

# ***e-Governance and Cloud Standards***

***NIST Standards in Trade Workshop with India on Information  
and Communication Technologies***

September 17, 2014

Mike Hogan  
ITL Standards Liaison

# ***USG in Transition***

- The Federal agencies are moving to using cloud computing services.
- E-government services will be provided more and more via public, private, community, and hybrid clouds.

# ***E-Government Act of 2002***

- Enhance the management and promotion of electronic Government services and processes by:
  - establishing a Federal Chief Information Officer (CIO) within the Office of Management and Budget, and
  - by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.
- government to citizen; government to business; and government to government

# *Office of E-Government & Information Technology*

<http://www.whitehouse.gov/omb/e-gov>

- Headed by the Federal Government's Chief Information Officer.
- Develops and provides direction in the use of Internet-based technologies to make it easier for citizens and businesses to interact with the Federal Government, save taxpayer dollars, and streamline citizen participation.

# ***Digital Government Strategy***

<http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html#top>

- May 23, 2012
- Enable the American people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device.
- Ensure that as the government adjusts to this new digital world, we seize the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways.
- Unlock the power of government data to spur innovation across our Nation and improve the quality of services for the American people

# ***Digital Government Strategy***

- Complements several initiatives aimed at building a 21st century government that works better for the American people.
  - Executive Order 13571 (Streamlining Service Delivery and Improving Customer Service),
  - Executive Order 13576 (Delivering an Efficient, Effective, and Accountable Government),
  - President’s Memorandum on Transparency and Open Government,
  - OMB Memorandum M-10-06 (Open Government Directive),
  - National Strategy for Trusted Identities in Cyberspace (NSTIC), and
  - 25-Point Implementation Plan to Reform Federal Information Technology Management (IT Reform).

# ***Benefits of E-Government Initiatives***

[http://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/fy14\\_omb\\_report\\_to\\_congress\\_on\\_the\\_benefits\\_of\\_e-government\\_initiatives.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy14_omb_report_to_congress_on_the_benefits_of_e-government_initiatives.pdf)

- Annual Report to Congress.
- Latest is January 8, 2014.
- Provides a description of the objectives and primary benefits of E-Government initiatives and lines of business.
- Highlights the accomplishments and cost-effectiveness of the initiatives.

# ***E-Government Initiatives & Lines of Business (LOB)***

- Budget Formulation and Execution LoB
- Disaster Assist Improvement Plan
- Disaster Management Program
- Federal Asset Sales
- Federal Health Architecture LoB
- Financial Management LoB
- Geospatial LoB
- Human Resources Management
- Information Systems Security LoB
- Internal Revenue Service Free File
- Recreation One-Stop
- SAFECOM

# ***Federal Cloud Computing Strategy***

<https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf>

- February 8, 2011
- Developed and championed by the Federal Government's Chief Information Officer.
- Provides information to help agencies modify their IT portfolios to fully take advantage of the benefits of cloud computing in order to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost.

# ***Federal Cloud Computing Strategy***

- To harness the benefits of cloud computing, institutes a ***Cloud First*** policy.
- This policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.

# ***Federal Cloud Computing Strategy***

## ***NIST's Role***

- “NIST will play a central role in defining standards, and collaborating with Agency CIOs, private sector experts, and international bodies to identify, prioritize, and reach consensus on standardization priorities.”

# ***Federal Cloud Computing Strategy***

## ***NIST's Role***

- “NIST will maintain a leadership role in prioritizing, developing, evolving and refining standards over time as the collective requirements for standards evolve in response to operationally driven innovation and technology evolution.”

# *Common Denominator*

- Digital Government Strategy
  - Requires standards (existing and new)
- Federal Cloud Computing Strategy
  - Requires standards (existing and new)

# ***USG Standards Mandate***

- USG law and policy requires Federal agencies to use ***international, voluntary consensus standards*** in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical.
  - Trade Agreements Act of 1979, as amended (TAA), July 26, 1979/December 8, 1994
  - The National Technology Transfer and Advancement Act (NTTAA), March 7, 1996
  - The Office of Management and Budget (OMB) Circular A-119 Revised: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, February 10, 1998
  - M-12-08, Principles for Federal Engagement in Standards Activities to Address National Priorities, January 17, 2012 (memo from three EOP offices: OSTP, OMB/OIRA and USTR)

# ***Standards Developing Organization (SDO)***

- An SDO is any organization that develops and approves standards using various methods to establish consensus among its participants.
- Such organizations may be:
  - accredited (e.g., ANSI-accredited [IEEE](#) or INCITS or NIST ITL)
  - international treaty-based (e.g., ITU-T or ICAO)
  - international private-sector based (e.g., ISO/IEC, [IEEE](#))
  - an international consortium (e.g., OASIS or IETF or W3C)
  - a government agency (e.g., DoD or DHS or NIST)

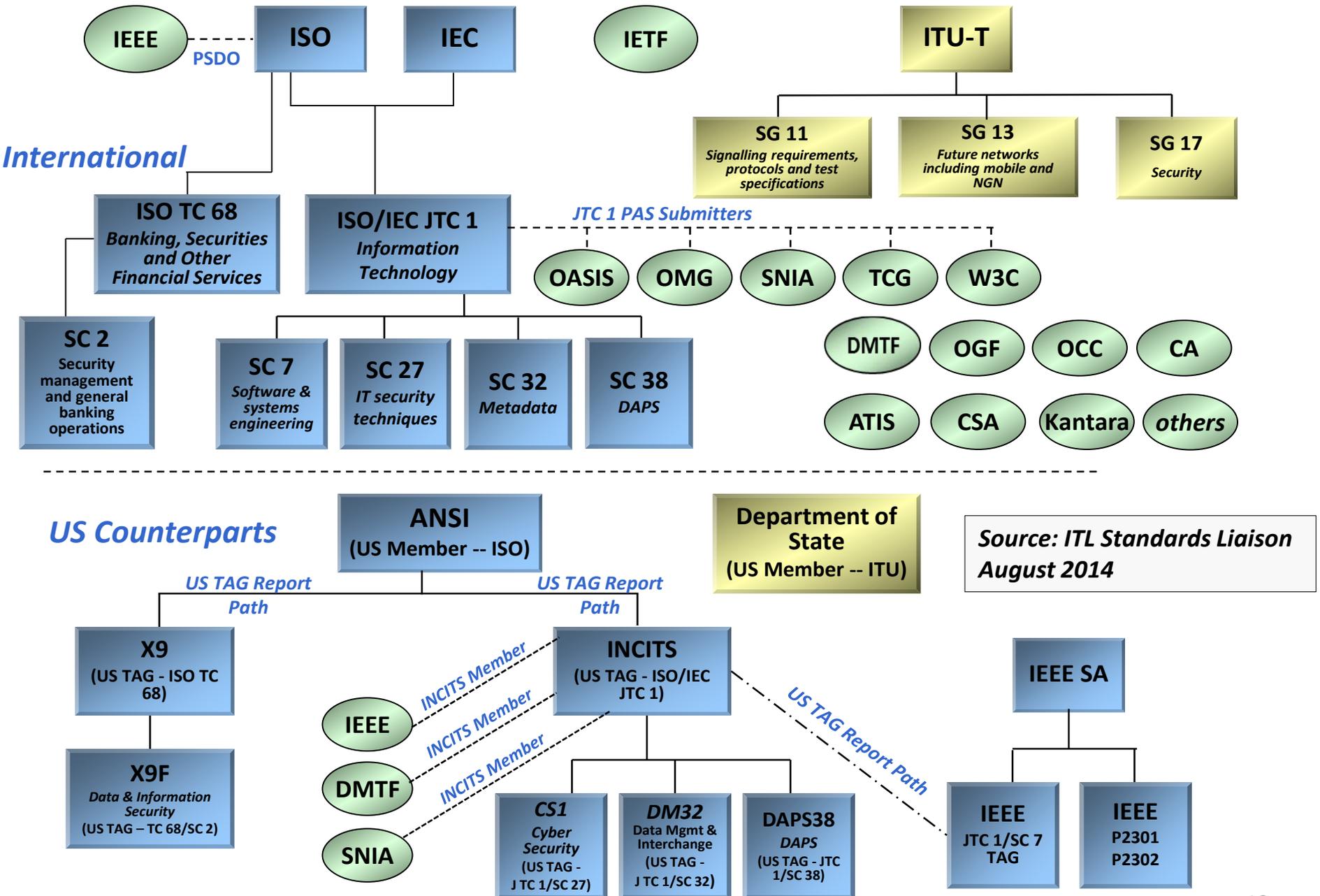
# ***ICT Standards Environment Complex, Dynamic, Darwinian***

- Providers and consumers of ICT products, processes, services, and systems rely on standards.
  - Company (sometimes proprietary) standards
  - Voluntary consensus standards (openly available)
  - Open source
- What combination of the above can best solve a stakeholder's needs is a complex issue.
- Due to ICT innovation, such solutions are a moving target.

# ***ICT Standards Environment Complex, Dynamic, Darwinian***

- *National Cooperative Research Act of 1984* provided coverage for joint research and development, which includes developing standards.
- As a consequence, where there was once about 25 SDOs involved in ICT standardization in the 1970s, there are now over 200 SDOs worldwide developing ICT standards.
  - CEN Survey of ICT Standards Fora and Consortia; July 12, 2010

# Some Key Cloud Computing Standards Developers



Key: PSDO = Partner Standards Development Organization; PAS = Publicly Available Specification; TAG = Technical Advisory Group

# ***NIST Cloud Computing Public Working Groups***

<http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome>

- Public Working Groups have been established by the NIST Cloud Computing Program to pursue its goals for accelerating the adoption of cloud computing through a combined public-private effort.
- Participation in a Public Working Group is open and free to all interested parties; there are no membership fees.
- The products of Public Working Groups prepared at the direction of NIST staff and/or its designated representatives are subject to NIST review and are intended for public release at NIST's discretion.
- Collaboratively authored documents from the Public Working Groups may become contributions to cloud computing standards projects in various SDOs.

# ***NIST Cloud Computing Public Working Groups***

<http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome>

- Business Use Cases
- Reference Architecture and Taxonomy
- Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC)
- Cloud Security
- Cloud Forensic Science
- Standards Roadmap
- Cloud Accessibility
- Cloud Services *new*
- Cloud Interoperability *new*
- Cloud Federated *new*

# ***NIST Cloud Computing Standards Roadmap***

[http://www.nist.gov/itl/cloud/upload/NIST\\_SP-500-291\\_Version-2\\_2013\\_June18\\_FINAL.pdf](http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf)

- NIST Special Publication 500-291 version 2, NIST Cloud Computing Standards Roadmap, July 2013
- Specific recommendations regarding engagement between federal agencies and SDOs are:
  - Recommendation 1 – Contribute Agency Requirements
  - Recommendation 2 – Participate in Standards Development
  - Recommendation 3 – Encourage Testing to Accelerate Technically Sound Standards-Based Deployments
  - Recommendation 4 – Specify Cloud Computing Standards
  - Recommendation 5 – USG-Wide Use of Cloud Computing Standards

# ***NIST Cloud Computing Standards Roadmap***

[http://www.nist.gov/itl/cloud/upload/NIST\\_SP-500-291\\_Version-2\\_2013\\_June18\\_FINAL.pdf](http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf)

- Cloud computing relevant standards have been mapped to the USG requirements of accessibility, interoperability, performance, portability, and security.
- High priorities for standardization:
  - SaaS application specific data and metadata format standards to support interoperability and portability requirement when migrating high-value, low-risk applications to SaaS
  - Resource description and discovery standards to support data center consolidation using private and community IaaS cloud systems
  - Security auditing and compliance standards to support secure deployment, assess, and accreditation process for cloud-specific deployment
  - Identity and access management standards to support secure integration of cloud systems into existing enterprise security infrastructure

# Standards Proliferation

HOW STANDARDS PROLIFERATE:  
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)



Source: xkcd.com

See: <http://xkcd.com/927/>

**NIST**

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

# Standards Maturity Model

## NIST Special Publication 500-291

No Standard	SDOs have not initiated any standard development projects.
Under Development	SDOs have initiated standard development projects. Open source projects initiated.
Approved Standard	SDO approved standard is available to public. Some SDOs require multiple implementations before final designation as a “standard”.
Reference Implementation	Reference implementation available
Testing	Test tools are available. Testing and test reports are available.
Products/Services	Standards-based products/services are available.
Market Acceptance	Widespread use by many groups. De facto or de jure market acceptance of standards-based products/services.
Sunset	Newer standards (revisions or replacements) are under development.

# ***NIST Participation in Cloud Standards***

## ***ISO /IEC JTC 1/SC 38***

- ISO/IEC 17788: 2014, Information technology -- Cloud computing -- Overview and vocabulary (ITU-T Y.3500)
- ISO/IEC 17789: 2014, Information technology -- Cloud computing -- Reference architecture (ITU-T Y.3502).
- ISO /IEC *Working Draft* 19086, Cloud Computing - Service Level Agreement Framework and Terminology
- Newly approved projects:
  - Data and their Flow Across Devices and Cloud Services
  - Interoperability and Portability

# ***NIST Participation in Cloud Standards***

## ***ISO /IEC JTC 1/SC 27***

- *ISO/IEC Committee Draft 27017*, Code of practice for information security controls for cloud computing services based on ISO/IEC 27002
- *ISO/IEC Draft International Standard 27018*, Code of practice for data protection controls for public cloud computing services
- *ISO/IEC Working Draft 27036-4*, Information security for supplier relationships – Part 4: Guidelines for security of cloud services
- *ISO/IEC Draft International Standard 27040*, Storage security

# ***NIST Participation in Cloud Standards***

## ***IEEE***

- P2301 - Guide for Cloud Portability and Interoperability Profiles (CPIP)
- P2302 - Standard for Intercloud Interoperability and Federation (SIIF)

***To find information on the NIST Cloud  
Computing Program ...***

# ***NIST Cloud Computing Program***

***<http://www.nist.gov/itl/cloud/>***

- Cloud Collaboration Site Information
  - NIST Cloud Computing Public Working Groups
- NIST Cloud Computing Related Publications
  - NIST Special Publication 500-291 version 2, NIST Cloud Computing Standards Roadmap, July 2013
  - NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture, September 2011
  - NIST Special Publication 500-293, US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume I High-Priority Requirements to Further USG Agency Cloud Computing Adoption, November 2011
  - Etc.
- Events; Points of Contact; etc.