Security Automation and the International Community

Kent Landfield, McAfee

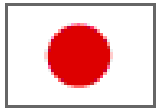
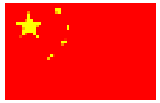
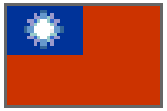
SCAP Developer Days

Tuesday, July 10, 2012

Objective

SCAP is gaining international appeal as other countries are recognizing its value. As such there are efforts in various international SDOs to advance security automation. This session will describe the reasoning behind the movement and how each is playing a role today. IETF, ISO, and ITU-T efforts will be discussed.

Global Participation in SCAP Components

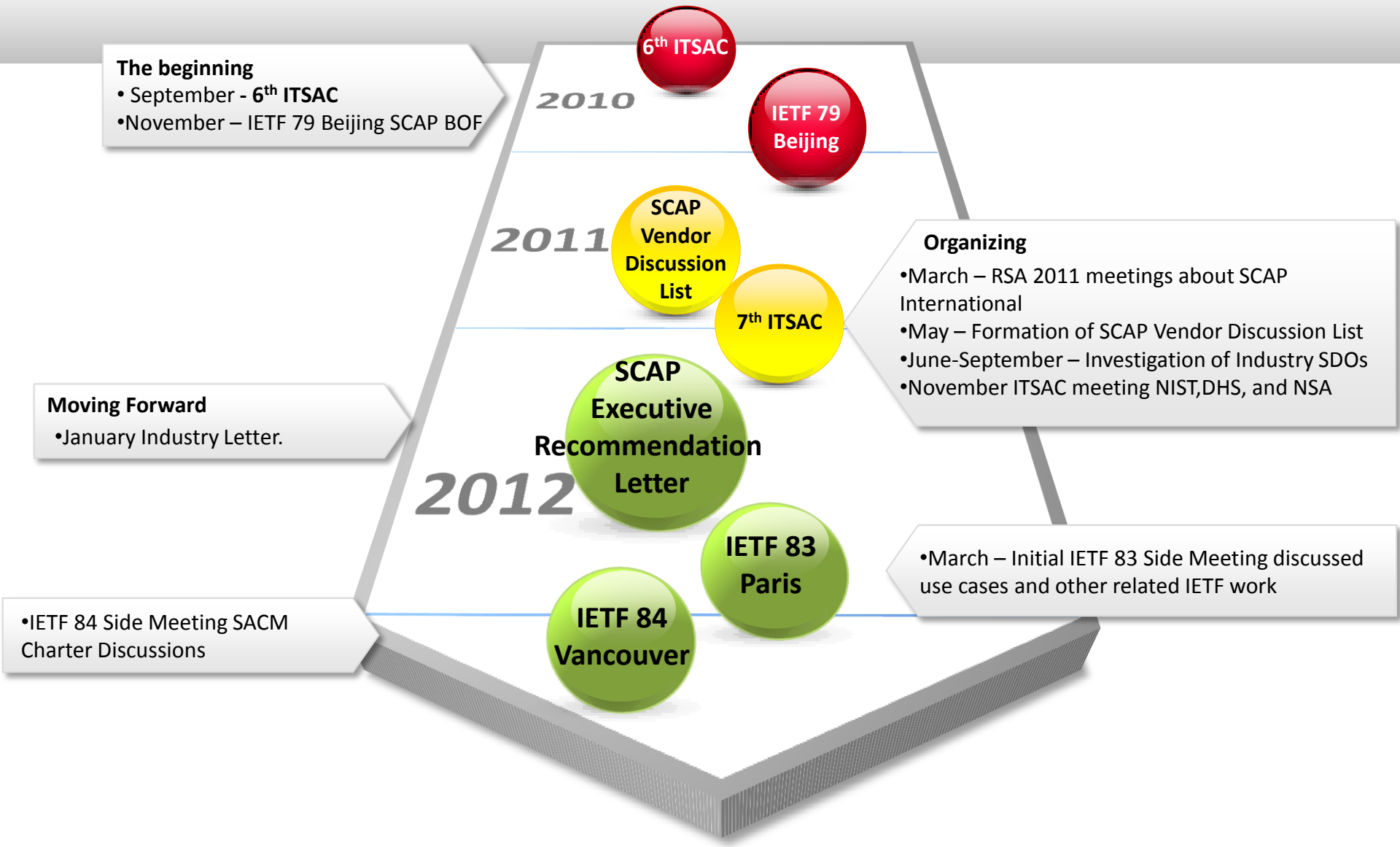
-  US
-  UK
-  Australia
-  Japan
-  China
-  Korea
-  Germany
-  India
-  Brazil
-  Taiwan
-  France
-  Russia

Reasons For Transitioning to International Development

- Perception of US effort restrictive of global participation
  - Global recognition of specifications
  - Global participation
- Too few technical eyes on newly proposed or modifications of existing specification's
  - More true transparency needed
  - More diverse use case perspectives needed
- Restrictive to initiation of innovation
  - Funding required to initiate a new projects
  - Inhibited vendors from creating new advances
- Need to enable derivative capabilities
  - Formal standards need to to be normative references
  - IP considerations
- Need to include and recognize work from other countries
  - Helps to gain a sense of ownership to gain global adoption (IODEF – from Europe (TERENA) and the forensic work from Korea)

TIMELINE of significant events leading up to present

Past 3 Years



Security Automation Specification Development

- Global Specification Development
  - Vendors proposed a transition of the specification development to the IETF
  - Government in support of these efforts
  - This is targeted at Technical Specifications only and will not affect operational components such as the NVD or MITRE OVAL repository
- A Letter of Support for the transition was signed by 16 SCAP security software vendors and was sent to NIST, NSA and DHS senior management
- Coordinating with NIST, DHS and NSA on the transition. They are participating with vendors in the effort.

Security Automation Executive Recommendation Letter

- Recommended transition 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)

Signatories

	Name	Title	Organization
1	Jeffrey Nick	Chief Technology Officer	EMC Corporation
2	Oliver Tavakoli	CTO, Security Business	Juniper Networks
3	Dwayne A. Melancon	Chief Technology Officer	Tripwire Inc.
4	Chandrashekhar Basavanna	Chief Executive Officer	SecPod Technologies
5	Timothy D. Keanini	Chief Technology Officer	nCircle
6	Randal S. Taylor	Chief Technology Officer	ThreatGuard
7	Alberto Bastos	Founder and CTO	Modulo Security
8	Mark Bohannon	Vice President, Corporate Affairs & Global Public Policy	RedHat
9	Eric Hibbard	CTO Security & Privacy	Hitachi Data Systems
10	Phyllis Schneck	VP and CTO, Public Sector	McAfee, Inc.
11	Carl Banzhof	CTO & Founder	Rockport Technology LLC
12	John Bordwine	Public Sector CTO	Symantec
13	Aaron Chernin	Security Automation	DTCC
14	Luiz Nunez	Principle Consultant	C3iSecurity
15	Billy Austin	Chief Security Officer	Saint Corporation
16	Ronald J. Gula	Chief Executive Officer	Tenable Network Security

Security Automation & Continuous Monitoring (SACM)

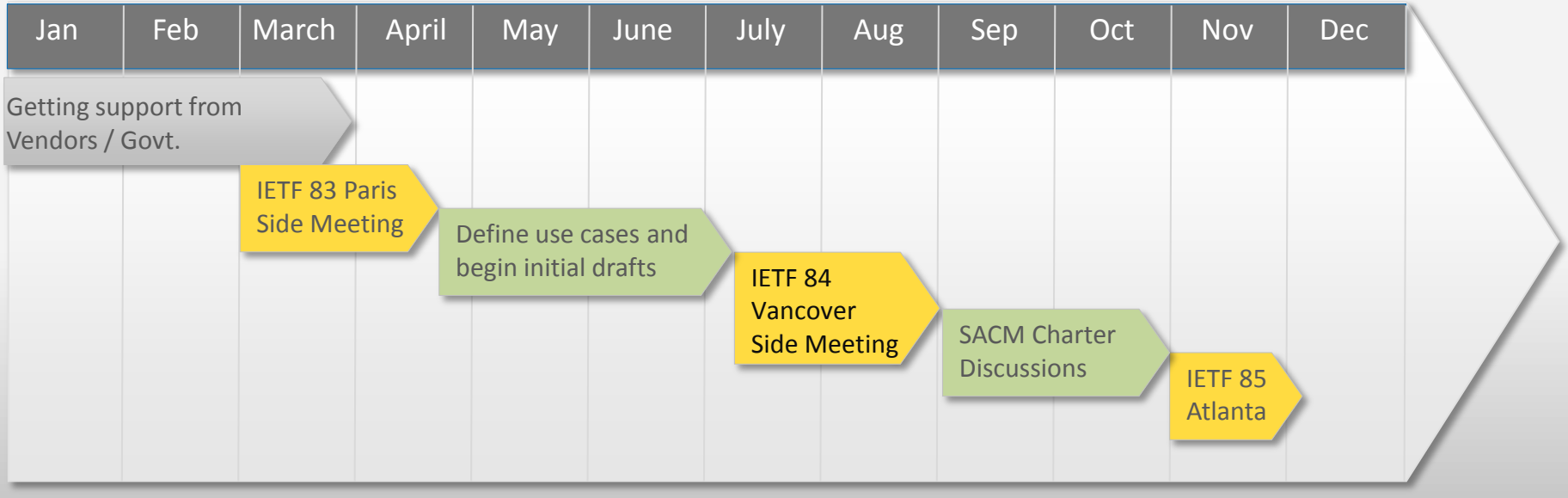
- Complete the job SCAP began while laying a foundation for future use cases and operations.
- Items listed below have been recently discussed on the IETF sacm mailing list as ***potential*** areas of work for the group.
  - Abstracting data at differing levels in the organization
  - Unified Scoring Models Integration / Evaluation
  - Semantic Vocabularies / Advanced Uses
  - Checking Language Development
  - Remediation
  - Content Distribution (Distributed Content Repository specifications supporting consistent access to content and reuse)
  - Content and Results Signing (Non-repudiation of input and output)
  - Enterprise Reporting (Ability to turn a set of single system results into an aggregated organizational picture)
  - Light weight Query and Tasking languages (Approved drilling down across organizational structure)
  - Transition Security Automation Specifications as appropriate

IETF SACM WG

TIMELINE and Milestones

1. Gain support for a Security Automation WG in IETF
2. IETF 83 Paris - lay the ground work for SACM WG formation
3. IETF 84 Vancouver – Discuss potential charter
4. IETF 85 Atlanta – Potential SACM WG forming BOF

2012



Security Automation & Continuous Monitoring Discussion List

This list is for discussions relating to advancing global security automation specifications and efforts while applying them to address current and emerging use cases.

Subscribe:

https://www.ietf.org/mailman/listinfo/sacm

Post:

sacm@ietf.org

IETF 84 Meetings

SACM Side Meeting:

Date: TBD

Time: TBD PDT

Meeting Room: TBD

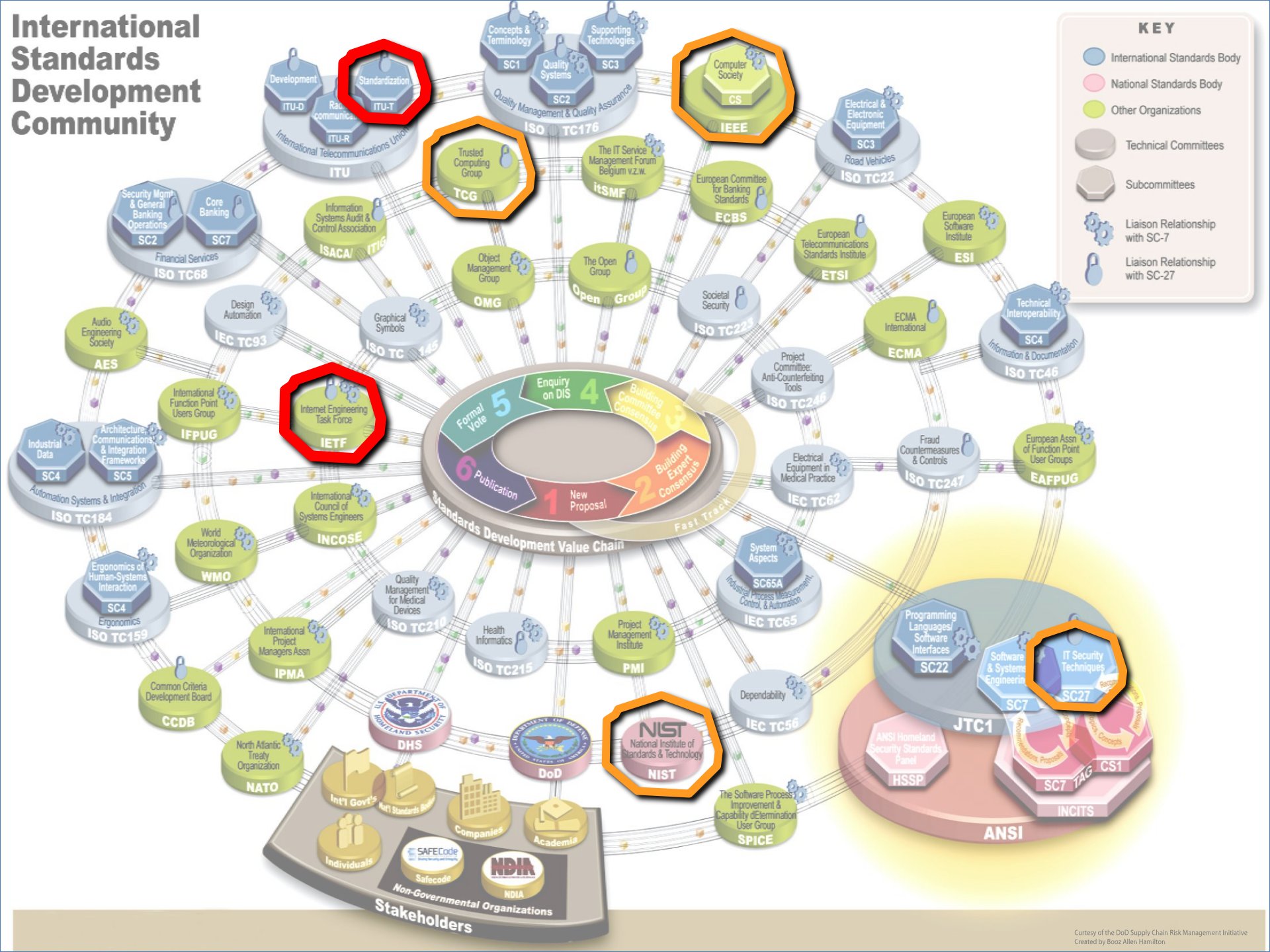
MILE WG:

Date: Tuesday, July 31, 2012

Time: 15:20 to 16:50 PDT

Meeting Room: Regency A

International Standards Development Community



Curtesy of the DoD Supply Chain Risk Management Initiative
Created by Booz Allen Hamilton

ITU-T

- X.1500 Series – Cybersecurity Information Exchange (CYBEX)
- Produced by Study Group 17
- Utilizes SCAP component pieces
- Use Case documents:
  - CVE – ITU-T X.1520
  - CVSS – ITU-T X.1521
  - CWE – ITU-T X.1524

- Potentially use the IETF and ITU-T in combination for the same work areas, where the community work is done with IETF and then a companion ITU-T Recommendation is created that points to the IETF RFC for the normative words/clauses. This "pairing" approach, of IETF RFCS and ITU-T Recommendations, is being fleshed out through the publication of IODEF, RID, and RID-T in both organizations.

- One of the values for doing this is to have stable "named" standards for use in policy, contracts and management efforts through the use of ITU-T Recommendations – where an update to an RFC in IETF means issuing a new RFC number that obsoletes the old one so any documents invoking the old one are now "wrong". By simply updating the ITU-T Recommendation to point to the same paragraphs in the new "replacement" RFC, anyone pointing to the ITU-T document will still be "current".

- Intellectual Property Rights issues are at the forefront of the discussions. There are other concerns with the ITU-T and it's procedures.

ISO SC27 – IT Security Techniques

- Fast Tracked XCCDF 1.2 into the ISO to become and International Standard
- Submitted by NIST October 28th, 2011
- As submitted, it was requested and is anticipated the IETF will be named the "maintenance organization" for XCCDF moving forward
- Current Status:
  - CS1 Executive Board (EB) letter ballot is underway. The EB ballot will close later in July. If this EB letter ballot passes, then the US will vote YES with COMMENTS on the ISO/IEC DIS 18180 ballot. Since CS1 recommended a YES with COMMENTS vote to the EB, it would seem very likely that the US will vote to approve. The US comment is to make the standard freely available.
  - The final voting tally by the ISO/IEC National Bodies for approval requires at least 75% APPROVE and no more than 25% DISAPPROVE. If the international ballot passes, there may be a need for a Ballot Resolution Meeting to dispose of comments. If there are no comments or only minor comments, the project editor (you) would deal with them in conjunction with the ISO editor.
- If the final tally fails, the fast track is over, no ISO/IEC standard.
- The final tally of National Bodies voting should be known sometime in August.

TCG TNC and SCAP

Supporting the evolving integration of security automation and TNC efforts

- **TNC Activity**
  - SCAP Messages for IF-M (draft)
  - Anticipated to be available for public review in October

References

IETF – http://ietf.org

ITU-T - http://www.itu.int/ITU-T/

ISO - http://www.iso.org/iso/home.html

TCG Trusted Network Connect - http://www.trustedcomputinggroup.org/developers/trusted_network_connect/

IETF SACM List Archives - http://www.ietf.org/mail-archive/web/sacm/current/maillist.html

IETF MILE - http://datatracker.ietf.org/wg/mile/

SCAP Vendor Discussion List - http://www.scap.com/mailman/listinfo/scapvendordiscussion_scap.com

Open Mic