2009 Open Forum for Standards Developers

Cybersecurity and Its Impact on NIST

Dan Benigni
NIST/ITL Computer Security Division
Chairman, INCITS CS1 – Cyber Security

Open Forum for Standards Developers
October 6, 2009

Part of the World Standards Week 2009 series of events

ANSI American National Standards Institute

Overview

From my perspective

- NIST Computer Security Division
- INCITS CS1 – Cyber Security (US TAG to SC 27)

Snapshot on cyber security standards

Too much to cover in any detail

Make the business case for cyber security standards and conformity assessment

Standards

- Coverage:
  - International, Regional, National, Company
- Developers:
  - Formal Private Sector, Formal Treaty-Based, Consortia, Companies, Other (e.g., IETF)
- Uses:
  - Voluntary, Mandatory
- Development Method:
  - Consensus, De Facto
- Availability:
  - Open, Proprietary

NIST ITL's Approach Standards

- The National Technology Transfer and Advancement Act (P.L. 104-113) encourages Federal agencies, as well as state and local governments, to achieve greater reliance on voluntary standards.
- To achieve our goals, NIST ITL works with industry and other agencies to develop information technology standards through voluntary consensus standards developing organizations.
- Federal Information Processing Standards (FIPS) are now developed on an exception basis -- when there are no existing voluntary standards to address immediate Federal requirements for computer security.

Standards for Cyber Security

- ***Standards*** include documentary standards, measurement and testing standards.
- ***Cyber*** refers to computers and networks.
- ***Security*** includes:
  - Confidentiality (of data and system information)
  - Integrity (of systems and data)
  - Availability (of systems and data for intended use only)

Cyber Security Mandates for NIST

- Computer Security Act of 1987 (Public Law 100-235)
- Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106)
- Aviation and Transportation Security (Public Law 107-71)
- Enhanced Border Security and Visa Reform Act (Public Law 107-173)
- Cyber Security R&D Act (Public Law 107-305)
- Federal Information Security Management Act of 2002 (Title III of E-Gov) (Public Law 107-347)
- OMB M04-04 E-Authentication Guidance for Federal Agencies
- OMB Circular A-130 and OMB Directive 05-24
- Homeland Security Presidential Directive - 12: Policy for a Common Identification Standard for Federal Employees and Contractors
- National Security Presidential Directive - 59/ Homeland Security Presidential Directive - 24, Biometrics for Identification and Screening to Enhance National Security

Why Cyber Security Standards?

- "Over the course of a few years, a new communications technology annihilated distance and shrank the world faster and further than ever before. A worldwide communications network whose cables spanned continents and oceans, it revolutionized business practices and gave rise to new forms of crime." [1]
- [1] *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers*, Tom Standage, 1999
- History of the 19th century telegraph repeats, with a vengeance, for the 20th century advent of digital electronic technologies.

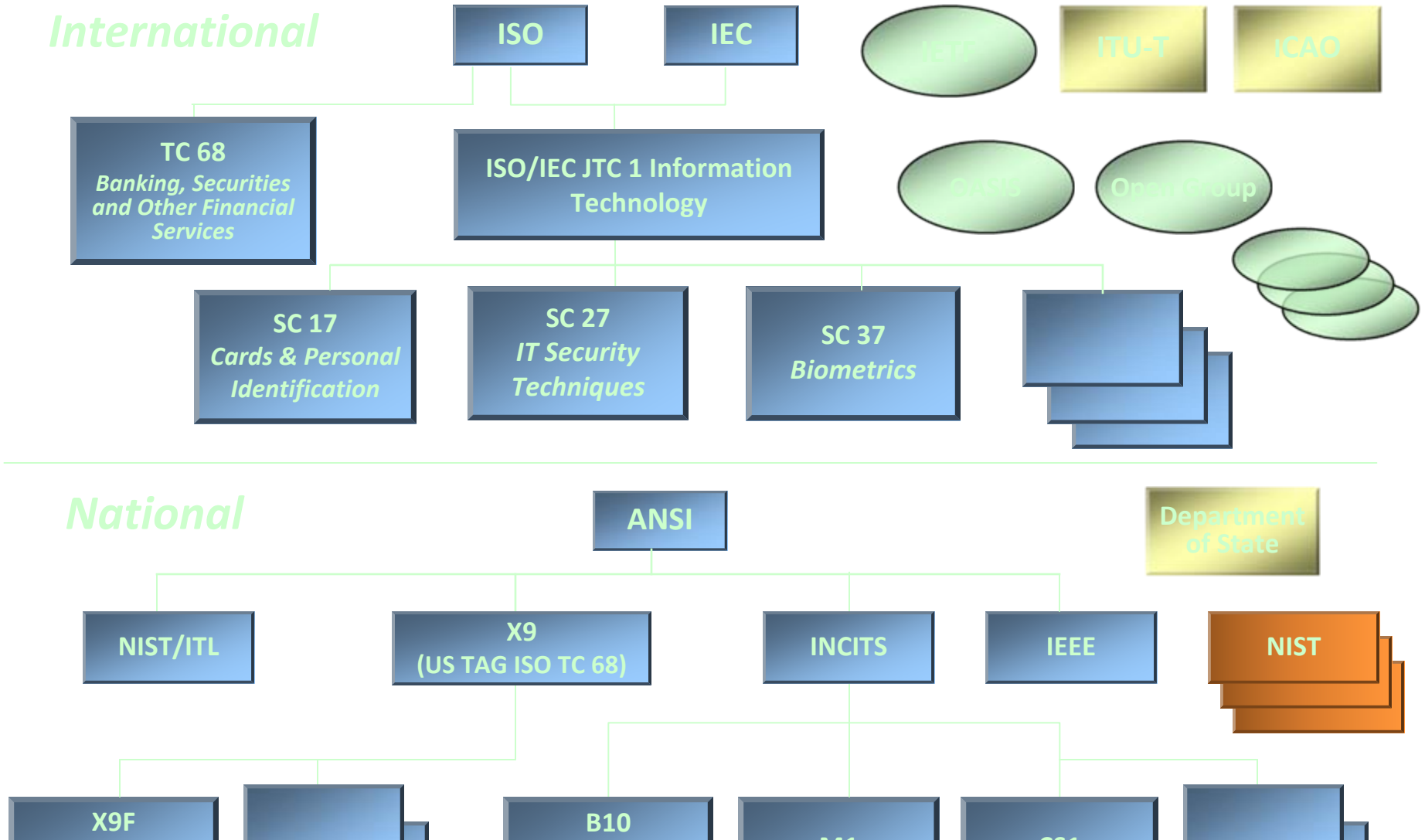
Why Cyber Security Standards?

- With the 20th century advent of digital information technologies and networks, the rise of crime seen with the 19th century telegraph repeats, with a vengeance.
- Now, one estimate is that business losses from cybercrime are as high as $1 trillion a year worldwide.
- Cyber security standards are necessary to support the deployment of significantly better, standards-based security solutions for business and government.

Cyber Security Standards Developers

- ISO/IEC JTC 1 on Information Technology
- ISO TC 68 on Banking and Other Financial Services
- Internet Engineering Task Force (IETF)
- InterNational Committee for Information Technology Standards (INCITS)
- X9, Inc. - Financial Industry Standards
- National Institute of Standards and Technology (NIST)
- Institute of Electrical and Electronic Engineers (IEEE)
- ***Many Others***

Cyber Security Standards Developers

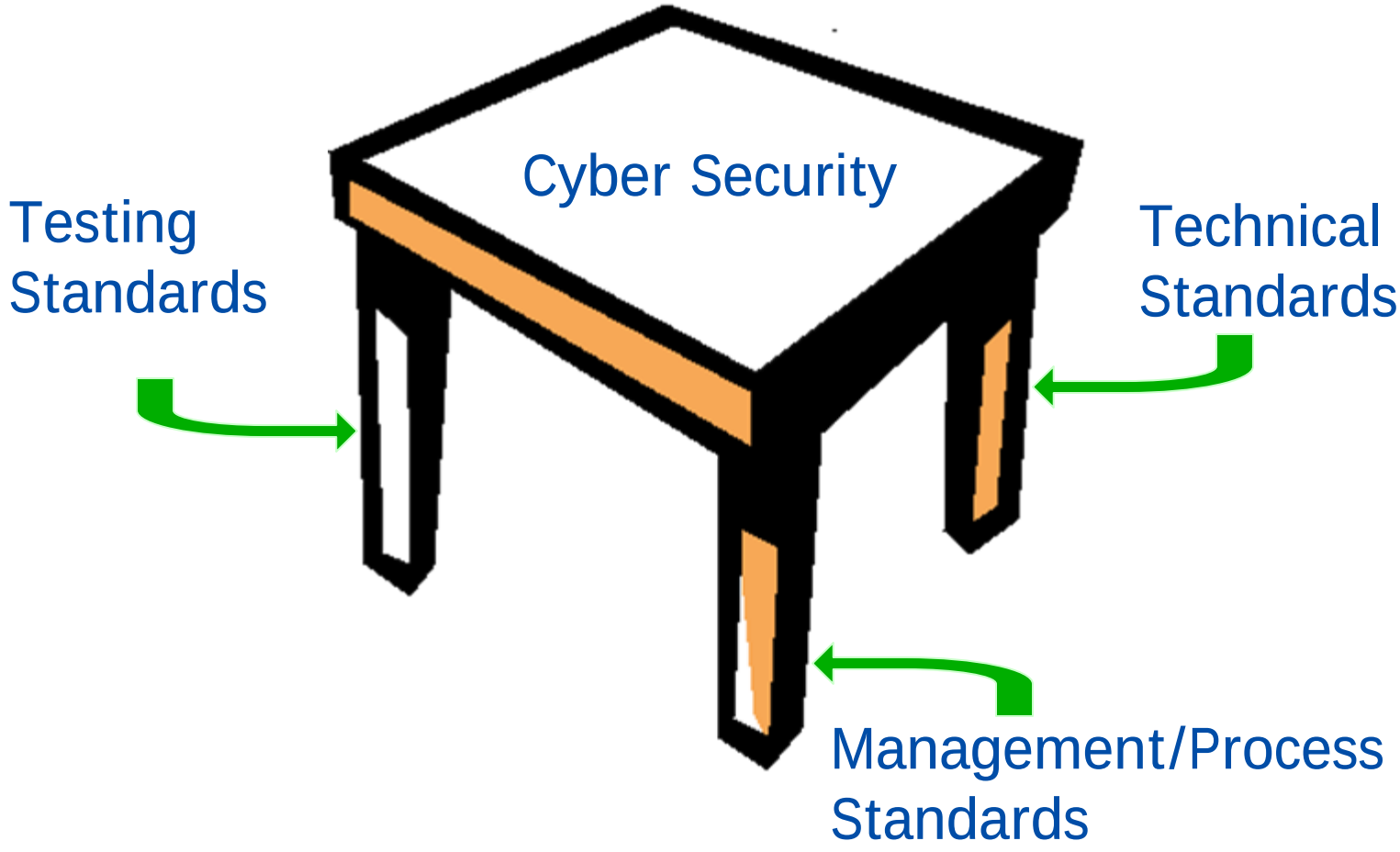


JTC 1/ SC 27 Scope (US TAG is INCITS CS1)

The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.

Three Categories of Standards



Management/Process Standards - Examples

- ISO/IEC 27000, *Information security management systems* (many parts)
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004 February
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, 2006 March
- INCITS, *Small Organization Baseline Information Security Handbook (SOBISH)* (project initiated – February 2009)

Technical Standards – Examples

- FIPS 197, *Advanced Encryption Standard (AES)*, November 2001 (part of ISO/IEC 18033-3:2005)
- FIPS 201-1, *Personal Identity Verification for Federal Employees and Contractors*, March 2006
- ISO/IEC 24727, *Integrated circuit card programming interfaces* (six parts)
- NIST SP 500-267, *A Profile for IPv6 in the U.S. Government – Version 1.0*, July 2008

Testing Standards - Examples

- NIST SP 500-273, *IPv6 Test Methods: General Description and Validation*, August 2009
- FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 2001
- ISO/IEC 15408:2005, *Evaluation criteria for IT security* (three parts)
- ISO/IEC 19795, *Biometric Performance Testing and Reporting* (multi part)

Why Conformity Assessment?

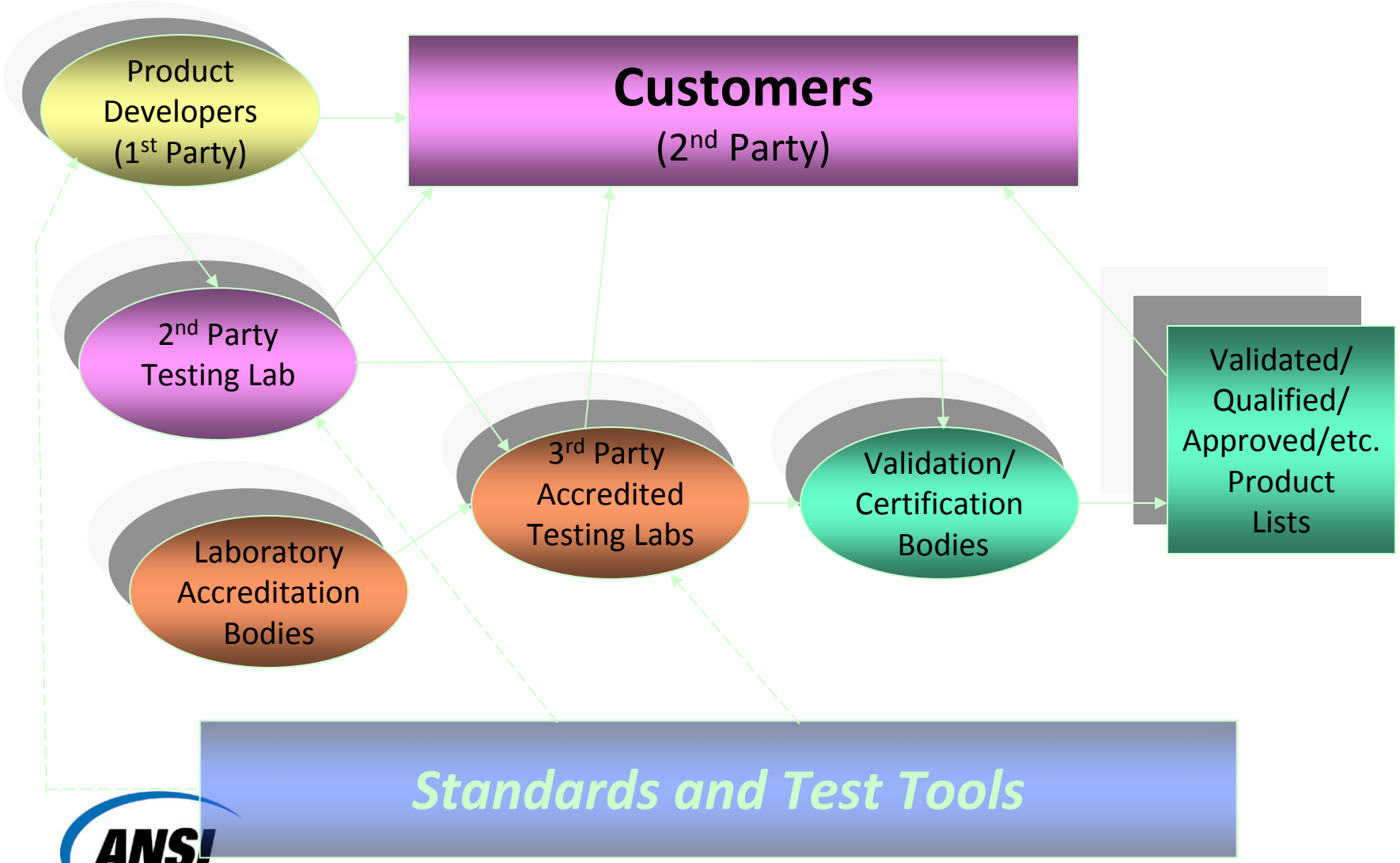
- ***Standards***, often, specify requirements.
- ***Conformity Assessment (CA)*** determines whether a product, service or system has fulfilled all of those requirements.
- ***Testing*** (1st, 2nd, or 3rd party) is often the most rigorous way to determine if a product, service or system has fulfilled all of those requirements.

Why Cyber Security Testing?

- "When you can measure what you are speaking about and express it in numbers, you know something about it; but when you cannot measure, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science."[2]

- [2] Lord Kelvin, William Thomson, who was knighted in 1866 and was raised to the peerage in 1892 (as Baron Kelvin of Largs) in recognition of his work in engineering and physics, was foremost among the small group of British scientists who helped to lay the foundations of modern physics.

Standards & CA Infrastructure



Ubiquity of IT Drives Cyber Security

- Cyber security is in its infancy.
- Less than 40 years ago, the concept of remotely interconnected systems began with the connection of four university mainframes.
- In 1971, the first email program was created to send messages across a distributed network.
- Now, it is estimated that business losses from cybercrime are as high as $1 trillion a year worldwide.

Ubiquity of IT Drives Cyber Security

- In 1980, an accidentally propagated status message caused the first denial of service “attack”, bringing down the burgeoning system.
- Today there are over two million Internet hosts with more than a billion users.
- We have become accustomed to the benefits of being always on and always connected and of just in time products and services.

Challenge for IT System Owners

- System owners must show due diligence in their security planning by calculating return on investments for their security initiatives.
- This is challenging because correlations are difficult to make between security controls and threats.
- This is where cyber security standards built by consensus of a variety of stakeholders can give us a great advantage.

Challenges for Standards (and Test) Developers

- Hundreds of cyber security standards have been and are being developed by dozens of standards developers.
- Maintaining effective and secure connectivity requires continuing standards development/maintenance and cooperation among many standards developers.
- The need for open, international voluntary consensus cyber security standards will continue to grow.
- These standards activities will be necessary to support the deployment of significantly better standards-based security solutions for business and government.