NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE IS SPONSORING:

The 2014 Cybersecurity Innovation Forum

TRUSTED COMPUTING • INFORMATION SHARING • SECURITY AUTOMATION

PARTICIPATING ORGANIZATIONS

NIST National Institute of Standards and Technology U.S. Department of Commerce

January 28-30, 2014 **Baltimore Convention Center**

Home
Call for Speakers
Registration
Agenda
Speakers
Sponsors/Exhibitors
Location
Contact Us

2014 Cybersecurity Innovation Forum

Background and Vision

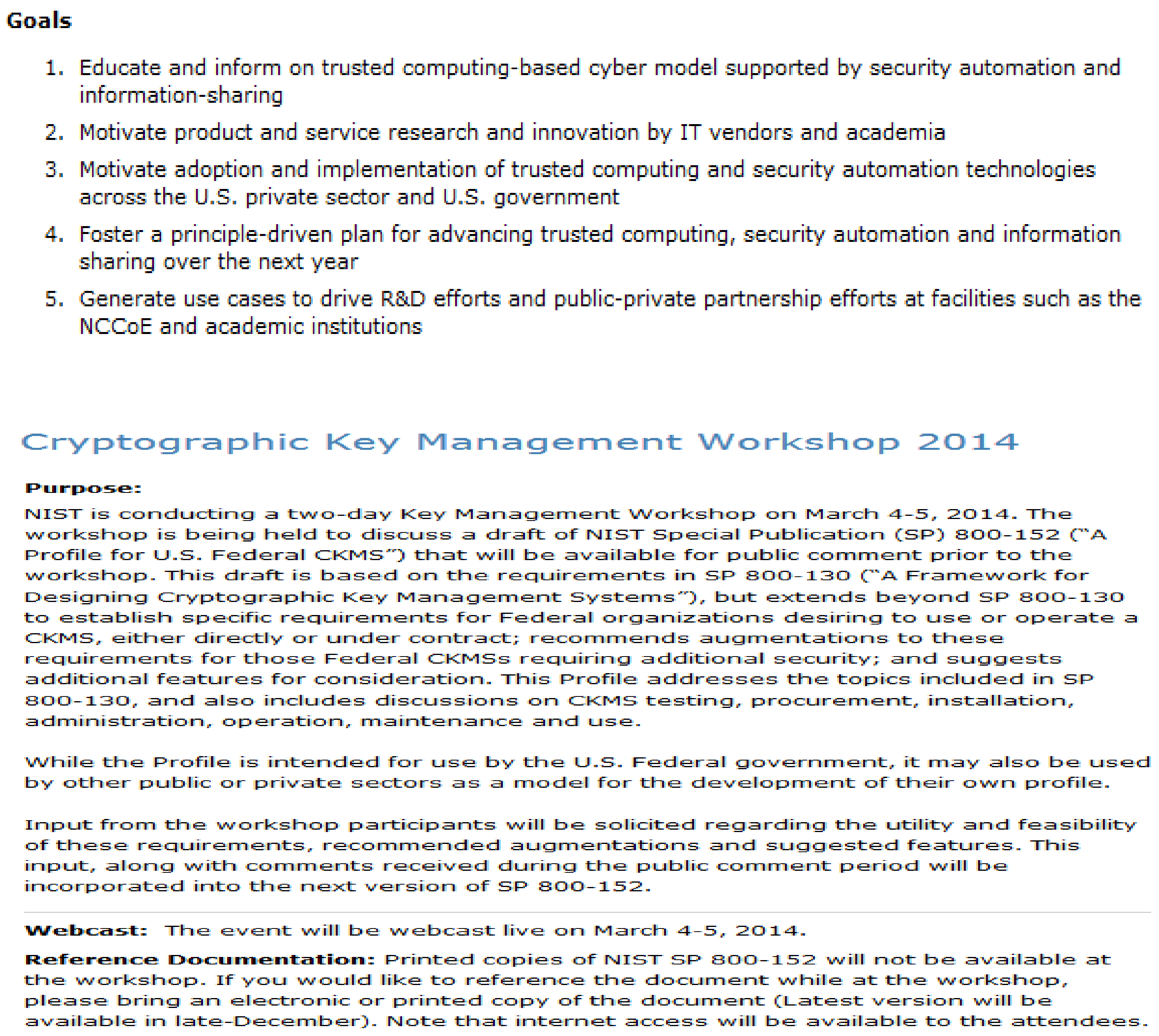
Every facet of our lives – personal and professional – is conducted digitally, yet we live in a world where those electronic transactions simply cannot be trusted. Investments in IT security continue to address discrete security problems in reaction to specific malicious attacks. This approach is unsustainable, non-scalable and inadequate for protecting our nation. It is imperative that we define and embrace a fundamentally different approach to enterprise architecture security – one that builds security in from the beginning as a robust and solid foundation upon which to conduct our transactions. Trusted computing and security automation technologies combined with a vision for, and commitment to, cyber information sharing provide the framework needed to protect our infrastructure, citizens and economic interests.

We need to propagate a cohesive public-private wave of strategic innovation and implementation to build a lasting, secure, resilient foundation for U.S. economic and national security that persists and flourishes despite the efforts of adversaries and criminals. Our vision is for trusted computing and security automation technologies to be ubiquitously embedded and used within enterprise architectures and enabled by automated information-sharing in order to facilitate a secure U.S. IT infrastructure.

Summary

The 2014 Cybersecurity Innovation Forum is a three-day event sponsored by the National Cybersecurity Center of Excellence (NCCoE) with the Department of Homeland Security, the National Institute of Standards and Technology, and the National Security Agency as primary participating organizations. The forum will cover the existing threat landscape and provide presentations and keynotes on current and emerging practices, technologies and standards. The 2014 forum will provide action-oriented outputs to fuel voluntary principle-driven consensus-based standards efforts, create opportunities for industry growth and drive research activities, and define use cases for subsequent exploration, which in turn will feed back into the coming years' forums, continually evolving the state of the art.

In 2014, the Cybersecurity Innovation Forum will bring the content, expertise and momentum from the Trusted Computing and IT Security Automation conferences and previous discussions on information sharing into a single event. Combining these events merges the discussions and will help develop more robust and



Goals

1. Educate and inform on trusted computing-based cyber model supported by security automation and information-sharing
2. Motivate product and service research and innovation by IT vendors and academia
3. Motivate adoption and implementation of trusted computing and security automation technologies across the U.S. private sector and U.S. government
4. Foster a principle-driven plan for advancing trusted computing, security automation and information sharing over the next year
5. Generate use cases to drive R&D efforts and public-private partnership efforts at facilities such as the NCCoE and academic institutions

Cryptographic Key Management Workshop 2014

Purpose:

NIST is conducting a two-day Key Management Workshop on March 4-5, 2014. The workshop is being held to discuss a draft of NIST Special Publication (SP) 800-152 ("A Profile for U.S. Federal CKMS") that will be available for public comment prior to the workshop. This draft is based on the requirements in SP 800-130 ("A Framework for Designing Cryptographic Key Management Systems"), but extends beyond SP 800-130 to establish specific requirements for Federal organizations desiring to use or operate a CKMS, either directly or under contract; recommends augmentations to these requirements for those Federal CKMSs requiring additional security; and suggests additional features for consideration. This Profile addresses the topics included in SP 800-130, and also includes discussions on CKMS testing, procurement, installation, administration, operation, maintenance and use.

While the Profile is intended for use by the U.S. Federal government, it may also be used by other public or private sectors as a model for the development of their own profile.

Input from the workshop participants will be solicited regarding the utility and feasibility of these requirements, recommended augmentations and suggested features. This input, along with comments received during the public comment period will be incorporated into the next version of SP 800-152.

Webcast: The event will be webcast live on March 4-5, 2014.

Reference Documentation: Printed copies of NIST SP 800-152 will not be available at the workshop. If you would like to reference the document while at the workshop, please bring an electronic or printed copy of the document (Latest version will be available in late-December). Note that internet access will be available to the attendees.