Point Paper
Federal Agencies' Engagement in Standards
March 6, 2011

US Government engagement in international standards development is critical for US industry competitiveness and continued US innovation in the market place. International standards landscape is complex and does not lend itself to a hierarchical structure; rather it is more like a web of a variety of organizations which makes it challenging to ensure that all critical efforts are covered. Standards are developed in a variety of standards development organizations (SDOs) broken down into a further set of subcommittees and working groups each of which is run by technical experts from a variety of countries. Participation by both governments and industry is voluntary and requires investment of people's time and organizations' financial resources (joining fees for national bodies, travel expenses, opportunity cost of expert time being spent on standards and not revenue-producing activities, etc). Having said that- this engagement is critical to a nation's global economic position.

The most widely used cyber security standards are developed by the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1 Subcommittee 27 (SC27), IT Security Techniques. SC27 standards portfolio includes over 90 standards ranging from encryption to disaster recovery, application security, and information and communication technology supply chain risk management (ICT SCRM). Systems and Software Engineering standards are developed by ISO/IEC JTC1 SC7 and are also critical for cybersecurity as they define the foundation for how cyber environments (IT systems, software, and services) are acquired, developed, integrated. Specifically in the area of cybersecurity, SC7 is developing ISO/IEC 15206, Systems and Software Assurance which will provide requirements and guidance for developing systems and software in a security-conscious way. SC27 is currently reviewing the initial draft of ISO 27036 on Information Security / Supplier Relationships.

SC27 is a good example of the composition of a JTC1 Subcommittee. It has been in operation 20 years and enjoys membership from over 40 countries where the most active countries are Japan, China, UK, Sweden, Germany, Korea, Malaysia, Australia, Poland, Russia, Singapore, Spain, and South Africa. Standards development takes years, requires knowledge of the process, good working relationships with the leadership and with the individual technical experts from a variety of countries. While US delegation to SC27 enjoys expert support from NSA and NIST and SC7 is supported by NIST and DoD, these experts do not provide appropriate coverage of all strategically important subjects for standardization. USG has filled its gaps by engaging contracted industry experts to participate in the work of SC27 and SC7 to leverage their knowledge and relationships to successfully create new standards in the areas of strategic importance, e.g. ICT SCRM and Systems and Software Assurance.

This outsourced expert support for USG cybersecurity standardization efforts is critical for US success in influencing international standards in this field and assuring that the right content is included to enable continued US industry competitiveness and appropriate protections for US critical infrastructure and overall cyber ecosystems. This outsourced support is continuously at a high risk of budget cuts because it rarely directly supports short term mission goals of those organizations that own the contracts enabling the outsourced capability. Eliminating this expert support will have lasting effects to US competitiveness and ability to influence international SDOs for the long term due to the fact that there are not enough government experts with relationships and expertise to immediately fill the void. Valuable time will be lost as it is expected that most critical content for cybersecurity standardization will be produced in the next 5 years. It is imperative that those relatively small efforts dedicated to continued USG participation in cybersecurity standardization are continuously funded and supported by the USG for the long term success and competitiveness of the United States.

One such example of this work today is DoD Outreach & Standardization efforts in support of the US Comprehensive National Cyber Security Initiative – (#11) Supply Chain Risk Management (SCRM). Attached are slides describing SCRM engagement and positive traction with the ISO Community.

Don Davidson (don.davidson@osd.mil)
Chairman, SCRM AdHoc WG
CyberSecurity 1, American National Standards Institute (CS1/ANSI)
In support of JTC1 / ISO