Technological Advisory Council

Spectrum Frontier Working Group

13 June 2013

Charter

- Looking to the future, what spectrum bands have the potential to become the new “beachfronts”?
- What technical or policy changes will be needed to make this realizable?
- What time frame might be anticipated in making this happen?

Working Group Members

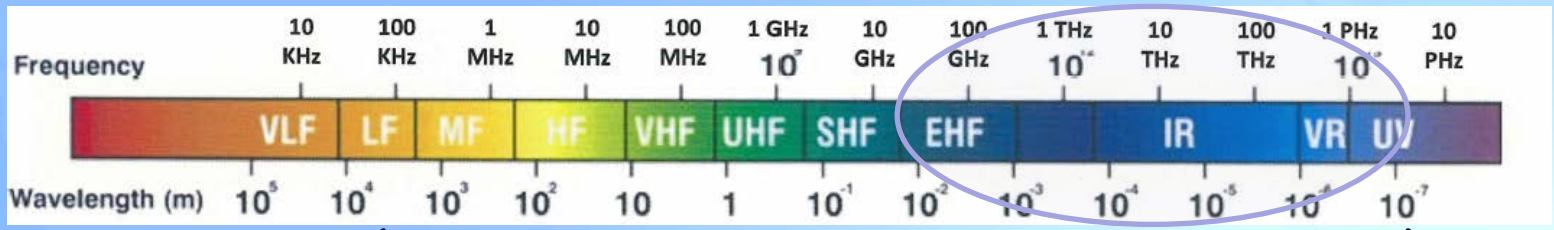
- WG Chair: Brian Markwalter
- FCC Liaisons: Michael Ha, John Leibovitz
- WG Members:
  - Ed Chan, Verizon
  - John Chapin, DARPA
  - Lynn Claudy, NAB
  - Marty Cooper, Dyna LLC
  - Adam Drobot, OpenTechWorks
  - Milo Medin, Google
  - Paul Steinberg, Motorola Solutions
  - Shahid Ahmed, Accenture
  - Dale Hatfield, Silicon Flatiron
  - Mark Richer, ATSC
  - Mark Bayliss, Visual Link Internet
  - Jesse Russell, incNetworks
  - Marvin Sirbu, Carnegie Mellon University
  - David Tennenhouse, Microsoft
  - Brian Daly, AT&T

Agenda

- Innovations enable more efficient use of current spectrum and often allow utilization of higher frequencies with reasonable economics
  - Smart Antenna Technology is a good example

- This presentation explores:
  - Overview of Higher Frequency Bands for broadband
  - Key FCC Allocations in mmW Bands
  - Mobile Broadband Applications in lower mmW Bands
  - License Status in 20/30GHz
  - Experimental License Status in mmW Bands
  - Future Investigations and Policy Considerations

Spectrum Chart



Cheaper terminals
Building Penetration
Longer Range

Smaller antenna arrays
Blocked/Reflected by Walls
Shorter Range

Major Areas of Focus

- Mobile Broadband at 30GHz
- 60GHz Unlicensed/ISM
- 100-300GHz mmW
- IR/Terahertz/Li-Fi

Key FCC Allocations of Millimeter Wave (30-300 GHz)

	Rules	Bands	Below 100GHz	100 GHz - 1000 GHz
Fixed Microwave	Part 101	31-31.3GHz, 38.6-40GHz, 71-76GHz, 81-86GHz, 92-94GHz, 94.1-95GHz	14.6 GHz	
RF Devices	Part 15	45.5-46.9GHz, 57-64GHz, 76-77GHz, 92-95GHz	12.4 GHz	
ISM Equipment	Part 18	59.3-64GHz, 116-123GHz, 241-248GHz	4.7 GHz	14 GHz
Private Land Mobile	Part 90	33.4-36GHz	1.6 GHz	
Satellite Communications	Part 25; mostly space-to-earth	37.5-40GHz, 40-42GHz	4.5 GHz	
Aviation	Part 87	32.3-33.4GHz	1.1 GHz	
Amateur	Part 97	47-47.2GHz 77-81GHz, 122.25-123GHz, 134-141GHz, 241-250GHz, 275-1000GHz	4.2 GHz	741.75 GHz

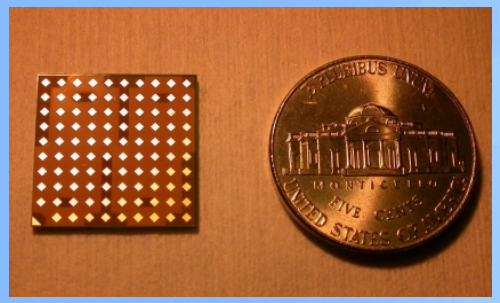
24/29/39GHz License Status

	24 GHz	LMDS (27.5-31.2 GHz)	39 GHz
Bandwidth	400 MHz	1,300 MHz	1,400 MHz
Licenses in FCC Inventory	873	480	1,259
Licenses Under Review	+102	+216	+365
Licenses Potentially Available	= 975	= 696	= 1,624

- They represent more than 99% of the 24 GHz EA licenses, 70% of the LMDS BTA licenses and 66%of the 39 GHz EA licenses. Note that these numbers do not translate into percentage of populations being reached.
- Note that EU and some Asian countries have Fixed and/or Mobile allocations in 27-29GHz but not harmonized.
- Further study needed to understand reasons for license returns

mmW Mobile Broadband Communications

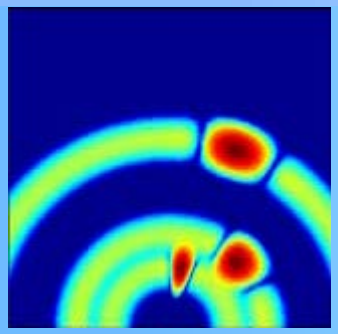
- Spectrum characteristics are suitable for short-range use
- Many countries (USA/ITU/EU) have pockets of fixed/mobile allocations in mmW band; international harmonization is still required
- Mobile use requires steerable antenna systems, which are becoming available
- May be suitable for urban mobile applications at up to Gbps data rates
- Research at various frequencies going on now
- May 2013, Samsung announced mobile broadband technology at 30GHz band and briefed our working group on progress to date



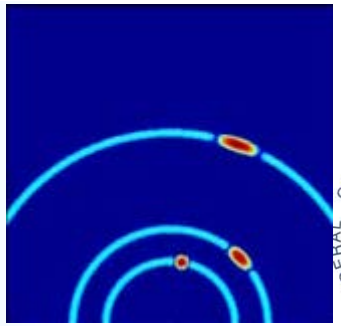
IBM mmW 90-94GHz transceiver with integrated 8x8 array of antennas (EETimes)

mmW Spectrum Applications

- 57 – 64 GHz
  - Unlicensed high-speed data links (point-to-point)
  - Wireless HDMI
- 28 / 79 GHz radar
  - Used for parking assistance, blind spot detection, collision avoidance, automatic cruise control
  - Systems use wide bandwidth (4 GHz – 5 GHz) for better performance
  - Radar is allowed in the US at 23-29 GHz and 76-77 GHz
  - 77-81 GHz is allowed in 48 countries;
    petition filed to align US with international policy



Wider bandwidth means tighter resolution when finding cars & pedestrians



30~275GHz mmW Band Experimental License Status*

Bands (GHz)	Pending	Expired	Granted/ Active	Dismissed	Total
30-80	15	736	92	103	946
80-120	3	156	23	34	216
120-275		33	2	5	40

- Lower frequencies more active than higher due to challenges at 100GHz+
- Shows that there is a big leap between Experimental License and “viable commercial market”
- A process is in place to support experimental licenses for upper frequencies

* Includes application types of Assignment, Modification, New, Renewal, STA and Transfer of Control.

Further Investigation

- IR/Terahertz/Li-Fi Band Activities
- Smart antenna technologies can offer improved spectral efficiency and are useful for extending range at higher frequencies. Current FCC rules are suitable for static transmitters and further study is recommended to exploit the benefits of antennas with dynamic beam forming.
- Potential to make a national solution with mmW mobile (short range, high capacity) in urban regions supplemented by UHF mobile (long range, lower capacity) elsewhere

Policy Considerations

- How can we accelerate the adoption of higher frequencies to become the next beach front spectrum?
- Spectrum made available requires an ecosystem to be commercially competitive.
- International harmonization is also a key driver of economies of scale
- Given the trend to incorporate an increasing number of radios in user equipment, are policy changes needed to ensure that this practice can continue beyond the UHF band?

Technological Advisory Council

Wireless COTS Working Group

Table of contents

- COTS working group members
- Workgroup Status
- Mission statement
- Objective and Approach
- Schedule/Next Steps
- COTS working definition
- COTS deployment scenarios

COTS working group members:

Name	Company	
Shahid Ahmed	Accenture	Workgroup Chair
Mark Bayliss	Virginia ISP Association	
Nomi Bergman	Bright House Networks	
Ed Chan	Verizon Wireless	
Diane Wesche	Verizon Wireless	
Greg Chang	YuMe, Inc.	
Brian Daly	AT&T	
Kevin Kahn	Intel Corporation	
Jack Nasielski	Qualcomm Inc.	
Jesse Russel	incNetworks	
Paul Steinberg	Motorola Solutions	
Bruce Oberlies	Motorola Solutions	
Glen Tindal	Juniper Networks	
Douglas Smith	Oceus Networks	
Kevin Stiles	Oceus Networks	
Jesse Russell	uReach	
Walter Johnston	FCC Laison	

COTS Working Group Mission Statement

Find ways to leverage technical and commercial benefits of scaled wireless solutions to:

1. Lower cost of entry for wireless applications
2. Accelerate deployment of wireless solutions
3. Limit necessity for application/sector specific spectrum allocations
4. Increase sharing of scarce spectrum and network resources
5. Increase overall spectrum efficiency

Work Group Status

- Identified specific companies/sectors to interview
- Defined COTS deployment scenarios
- Scheduling interviews/discussion with sector stakeholders
- Will identify COTS potential and useage issues

Objective

Start off with collecting empirical data from industry interviews to determine lessons from industries where COTS has worked and focus on 2-3 specific use-cases where COTS is a common platform. Some examples include: Use of LTE for Military, Public Safety and Smart Grid and Network Sharing (both physical and virtual)

Approach

Create Interview Target List and Questions

- CBP/ DOD - Gov
- Utility Telecom Council
- Qualcomm - CMT
- Samsung - CMT
- FirstNet - Gov
- OnStar- CMT
- Caterpillar - Transportation
- Nest
- Stanford Hospital – Health Care

Conduct Company Interviews

- Discuss 2 to 3 Use Cases
- Seek input from industry leaders
- Discuss recommendations

Consolidate and Summarize Findings

- Consolidate findings
- Provide interim updates to the FCC TAC group

Developed Final Recommendations

- Present final COTS models and recommendations

COTS Working Definition

- Wireless equipment and systems commercially sold in significant quantity across diverse industry groups
  - Volume sales lower acquisition cost
  - Large commercial market stimulates ongoing investment in technology
  - COTS market creates further opportunities for complementary software, devices, and technologies

COTS Deployment Scenarios

- COTS platform supporting multiple enterprises
  - e.g. broadband cellular network supporting customized VPN for specific enterprise/sector
- COTS platform deployed within specific sector
  - e.g. public safety deploying LTE for first responder needs, military looking at LTE for war fighter needs
- Hybrid deployments where COTS is a part of total solution
  - e.g. domestic UAV use limited by spectrum availability; potential future air/ground broadband commercial systems could provide partial support for UAV communication needs
- Other COTS scenarios outside scope of study
  - e.g. COTS components (filters, sensors, etc.) adaptable to wide range of uses

Next Steps and Schedule:

- June to September:
  - Identify industry contacts and begin interviews/discussion
- September – November:
  - Complete 50% to 75% of interviews
  - Industry conference
- End of December
  - Complete interviews
  - Provide COTS recommendations
  - Identify key issues

Technological Advisory Council

Spectrum / Receiver Performance

Working Group

13 June 2013

Working Group Members

- Lynn Claudy
- Mark Gorenberg
- Dave Gurney
- Dale Hatfield
- Greg Lapin
- Brian Markwalter
- Geoffrey Mendenhall
- Pierre de Vries
- Matthew Hussey*
- Bob Pavlak*
- Julius Knapp*
- Dennis Roberson

* FCC Liaisons

2013 Mission Statement

- The work group will provide support as the Commission considers the TAC recommendations related to proposed interference limits policy
- The group will make recommendations in areas focused on improving access to and making efficient use of the radio spectrum from a systems perspective

Study Areas / Deliverables

1. Examination of Interference Studies including statistical analysis, OOBE, Public Notice comments…
2. Multi-stakeholder Groups
3. Assist in developing a “radio service knowledge base”
4. Investigation of emerging technologies that:
   - Improve interference measurement and mitigation
   - Enhance receiver performance
   - Foster greater spectral efficiency of devices
5. Recommendation on enforcement approaches

Interference Studies

- **Goals**

  ***Implementation of Interference Limits Policy*:** Support the development of harm claim thresholds by providing applicable technical analysis

  Statistical Interference Risk Analysis: Make recommendations about the use of statistical risk metrics in the formulation of rules and analysis of harmful interference

- **Deliverables**
  - September TAC Meeting
    - Report on harm claim threshold implementation in TBD case
    - Review of the current use of statistical techniques and harm metrics
  - December TAC Meeting
    - Recommendation on statistical metrics for formulating harm claim thresholds
    - Recommendation on use of statistical risk assessment by FCC

Interference Limits Implementation

- **Context**
  - Last year principles were established and examples given
  - Next step is to drill down on details
- **Topics**
  - Infer harm claim thresholds from coexistence studies and operating parameters for existing systems
  - Study the use of measurement and/or modeling to determine harm claim thresholds during rulemaking, and in dispute resolution
  - Make recommendations about the use of statistical metrics in the formulation of harm claim thresholds

Statistical Interference Risk Assessment

- **Context - Risk = probability x severity**
  - Most analyses to date have focused on **severity** of worst case, and **excluded probability**
- **Topics**
  - Review the use of statistical techniques and harm metrics
    - By FCC and other radio regulators
    - In standards development, deployment & dispute resolution
    - In other regulated industries
  - Compare and contrast statistical vs. worst-case risk analysis
  - Make recommendations re interference analysis in rulemaking and enforcement

Multi-stakeholder (MSH) Organizations

- Characteristics of MSH approach
  - Group of diverse interests that come together to achieve a common purpose that typically cuts across natural industry boundaries
  - Appropriate role for government participation may vary widely
- MSH approach is successfully used in Internet governance context [e.g., ICANN (IP addresses), IETF (Internet standards), W3C (best practices for Internet governance), BITAG (Internet-related network management issues)]
- Basic Question: Can an MSH process as described in the TAC White Paper be successfully used to establish harm claim thresholds given that spectrum stakeholders are apt to be competitors?

Multi-stakeholder (MSH) Organizations

- Subsidiary Questions: (a) Can well defined, quantitative goals be developed? (b) What is the governance template for such a group? (c) How can trust / collaboration be developed among participants? (d) What resources need to be available / who should supply them? (e) What is the proper role for the FCC in the MSH group? (f) Are there other challenges associated with federal government users participating in the group? (g) Would a pilot program be useful to test the concept? (h) What frequency band(s)?
- Deliverables
  - September TAC Meeting
    - Compare and contrast MSH and other regulatory approaches
    - Explore levels of increasing guidance from the MSH as outlined in White Paper
    - Scenario descriptions for MSH use at candidate band/allocation boundaries
  - December TAC Meeting
    - Recommendation for governance template(s) for interference limits MSH
    - Recommendation for specific allocation boundary where MSH could be used to develop interference limits

Radio Service Knowledge Base

Goal: To enable equipment and system designers to plan to avoid potential adjacent channel interference as well as other nearby in-band and out-of-band interference sources

Product - Provide a publicly-accessible resource to help designers determine:

- What RF services they can expect to find in spectrum adjacent to their allocation
- Data to predict in-band / out-of-band signal levels the receivers must cope with
- Specific references to design standards and spectral performance of the types of transmitters and receivers in the nearby/adjacent spectrum

Challenges - Defining all types of RF services

- Some services operate differently in different bands
- Many bands have numerous standards (e.g., ISM), or proprietary services

Radio Service Knowledge Base

Challenges (cont.):

- Not all RF emitting devices have industry standards
- FCC databases have useful information for proactively avoiding interference
  - However, license data were not intended to include all information needed to proactively avoid interference between radio services
  - Independent frequency managers may develop band plans and assign specific frequencies and channels for many radio services
  - Licensees may hold relevant information that is proprietary, *e.g.*, radio site locations for geographic (market-based) licenses
  - Some radio services, e.g., in Part 95, Part 15, are not site-based or specific to individual users or organizations

Deliverables:

- September TAC: Gap analysis report on radio service types and availability of desired information for avoiding interference between radio services
- December TAC: Identify references to industry knowledge sources

Emerging Technologies

Goal: To investigate receiver and transmitter design techniques that improve efficient use of the spectrum

Product: Develop list of techniques being researched that show promise in improving spectrum efficiency often by increasing interference tolerance

Deliverables:

- September TAC Meeting:
  - Cost, Performance, Power Consumption and Over-the-Air Updatability of Current SDR Technologies
- December TAC Meeting
  - White paper on emerging technologies
  - Report on policy issues affected by emerging technologies

Emerging Technologies

Findings to Date:

- Techniques that mitigate co-channel and adjacent channel interference:
  - Full duplex operation on a single channel:
    - Transmit signal cancellation using multiple phase-related, diverse, antennas
    - *A priori echo* cancellation of the transmitted signal by producing its inverse
  - Interference Cancellation:
    - Cont. Adaptive In-Band Nulling (CAIN) beam steered antennas null interferer
    - Single and Dual Antenna Interference Cancellation (SAIC/DAIC)
    - Enhanced inter-cell interference coordination (eICIC)
  - Waveforms that support multiple services coexisting in same spectrum
  - Devices provide transmit activity & received noise levels to database
- Techniques that harden receivers to resist interference:
  - Software-defined radio with direct conversion, digital filters, high dynamic range A/D
  - Front end amplifiers and mixers with increased IP3 dynamic range
  - Dynamically tunable front-end filters based on RF MEMS technology

Actionable Recommendations: Develop white paper describing emerging technologies

Interference Resolution and Enforcement

- **Motivation:** Rapidly evolving wireless system architectures and characteristics and the operation of both intentional and unintentional radiators in close proximity has changed the nature of interference risks while at the same time providing technological opportunities for more efficient and effective procedures for interference resolution and enforcement
- **Goal:** To recommend policies that would lead to the establishment of a standardized set of procedures for interference resolution and enforcement in an increasingly complex radio spectrum environment
- **Background:**
  - Opportunities exist in traditional interference resolutions step: detecting interference, locating interference sources, identifying interference sources, facilitating voluntary interference resolution and initiating and conducting enforcement actions
  - Traditional resolution / enforcement tools include call signs and related identifiers, station licenses, operator licenses, technician licensing, equipment type approval/type acceptance, equipment labeling, monitoring and inspections, educational efforts/outreach advisories, voluntary/self enforcement

Interference Resolution and Enforcement

- **Opportunities for Change (Examples):** Standardized interference incident management reporting; crowd sourcing using User Equipment (UEs) to: (a) assist in detecting, identifying and locating sources of interference and (b) routinely measuring interference and noise to "calibrate" propagation models; with appropriate privacy protection, use of UEs to record information on system/device performance and interference/noise environment in order to later identify the cause and source of interference incidents (similar to aircraft "black boxes" recorders)
- **Deliverables:**
  - September TAC Meeting
    - Deliver preliminary recommendations regarding interference resolution ("de-confliction"), enforcement programs and procedures, and methods for improving interference measurement and mitigation
  - December TAC Meeting
    - Deliver draft of final report with specific recommendations regarding new or revised enforcement strategies

Discussion

Resiliency WG

Chair: Russ Gyurek

FCC – Henning Schulzrinne

June 13, 2013

TAC Resiliency WG

How can we ensure networks are more resilient in 5, 10 & 15 years than they are today?

WG Members (24)

- Russ Gyurek- (WG Chairman)
- Ralph Brown
- Harold Teets
- Ed Chan
- KC Claffy
- Adam Drobot
- Mark Bayliss
- Dale Hatfield
- Doug Jones
- Dave Clark
- Greg Lapin
- Jack Nasielski
- John McHugh
- John Barnhill
- Mark Bregman
- Marvin Sirbu
- Brian Daly
- Paul Steinberg
- Glen Tindal
- Charlie Vogt
- Brian Fontes
- Vish Nandlall
- Joe Wetzel
- Henning Schulzrinne (FCC)

Premise

- Recent natural disasters show the importance for network resiliency of access and, to a lesser extent, backbone networks
- WG to discuss both natural and man-made disasters
  - small scale & catastrophic
  - natural disaster, accident (back hoe), intentional (terrorism), cyber attack
- All kinds of access networks:
  - residential and small business copper, coax, and fiber
  - cellular wireless
  - trunked radio
- But also supporting services (BGP, DNS, DHCP, …)
- Deliverable: White paper by Dec. 2013
  - With intermediate updates for Sept. & Dec. meetings

Proposed Scope

- Define ***resiliency*** as it applies to communications networks (cable, wireless, landline, …)
- Focus on:
  - Disasters: avoidance, recovery, substitution
  - Virtual (cyber attacks): avoidance & recovery
    - Liaison opportunity with Communications information security WG
- WG to focus on "distribution" part of network
  - Rationale: there is redundancy in core
- Traffic prioritization review and investigation of current status
  - Voice and data
- Specific issues for rural infrastructure

Merriam-Webster Definition: Resiliency

- *an ability to recover from or adjust easily to misfortune or change*
- *an occurrence of rebounding or springing back*
- *the physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit*

Proposed Actions/Deliverables-1

- Whitepaper:
  - define resiliency for telecom
  - define use cases for resiliency
  - disruption & redundancy in distribution networks
  - review of traffic prioritization to address traffic congestion – current practice & possibilities
  - expedited plant repairs in event of disaster
  - protocols to facilitate resiliency in networks - failover, multi-pathing, …
  - program proposal to evaluate impact and survivability forecasting
  - investigation of user diversification in terms of services
  - rural issues
- Investigate emergency services/public safety tie-ins

Proposed Actions/Deliverables-2

- Recommendations:
  - focus on market-driven collaboration for temporary services
  - OSP disaster avoidance practices
  - how to improve speed of recovery/response time (e.g., coordination with electric utilities)
  - gov't reporting
- Incentive & government programs for temporary restoration of services (e.g., portable telecom container)
- Explore measurements & metrics
  - Leverage existing FCC data to focus on MTTF/MTTR
  - How to design for survivability. Explore whether FCC can perform analysis with time-line data.

Next Steps

- Form sub-groups within WG to focus on main areas
- Liaison with FCC on existing resiliency data
- Liaison with Security team, and emergency services
- Weekly/regular sub-group meetings
- Regular all-hands meetings to share data
- Start whitepaper outline immediately
- Sept. TAC: Present draft whitepaper and draft recommendations
- Dec. TAC: Present formal whitepaper and actionable recommendations

Comments and Feedback

Resiliency WG

Back up slides

- Network protocols
  - Can network protocols be designed to be more robust?
  - Can multipath BGP and TCP help?
- Implementation
  - How can providers facilitate multi-homing for residences and businesses?
  - New backup power solutions?
    - e.g., solar, fuel cells?
- Topology
  - How can access network topologies be designed cost-effectively to avoid single points of failure?

- Measurement
  - What is the reliability of IP and VoIP services during normal operation?
  - How can we estimate resiliency ahead of major events?
- Recovery
  - How can we accelerate recovery?
    - Quick ways to restore power?
    - Add other backhaul technologies?
  - How can we maintain situational awareness?
    - User-based measurements?
    - Measurement infrastructure?

- Substitution
  - When the main network is temporarily unavailable, what substitutes can be made available quickly?
    - e.g., mesh networks backed by satellite?
  - What services have the highest priority?
    - What communication services can facilitate overall recovery?
    - e.g., basic text messaging? Low-rate IP connectivity?

Communications Infrastructure Security

Chair: Paul Steinberg
Vice Chair: Adam Drobot
FCC Liaisons: Greg Intoccia, Ahmed Lahjouji

Mission Statement

The evolution of the nation's communications infrastructure towards a broadband IP-based network is occurring at an ever faster rate. This evolution includes an environment in which cloud based services are increasingly relied upon as substitutes for desktop applications, and even network services, and where attributes such as mobility, identity, and presence influence both the ability to access data as well as the context in which data may be presented.

- In an emerging era where consumers and business rely upon cloud services for critical functions, what are the key areas of concern for security?
- How cloud infrastructure and service providers best develop awareness of these issues and ensure that the ongoing evolution incorporates industry best practices, ensuring adequate protection for critical services?

Mission Statement Key Objectives

- What are the top ten security concerns, and are there any ”low hanging fruit” solutions?
- Who are the key cloud computing standards groups?
- What, if any, collaborative activities with industry, government, and academic organizations focus on cloud computing security?
- What is the security gap between what is needed and what is available or offered by cloud providers?
- What role could the FCC play in facilitating positive changes in the security of cloud computing market?

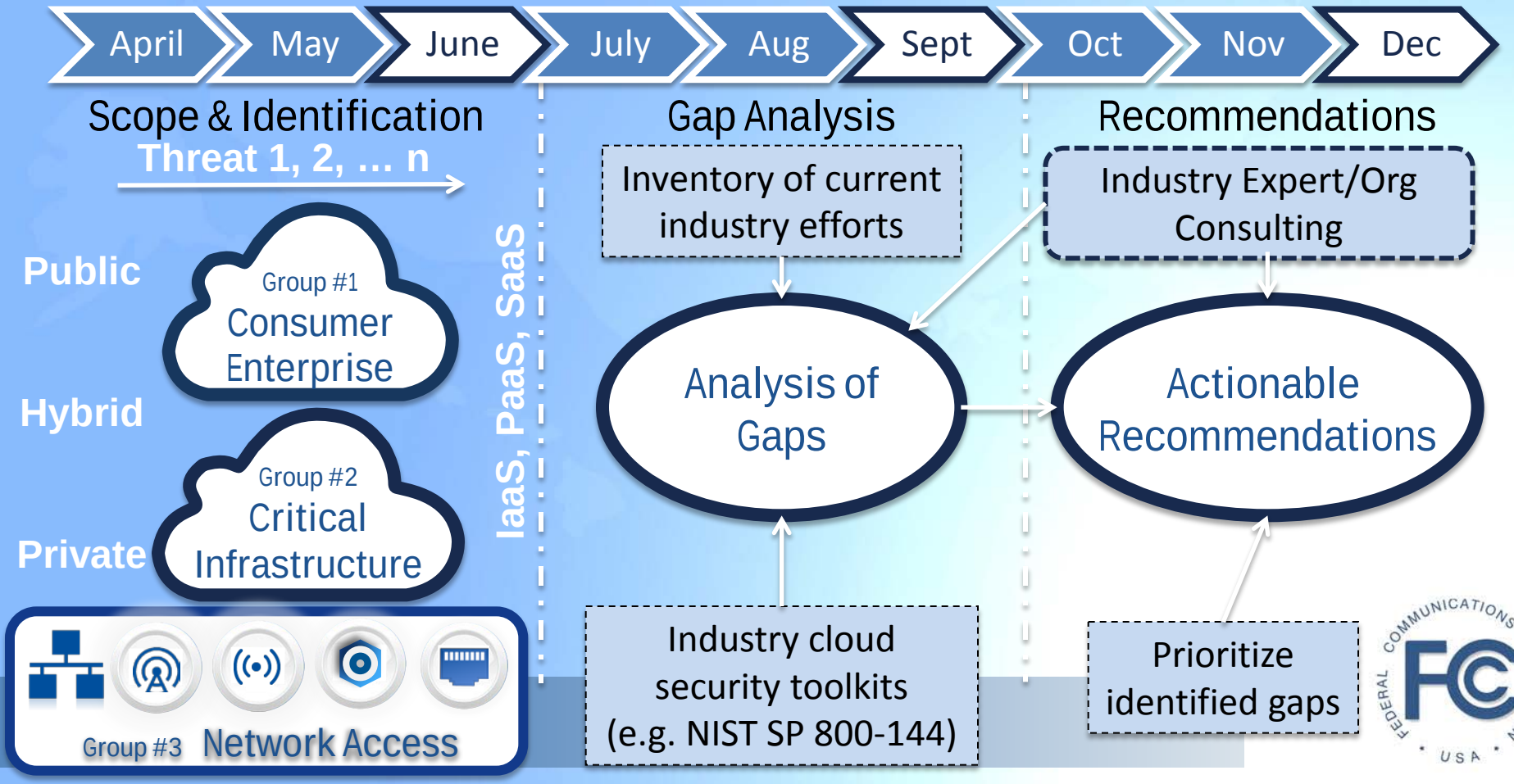
Working Group Members

- WG Chair: Paul Steinberg, Motorola Solutions
  Vice Chair: Adam Drobot (OpenTechWorks)
- FCC Liaisons: Greg Intoccia, Ahmed Lahjouji
- Members:
  - John Barnhill, GENBAND
  - Mark Bayliss, Visual Link Internet
  - Peter Bloom, General Atlantic
  - Dick Green, Liberty Global
  - John Howie, Cloud Security Alliance (TBC)
  - John McHugh, NTCA
  - Mike McNamara TWTelecom
  - S. Aon Mujtaba, Apple
  - Deven Parekh, Insight Partners
  - G. (Ramani) Pandurangan, XO Communications
  - George Popovich, Motorola Solutions
  - Jesse Russell, incNetworks
  - Harold Teets, TWTelecom
  - David Tennenhouse, Microsoft
  - Donald Tighe, Verizon
  - Charlie Vogt, GENBAND
  - Joe Wetzel, Earthlink

Work Group Progress Summary

- Established Scope, Landscape, and Vernacular
- Met with CSA to Review Cloud Security Current Issues including the "Notorious Nine"
- Established 3 sub-groups
  - Consumer/Enterprise, Public Cloud Topologies
    - Leader: Joe Wetzel, with Mark Bayliss, Peter Bloom, Dick Green, Deven Parekh, Jesse Russell and David Tennenhouse
  - Critical Infrastructure, Private Cloud Topologies
    - Leader: George Popovich, with Adam Drobot, and Paul Steinberg
  - Network Access
    - Leader: Harold Teets
    - Members: John Barnhill, John McHugh, Mike McNamara, Donald Tighe, Joe Wetzel
- Developed
  - Initial Assessment of 3 Focus Sub-group Areas
  - Overview of Cloud Security initiatives (Landscape)

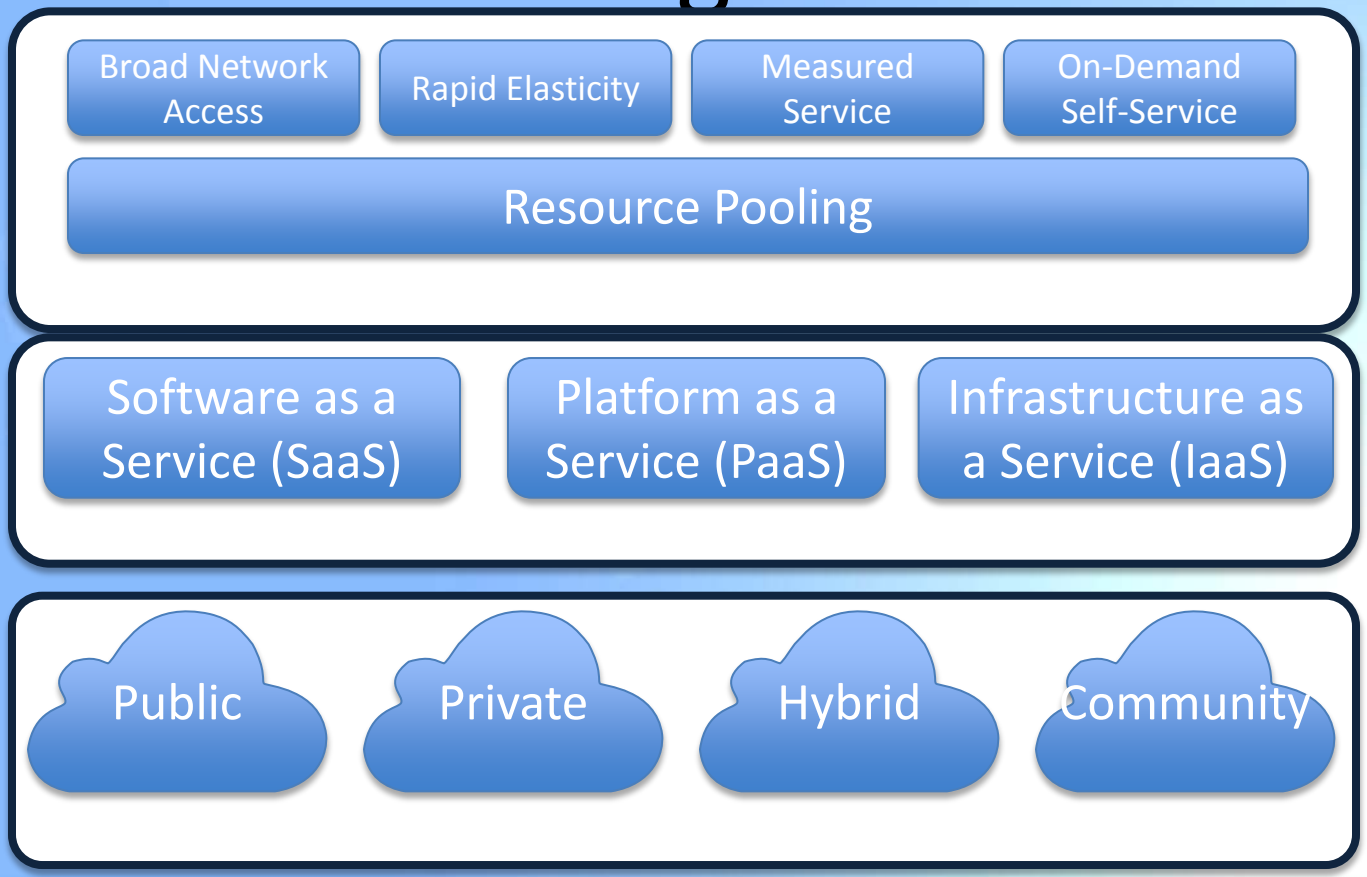
2013 Work Group Plan



Work Group Analysis Points

- Top security areas of concern for each (Starting point Notorious Nine)
- Relevant standards groups for each
- Potential collaborative activities for each
- Additional expertise (and candidate sources)

Defining the Cloud: NIST



Essential Characteristics

Service Models

Deployment Models

http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Observations of the State of Cloud Security

John Howie (COO of CSA)

CSA is a non-profit consortium. Consists of cloud solution providers & enterprises (cloud customers). The CSA is not a lobbying group – it's goal is to provide objective information.

- Recent focus: Big Data, Mobile Devices, Security_aaS
  - CSA guided by NIST documents (SP 500-292. Cloud Ref Arch), 800-144, 800-145
  - Cloud providers are contemplating the future, with regard to regulations
  - The "Notorious Nine" list is viewed as a compilation of general threats to established cloud users
  - Top 5 barriers to cloud adoption: 1) availability, 2) standards compliance, 3) confidentiality & privacy, 4) supply chain concerns, 5) how to get out (e.g. switch providers)

Industry Acknowledged Threats

The CSA "Notorious Nine"

- Data Breach
- Data Loss
- Account Hijacking
- Insecure APIs
- Denial of Service
- Malicious Insiders
- Abuse of Cloud Services
- Insufficient Due Diligence
- Shared Technology Issues

John's Suggested TAC Focus Areas:

- Cloud auditors: currently the industry self-regulates
- Is the cloud considered critical infrastructure? It's a difficult question to answer
- Hole at the cloud carrier level is availability – we need x9s in SLAs
- Network access is a big issue
- Recommend potential investigations around secure methods like scalable DNS Security Extensions, Border Gateway Protocol Security, Improved Payment Card Industry Data Security, Extended Validation digital certificates

Landscape of Cyber Security Organizations

Extensive Global Engagement, Extensive Documentation and Knowledge

US Government
Including Federal, State, Local

FEDRAMP, NIST, GSA, DHS, HHS, DISA, OSDCIO, ODNICIO, FBI, NNSACTO, GCIO

Research and Academia

NITRD, NSF, CISE, DARPA, IARPA, DOE, DHS

Standards Bodies & Industry Assoc.

CSCC, OGF, ARTS, Openstack, OMG, CSA, W3C, OCC, PCISSC, Oasis, SNIA, IETF, OSLC, TM, SIIA, DMTF, TIA, IEEE, ETSI, ATIS, AICPA, GICTF, Open, Group, NDIA, ISO, MPAA

International Governments & Associations

ENISA, ERTICO, EURESCOM, TWCloud, IDA, EDB, etri, MPT, MPS, OGCIO_HK, ECP, ITU, SECCRIT

Partial List. More Detail included In Backup materials

Common Building Blocks & Threats

Threats

- Identification and Mitigation
  - Public: DoS, DDoS, DNS spoofing, IP spoofing, BGP
  - Private: compromise from within
  - Community of Interest: Multiple risks
- Threat Classifications
  - Confidentiality - Data Loss, Breach, Phishing
  - Integrity - Account Hijacking, Insecure API, Hacking, BYOD, USB Keys
  - Availability - DoS, DDoS

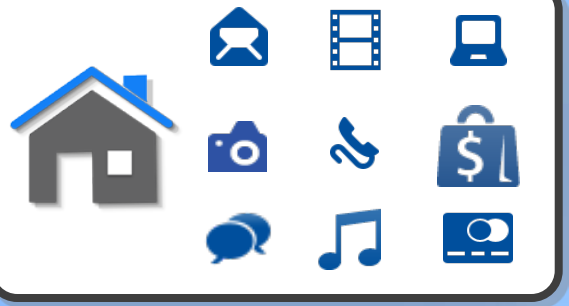
Grp #1: Consumer & Enterprise /Public Cloud

Cloud Use Cases

Threats

Controls

Consumer



Enterprise

- Governance
- Compliance
- Audit
- Access Mgmt
- Identity Mgmt
- Encryption

Grp #2: Critical Infrastructure / Private Cloud

DHS definition of critical infrastructure

- **42 USC § 5195c** (e) **Critical infrastructure defined**
  …**"critical infrastructure"** means **systems** and **assets***(and **networks**)*, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a **debilitating impact** on security, national economic security, national public health or safety, or any combination of those matters.
- Critical infrastructure is the backbone of our nation's economy, security and health. We know it as the **power** we use in our homes, the **water** we drink, the **transportation** that moves us, and the **comm. systems** we rely on to stay in touch with friends and family.

Top security areas of concern, beyond CSA's "The Notorious Nine"

- Cyber-terrorist threats where the goal is service disruption, threat to human life
- Sophisticated, multi-pronged, long term, nation-state attacks
- Disruption of first responder communications
- Concerns over lack of logical redundancy within clouds (e.g. same SW everywhere)

Grp #2: Critical Infrastructure / Private Cloud

Potential collaborative activities

- Leverage CSA involvement with the TAC
- Reach out to ENISA for consulting, information sharing
- Contact NIST for potential collaboration
  - The "Improving Critical Infrastructure Cyber security" executive order is triggering NIST to work with industry to develop a voluntary framework to reduce cyber security risks to the nation's critical infrastructure

Additional expertise (and candidate sources)

- Smart Grid related activities
  - The Smart Grid Interoperability Panel (SGIP) has been looking at smart grid security over the last several years
  - One major output of SGIP's efforts has been the Smart Grid NISTIR 7628 cyber security document, which provides guidelines for securing the smart grid against cyber attacks
  - More recently, the SGIP created the Smart Grid Security Cloud Working Group
  - It seeks to recommend options that can vastly simplify the task of managing and securing the cloud

Grp #3: Access Vulnerability

- Private Network
  - Apps On or Off Premise, Managed Access & Devices
- Community Network
  - Shared Apps & Access, Causing Increased Vulnerabilities
- Public Internet
  - Un-Managed Access
  - Managed or Un-Managed Devices

Dealing with The Basics

- Access
  - Authentication
  - Authorization
  - Accounting
- Availability – have a Business Continuity/Disaster Recovery plan to cover physical/logical security
- Data Protection – encryption for data in motion and at rest

2013 Action Summary

April | May | June | July | Aug | Sept | Oct | Nov | Dec

Scope and Identification

- Develop overview of Cloud Security
- Organize Workgroup to address threat types
- Summarize industry initiatives, standards and stakeholders
- Reach out to Industry Experts to gain expertise and background

Gap Analysis

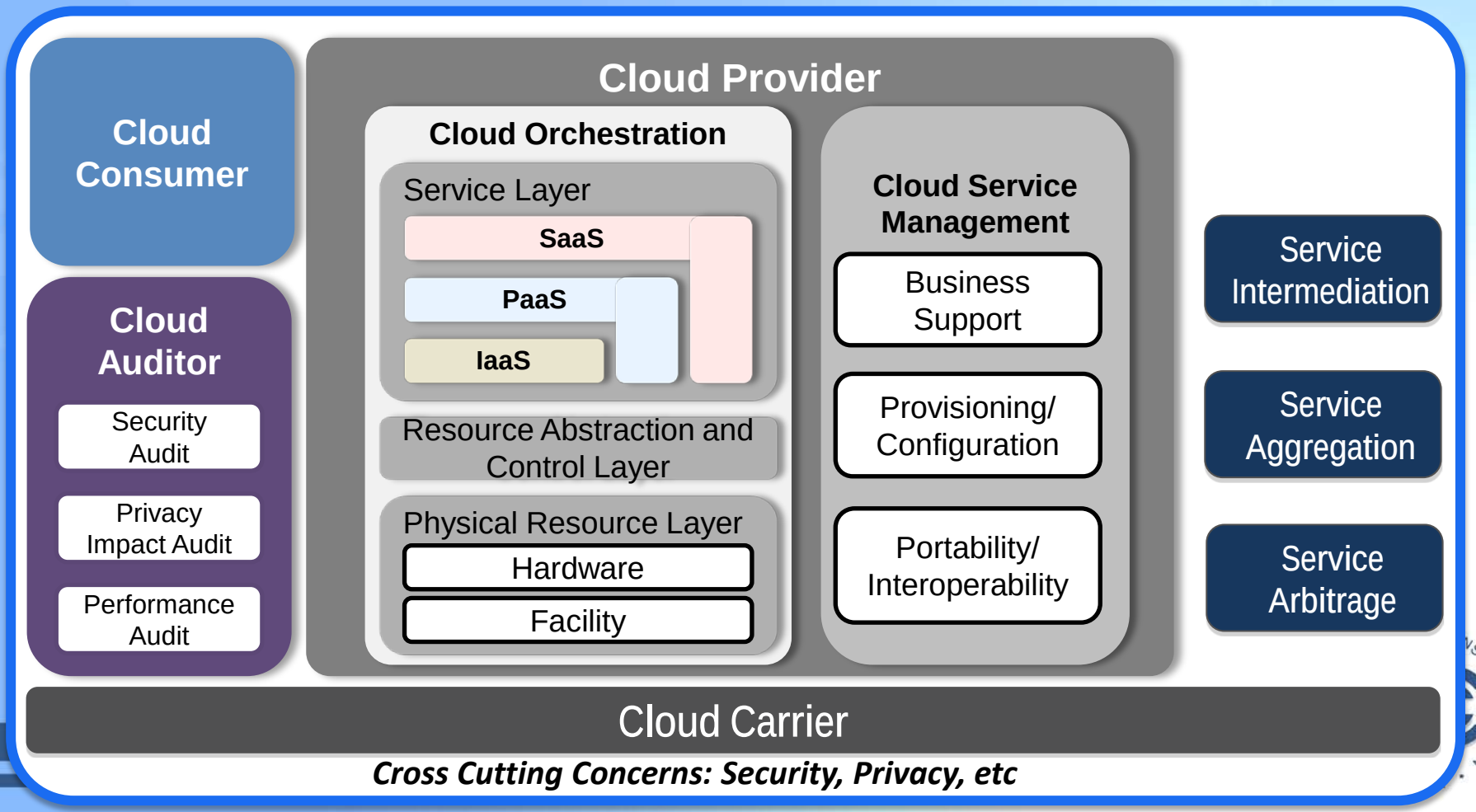
- Evaluate Threats and assess current actions.
- Narrow list of threats for Focus Group analysis
- Develop Action plans for identified sub-set of potential actions
- Recruit expert bodies to further clarify issues & identify gaps / mitigation

Recommendations

- Develop Final TAC Recommendations
  - Based on selected Threats/Issue subsets
  - Specific focus on actionable and most-realistic for FCC

Additional Information

Draft NIST CC Reference Architect



Government: Operational and Capability Responsibilities

(partial list)

• Federal Risk Authorization Management Program – FEDRAMP	http://www.fedramp.net
• National Institute of Science and Technology Cloud Security Working Group - NIST	http://www.nist.gov
• General Services Administration – Cloud Computing Program Management Office	http://www.gsa.org
• Department of Homeland Security Office of Cyber-Security and Communications	http://www.dhs.com
• Health and Human Services Office of the CIO	http://www.hhs.gov/ocio/ea
• Defense Information Systems Agency - DISA	http://www.disa.mil
• Office of the Secretary of Defense Chief Information Officer – OSDCIO	http://www.osd.mil
• Office of the Director of National Intelligence Chief Information Officer – ODNICIO	http://www.dni.gov
• National Nuclear Security Agency Office of the Chief Technology Officer – NNSA CTO	http://www.nnsa.energy.gov
• Government Chief Information Officer Council	http://www.cio.gov

Government: Research Agencies (partial list)

• The Networking and Information Technology Research and Development Program	http://www.nitrd.gov
• National Science Foundation – Computer & Information Science & Engineering Directorate	http://www.nsf.gov
• Defense Advanced Research Projects Agency – DARPA	http://www.darpa.mil
• Intelligence Advanced Research Projects Agency – IARPA	http://www.iarpa.gov
• Department of Energy Office of the CIO and Office of Science	http://www.doe.gov
• Department of Homeland Security – Science & Technology Directorate	http://www.dhs.gov/st-directorate

Industry Organizations - Standards

• Cloud Standards Customer Council – CSCC	http://www.cloud-standards.org
• Openstack	http://www.openstack.org
• W3C	http://www.w3.org/community/cloud
• Organization for the Advancement of Structured Information Standards – Oasis	http://www.oasis-open.org
• Open Services for Lifecycle Collaboration	http://www.open-services.net
• Distributed Management Task Force – DMTF	http://www.dmtf.org
• European Telecommunications Standards Institute – ETSI	http://www.etsi.org
• Global Inter-Cloud Technology Forum – GICTF	http://www.gictf.jp
• Open Grid Forum – OGF	http://www.gridforum.org
• Object Management Group – OMG	http://www.omg.org
• Open Cloud Consortium – OCC	http://www.opencloudconsortium.org
• Storage Networking Industry Association – SNIA	http://www.snia.org
• Tele Management Forum – TM	http://www.tmforum.org
• Telecommunication Industry Association – TIA	http://www.tiaonline.org
• Association for Telecommunications Industry Solutions – ATIS	http://www.atis.org
• The Open Group	http://www.opengroup.org
• Association for Retail Technology Standards – ARTS	http://www.nrf-arts.org
• Cloud Security Alliance – CSA	https://www.cloudsecurityalliance.org
• PCI Security Standards Council – PCISSC	https://www.pcisecuritystandards.org
• Internet Engineering Task Force – IETF	http://www.ietf.org
• Software and Information Industry Association – SIIA	http://www.snia.org
• IEEE Cloud Computing	http://cloudcomputing.ieee.org
• American Institute of CPAs – AICPA	http://www.aicpa.org
• National Defense Industry Association – NDIA	http://www.ndia.org

International Organizations - Partial

• European Network and Information Security Agency – ENISA	http://www.enisa.europa.eu
• Intelligent Transportation Systems for Europe – ERTICO	http://www.ertico.com
• European Communications Organization – EURESCOM	http://www.eurescom.eu
• Cloud Computing Association In Taiwan	http://www.twcloud.org.tw/
• Infocomm Development Authority of Singapore – IDA	http://www.ida.gov.sg
• Singapore Economic Development Board – EDB	http://www.edb.gov.sg
• Korean Electronics and Telecommunications Research Institute	http://www.etri.re.kr
• Ministry of Posts and Telecommunications PRC – MPT	
• Ministry of Public Security PRC – MPS	http://www.mps.gov.cn
• Office of the Government Chief Information Officer, HK	http://www.ogcio.gov.hk
• European Cloud Partnership	https://ec.europa.eu/digital-agenda
• International Telephone and Telegraph Union Cloud Computing ITU-T	http://www.itu.int/en/ITU-T/jca/Cloud

Private Cloud: Relevant Standards and Industry Groups

European Network and Information Security Agency (ENISA)

- Focuses on Internet and Information Security and Collaboration in the European Union
- Critical Cloud Computing initiative (CIIP – Critical Information Infrastructure Protection)

FBI guidelines on cloud computing and Criminal Justice Information Services (CJIS)

- Recommendations for implementation of cloud computing solutions (policy and procedures)
- Relevant, for example, to controlling first responder access to federal crime databases

FedRAMP (Federal Risk and Authorization Management Program)

- US Government program for security assessment, authorization, &auditing of cloud products/svcs
- Result of collaboration with cyber security and cloud experts from GSA, NIST, DHS, DOD, NSA, OMB, the Federal CIO Council

SEcure Cloud computing for Critical infrastructure IT (SECCRIT) Consortium

- Ten companies and universities from Austria, Finland, Germany, Greece, Spain and the UK.
- Tasked with analyzing and evaluating cloud computing security risks in sensitive environments

Industry and Standards Groups (Examples)

Virtualization	Cloud Management Working Group, Dist. Mgmt Task Force, Open Virtualization Forum
Application Mgmt	DIACAP
Audit	ISO 27001, SSAE - 16
Data Mgmt	MPAA, HIPPA, FISMA
Access Mgmt	FISMA

Security Control Type

(Per NIST SP NIST SP 800-144)

- Governance
- Compliance
- Trust
- Identity & Access Mgmt
- Tenant Isolation
- Data Protection
- Availability – may be covered in another working group
- Incident Response

Cloud Essential Services

- On-demand self-service.
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured Service

Cloud Service Models

- SaaS (Software as a Service)
  - Delivers software or more specifically applications to the end user
- PaaS (Platform as a Service)
  - Delivers application environments (i.e. OS and development environments) for end users to create their own applications for their end users
- IaaS (Infrastructure as a Service)
  - Delivers virtualized resources such as virtual machines to the end user for their own OS, application environment and application services

Cloud Market Tiers

- Consumer
  - The consumer space is mainly driven by SaaS solutions
  - Cloud based identity is showing greater momentum for consumers (e.g. federated Google identities)
- Enterprise
  - More rigorous security standards
  - More stringent availability requirements
  - More complicated scenarios like BYOD must be addressed
- Government, medical, and public safety
  - Most stringent availability requirements
  - Compliance to government standards and criteria
    - E.g. FISMA and Criminal Justice Information Security (CJIS) compliance
    - HIPAA Compliance
  - Critical infrastructure is another candidate for scope inclusion

Cloud Deployment Models

- Public
  - Cloud provider is external to the customer
  - Multiple, independent customers supported by the cloud provider
  - Consumer facing clouds fit into this category
- Hybrid
  - A mix of more than one deployment type, with some form of binding between cloud types
- Community
  - Cloud operated exclusively for more than one organization
- Private
  - Cloud operated exclusively for the use of one organization

Cloud Access Types

- Public
  - Cloud is accessed over the Internet
- Private
  - Dedicated network resources and capacity
- Community of Interest
  - Dedicated network resources shared among a small group of private users