable web pages.

d. No Royalty – Some definitions allow incorporation of essential patents under "reasonable and nondiscriminatory (RAND) conditions," although that term is also undefined and has received negative comments from some definers of the term "open standards." Most definitions require royalty-free use of any essential patents. One definition notes that a fee may be charged for compliance testing.

e. No limitations on implementation – One definition states: "An 'open standard' must not prohibit conforming implementations in open source software." This leads to other requirements identified above and to the requirement that no license agreement, non-disclosure agreement, or any of a number of other forms of permission "should be needed to deploy conforming implementations of the standard." Many other definitions have similar requirements.

f. Avoidance of "vendor lock-in." Some definitions explicitly identify avoidance of vendor lock-in as a major goal of open standards and use it as a basis for requiring some of the more stringent of the above requirements (such as no cost for documents, royalty-free use, and no limitation on implementations). Related to this, some definitions require the avoidance of features that would favor a particular proprietary platform or other supporting technology.

What NIST used for the Smart Grid was the Federal definition of a voluntary consensus standard. That definition lacks many of the provisions of other definitions and is the least restrictive definition available.

One provision in the NIST definition of an open standard is the allowance of RAND conditions in the SDO policies on patents. For software intended for open source licensing, such as is being developed by OSECS, RAND conditions are clearly unreasonable and discriminatory. RAND conditions would allow charging of license fees for patents used in open source software. Any such fees violate the underlying principles of open source software licenses.

2. The stronger role of foreign governments in standards needs to be balanced by the US

The US government should take a greater role in certain international standards bodies to help balance the roles taken by foreign governments in those bodies. The influence of foreign governments in those bodies places US companies, and especially US small businesses, at a disadvantage in activities of those standards bodies and access to the resulting standards. Foreign governments treat that involvement as an economic development issue. The US government should also treat it as such.

International standards bodies including the International Standards Organization (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunications Union (ITU) have much greater involvement of foreign governments than do many other SDOs. The ITU is a specialized agency of the United Nations and is explicitly governmental, although US participation involves a public/private arrangement. The ISO and IEC have many characteristics of quasi-governmental organizations, such as membership and balloting by country instead of by individual participant. We were also surprised to learn recently that ISO and IEC standards have special status in international agreements, such as treaties on trade. Although IEEE is an international organization, its standards do not have the same status, except for occasional arrangements it makes for joint publication with ISO or IEC.

Foreign governments have a much greater involvement in the processes of standards development and use than does the US government. It is our understanding that foreign governments subsidize participation and provide copies of standards to their citizens.

US companies, especially small businesses, are at a disadvantage in dealing with ISO and IEC standards. The fully private nature of US participation in these entities is at the core of the issues raised at the recent FERC Technical Conference regarding the very high costs of the five IEC standards referred by NIST to FERC for rulemaking consideration. According to the response of the IEC representative in the Smart Grid efforts, provided at a special session of Grid Interop 2009, the national committees have jurisdiction over distribution of IEC standards in their countries. For the US, that would be the US National Committee (USNC), a unit of ANSI.

3. There are a wide variety of reasons and rules for standards participation.

Standards are central to many activities in computer hardware/software and data communications. Participation in standards activities allows the participant to gain knowledge of the standards as they are being developed, to influence development of the standards, and to contribute professionally. Especially for standards that must be purchased, often at great expense, participation in standards activities allows participants to become sufficiently knowledgeable about the standards to advocate for or against adoption of the standards within their organizations. Participation in standards activities is generally voluntary, although some people are assigned by their organizations to participate.

The rules for standards participation are as varied as the governance and adoption structures of the various standards developing organizations (SDO). In addition, there are rules -- both written and unwritten, with varying enforcement – that govern the operation of both SDOs and their standards-drafting working groups.

Participation is also influenced by the use or non-use of technology to support working group operations. Some working groups conduct their activities using a combination of face-to-face meetings, teleconferencing, and email. Most working groups require a level of attendance to allow continued good standing of membership. Some SDO's allow “Corresponding Membership” in which the participant receives the information and is able to comment by email but is not required to attend face-to-face meetings.

OSECS experience in standards participation has varied. Dr. Klein has participated in a number of IEEE standards, either as a member of the working group or of the ballot pool. However, although Dr. Klein is a US participant in IEC TC 57 WG 15 (on cybersecurity for the TC 57 standards) he was refused participation in WG 10 and WG 17 because OSECS could not commit to extensive international travel for face-to-face meetings. The requirement for such commitment is unwritten, and the US Technical Advisory Group (TAG) for TC 57 does not allow Corresponding Membership (although other countries do allow it).

The rules of the IEC are much more strict regarding the benefits of participation than are, for example, the IEEE. The IEC places limits on members of one TC 57 working group accessing the discussions or preliminary materials of another working group in the same committee. The draft standards are marked to indicate that their use is to be only for preparing national committee comments to the standard. Copies of standards for other uses are expected to be purchased, even by the volunteers who drafted them. By contrast, after an IEEE standard has been adopted, members of the working group are given complementary copies by IEEE.

4. The US government role in standards has varied and needs to become more consistent

The US government role in standards has been highly variable. At some times it has been very influential, At other times it has done little, even when it could have been very helpful. The US government role in standards needs to become more consistent and sensitive to its impacts. Here are some examples:

- From the early 1980's up to the early 1990's, the government was deeply involved in the development of the ISO Open System Interconnection standards. NIST and NASA personnel participated in the committees. NIST hosted an OSI Implementers Workshop (OIW), that was one of three in the world bringing developers together to work out issues in OSI technology and its implementations. There was also a Government OSI Profile (GOSIP) and work on an Industry Government Open System Specification (IGOSS). The work on IGOSS was coordinated with work at the Electric Power Research Institute (EPRI) on the Utility Communications Architecture (UCA). The UCA is the underlying technology for two of the five standards referred by NIST to FERC.

- It is not well known, but although IEC-61850 uses the Internet Protocol Suite (commonly known as TCP/IP) for transport, its upper layers are one of the few remaining uses of ISO OSI. The US government involvement in OSI was ended early in the Clinton administration. There are documents referenced in 61850-8-1 that are based on the Stable Implementers Agreements prepared by the NIST-sponsored OIW. These documents are difficult to find because NIST no longer maintains the OIW documents on its web site.

- The ending of US government involvement in ISO OSI resulted in the broad adoption and deployment of the Internet Protocol Suite. The Internet was originally a government project, and the Internet Engineering Task Force, that develops the Internet standards, a government sponsored entity.

- In preparing IEEE-1686, which is a standard for electric power substation device cybersecurity features, a need was identified for specifying requirements for strong authentication. The best information available on strong authentication appears to be NIST Special Publication 800-63. However, SP 800-63 was written as an internal government guideline. Its form, structure, and some of its content make it unsuitable for use as a normative reference in an IEEE standard. It would have been useful had the document been written with a view toward allowing normative citation of portions of the document in non-government standards. Such considerations especially apply where NIST has leading expertise in particular technical areas.

5. The Veeck decision is relevant for government rules related to standards

In the Veeck case -- Veeck v. Southern Building Code Congress Int'l, Inc. , 293 F.3d 791 (5th Cir. 2002) – the court essentially decided that when standards become part of law or regulation the right of the public to know the law trumps the right of a copyright-holding standards publisher to charge for and exclusively distribute copies of the standard. The case involved a building code standard that was adopted into municipal law. Some of the application of this decision to efforts such as the Smart Grid and health care data standards may be legally murky. However, the principles of the decision – that the Supreme Court refused to review – should be considered by US government agencies as technical standards become increasingly intertwined with law and regulation.

SUMMARY AND RECOMMENDATIONS

The Sub-Committee on Standards should take appropriate action or make appropriate recommendations in the following areas:

- The need for a Federal definition of “open standard”
- The need for maintaining archives of NIST-sponsored documents that may later be identified as normative references in standards
- The advisability of formatting and structuring NIST technical guidelines so they may be used as normative references in non-NIST standards, especially in cases where NIST has leading expertise in the relevant technology
- The advisability of the US government becoming more active in supporting participation by US entities in international standards. Such activity could be as simple as advocacy and support for increased remote access to international standards meetings or as extensive as subsidy for the international travel required if remote access is not provided.
- The effects of the Veeck decision on public availability of standards that are referenced or incorporated into law or regulation. Many members of the public may have reason to seek access to standards that are officially recognized for activities such as the Smart Grid.

  This especially applies to standards directly affecting the public. An example of direct impact would be standards relevant to implementation of privacy requirements when they arise in state public service commission rulemakings. Many privacy requirements are implemented by cybersecurity standards (such as encryption to protect confidentiality), and a full understanding of these standards may require access to data structures, formats, and semantic definitions.

  Examples of possible solutions could include:
  - Negotiation of nationwide “site licenses” with the SDOs
  - Making copies available through public libraries
  - Avoidance in these activities of standards that are not freely available to the public.