

January 12, 2012
Donna Dodson
Division Chief, Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Ms. Dodson:

The Security Content Automation Protocol specifications (hereinafter, “Specifications”) have matured significantly over the past several years. The concept and development led by MITRE and the US Government is greatly appreciated and has been extremely valuable to improve the automation capabilities for information security. As vendors serving a broad customer base, we have come to recognize these Specifications are instrumental for improving the security posture for the commercial sector as well as international customers. Although the contributions of the technical development community have been significant, having them developed as a perceived US Government effort is preventing global adoption of their use in commercial products. We believe there is a critical and immediate need to move the Specifications to an internationally respected standards body for continued technical development, where other standards bodies can normatively reference these Specifications. We commend the sponsoring US government agencies for the work they have done thus far, for the work we expect them to continue, and for actively participating in our ongoing discussions.

This recommendation is a result of vendor consensus from a systematic review of several candidate organizations, including: The Distributed Management Task Force (DMTF), the Object Management Group (OMG), the OpenGroup, the Organization for the Advancement of Structured Information Standards (OASIS), the Trusted Computing Group (TCG), and the Internet Engineering Task Force (IETF).

The undersigned Vendors recommend moving the security content automation specifications development to the IETF.

Our recommendation is based upon the following considerations:

- The IETF operates using a similar structure as the current custodians
- Participation in the IETF is free and open to everyone on a global scale
- IETF meetings are held tri-annually around the world, and remote attendance is supported
- A process exists for vendors to ensure interoperability of standards
- A process exists to evaluate proposals that may involve competing solutions for standards
- IETF standards can be normatively referenced by other bodies such as the International Telecommunications Union (ITU-T) and the International Organization for Standardization (ISO)

We hope you and the other members of the Cross Agency Committee (NIST, DHS, and NSA) will join us in this recommendation. We believe it will propel the Specifications onto the global stage, accelerating the development of security automation while providing for widespread adoption by organizations of all types.

Sincerely,

CC: John Banghart, Security Automation Program Manager, Computer Security Division, National Institute of Standards and Technology
Inette Furey, Director, Research and Standards Integration, National Cyber Security Division, U.S. Department of Homeland Security
Joe Jarzombek, PMP, CSSLP, Director for Software Assurance, National Cyber Security Division, Department of Homeland Security
Tony W. Sager, Jr., Chief Operating Officer (COO), Information Assurance Directorate, National Security Agency
Matthew Scholl, Deputy Division Chief, Computer Security Division, National Institute of Standards and Technology
Richard J. Struse, Deputy Director for Software Assurance, National Cyber Security Division, U.S. Department of Homeland Security