FCC Technological Advisory Council

December 9th, 2013

Agenda

- Status of Technology Transition Task Force
- Resiliency Work Group
- Spectrum/Receiver Performance
- Spectrum Frontier
- COTS Work Group
- Security

TAC Scorecard 2013
Spectrum Frontier

- Recommendation on study of 30-40GHz mmW technologies and industry activities to support Gbps speed for mobile broadband
- Recommendation to pursue sharing discussion with Radio Astronomy in 95-275GHz band
- Recommend FCC increase Understanding technology developments in 95-275GHz band for higher speed and balance risk/reward of adopting service rules in this band
- Held Discussions with IEEE Special Interest Group on Terahertz technology and relevant applications
- Following up on the ITU spectrum allocation activities on 275MHz - 1THz space

Future

- Host a workshop on the enabling technologies for 30-40GHz mmW Mobile Broadband
- Host a Technology Day to understand technology developments in >95GHz band
- Recommend a coexistence/sharing framework with passive services in >95GHz bands

TAC Scorecard 2013

Resiliency

- Recommendations on joint industry development of consumer education materials, optimizing service restoral process, collaborative relationship with power industry on power strategies, ‘dig once’ policies, improved reporting metrics
- Developed detailed white paper on resiliency
- Met with industry experts/stakeholders
- Examined FCC’s existing resiliency data

Future

- FCC Workshops : Consumer Awareness, Labeling, Physical Infrastructure Reliability Summit

TAC Scorecard 2013
COTS

- Conducted interviews with companies and industry experts across sectors: Defense, Transportation, Telecom, Energy, and Consumer
- Recommendations to the Commission on developing sector specific COTS strategies, sharing strategies in underbuilt areas
- Defined use cases for COTs across industry sectors and aggregated specific use cases to more general form

Future

- Workshop on Enterprise Services in Wireless Broadband Network discussing QOS needs of specialized enterprises such as Defense, Oil, Energy and derivative policy/regulatory issues

TAC Scorecard 2013
Security

- Identified Key Sectors for Security Analysis
- Performed GAP analysis on each sector
- Met with a range of industry experts and organizations to develop recommendations
- Developed 2 white papers: Cloud Security Recommendations, Mission Critical and Critical Infrastructure Cloud Usage: Use Cases/Concerns
- Made Short Term/Long Term Recommendations on educational efforts, accountability, industry collaboration, certification
- Made recommendations for continuation of TAC work in 2014

TAC Scorecard 2013
Spectrum/Receiver Performance

- Published Interference Limits White Paper and FCC public notice seeking comment
- Made recommendation on MSH Group to pilot interference policy for 3.5 GHZ
  - Receiver group influential in guiding FCC small cell strategy applied to 3.5 GHZ
- Enlisted cooperation of spectrumwiki website in examining use of site for repository of links on rf standards
- Recommendations on NOI for SDO action supporting access to rf standards and liaison with key stakeholders

Future

- Developing technology notes on emerging RF technologies

Technology Transitions Policy Task Force Overview & Update

December 9, 2013

Changing Communications Landscape

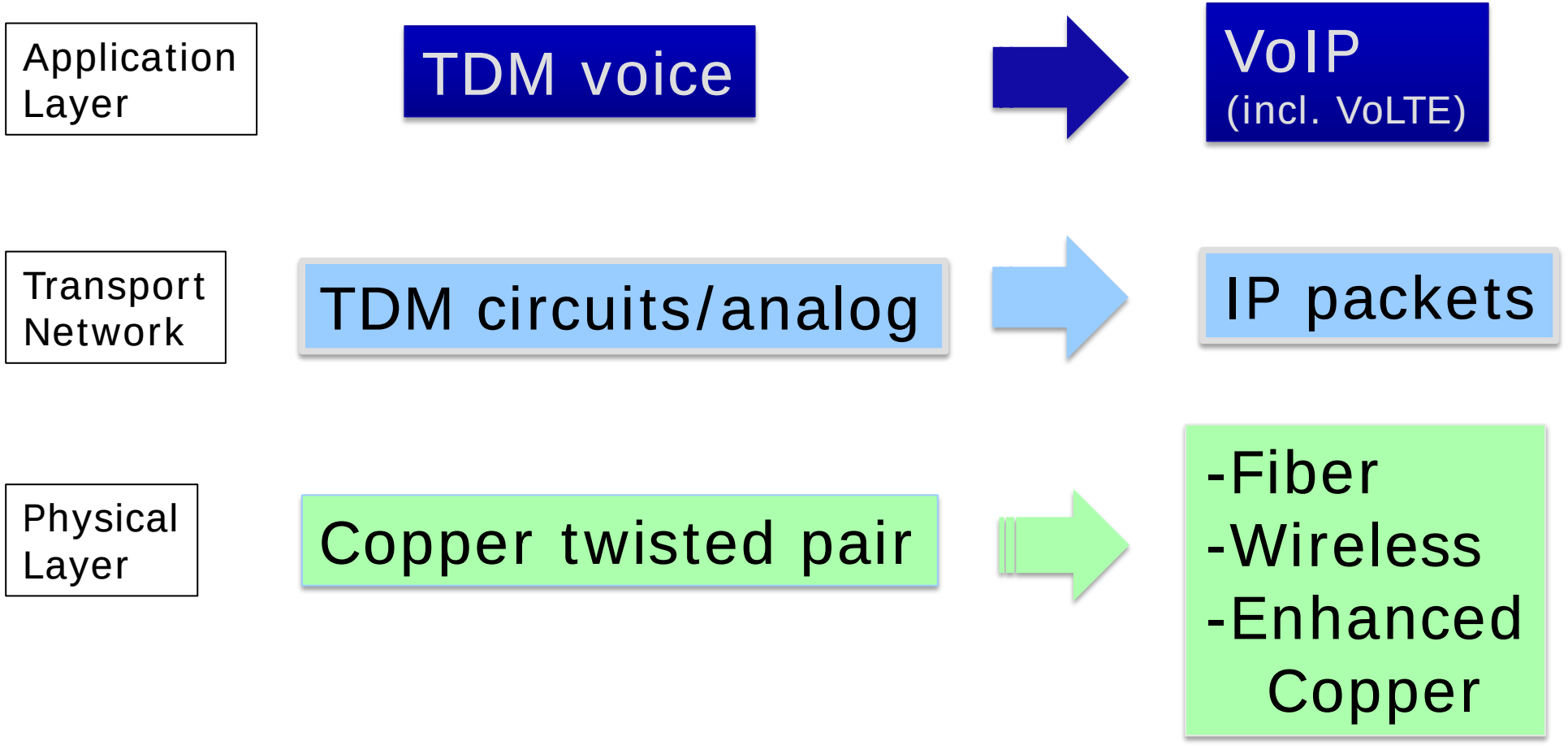
- December 2009 vs. December 2012*
  - **Retail switched access lines**: decrease from 127 million to 96 million
    - Compound annual decline of 9%
  - **Interconnected VoIP subscriptions**: increase from 26 million to 96 million
    - Compound annual growth of 17%
  - **Mobile subscriptions**: increase from 274 million to 305 million
    - Compound annual growth of 4%
- Nearly 40% of U.S. households are now wireless-only (over 60% for adults age 25-29)**
- Over 55% of mobile subscribers now have smartphones (up from 16% in 2009)***
- Widespread rollout of 4G LTE networks
- Gigabit cities from Kansas City, to Burlington, VT to Cedar Falls, IA

Sources: *Nov. 2013 FCC Local Telephone Competition Report

**June 2013 CDC National Health Interview Survey on Wireless Substitution

***comScore January 2013 U.S. Smartphone Subscriber Market Share Report

IP Transition: Multiple Layers, Multiple Transitions



Task Force Background

- FCC Technology Advisory Committee (TAC) Dec. 2011 recommendation; FCC should

  "establish a task force to conduct a thorough policy and regulatory and review as it relates to the PSTN, which results in policies for the new communication environment."

- Established by former Chairman Genachowski on Dec. 10, 2012

  "The Task Force will conduct a data-driven review and provide recommendations to modernize the Commission's policies in a process that encourages the technological transition, empowers and protects consumers, promotes competition, and ensures network resiliency and reliability."

- Builds on past and ongoing Commission activities
- Coordination through multi-stakeholder process

Core Values Guiding Task Force

- Promote growth, competition, innovation

- Preserve fundamental values (the “Network Compact”)
  - Public Safety
  - Universal Access
  - Competition
  - Consumer Protection

IP Transition: In the Words of the Commissioners

"The way forward is to encourage technological change while preserving the attributes of network services that customers have come to expect – that set of values we have begun to call the Network Compact."

-Nov. 19, 2013, *The IP Transition: Starting Now* (blog by Chairman Tom Wheeler)

"People have a lot of opinions about how the IP transition will affect consumers. But prediction is no substitute for practice. Or, as Albert Einstein put it, a 'pretty experiment is in itself is often more valuable than twenty formulae extracted from our minds.'"

-Mar. 18, 2013, Task Force Workshop Opening Remarks of Commissioner Ajit Pai

"As we develop a new policy framework for IP networks, we must keep in mind the four enduring values that have always informed communications law--public safety, universal service, competition, and consumer protection."

-Sep. 11, 2013, Congressional Testimony of Commissioner Jessica Rosenworcel

IP Transition: In the Words of the Commissioners

"*The Commission should explore all relevant issues to ensure that consumers are not harmed, that our networks are resilient and reliable, and that we continue to promote universal service and competition*."

-May 10, 2013, Statement of Commissioner Mignon Clyburn

"*I think the Internet is a very disruptive technology and that's to the benefit of consumers. So it's difficult to manage and control. However, the Commission has explored the opportunity of running or testing a number of trials in this space and I would be supportive…*"

-Sep. 18, 2013, Nominations Hearing Testimony of Commissioner Michael O'Rielly

Task Force Actions To Date

- Dec. 14, 2012: Established a pleading cycle on two technology transition-related petitions from AT&T and the National Telecommunications Cooperative Association (NTCA)

- Jan. 10, 2013: Issued Public Notice indicating that presentations made to the Task Force are subject to the Commission's ex parte rules (Docket 13-5)

- Mar. 18, 2013: Held public workshop focused on the capabilities and limitations of new and emerging technologies

- May 10, 2013: Issued Public Notice proposing to conduct a series of potential technology trials

Task Force Next Steps

- Task Force Presentation at Dec. 12 FCC Open Meeting
- Consideration of item at Jan. 30 FCC Open Meeting to consider recommendations on how FCC can best:
  - Obtain comment on and begin a diverse set of experiments
  - Collect data to supplement lessons learned from experiments
  - Initiate process for FCC consideration of legal, policy, and technical issues outside of experimental process
- See *The IP Transition: Starting Now* (Nov. 19, 2013 blog by Tom Wheeler, FCC Chairman)

Questions?

TAC Resiliency WG

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

Resiliency WG

December 9, 2013

- Russ Gyurek- (WG Chair)
- Ralph Brown
- Harold Teets
- Ed Chan
- KC Claffy
- Adam Drobot
- Mark Bayliss
- Dale Hatfield
- Doug Jones
- David Clark
- Greg Lapin
- Jack Nasielski
- Nomi Bergman
- Jim Shortal
- John Barnhill
- Mark Bregman
- Marvin Sirbu
- Brian Daly
- Paul Steinberg
- Glen Tindal
- 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
- Explore Layer 3 + issues
- Deliverable: White paper by Dec. 2013
- Actionable recommendations Dec 2013

Proposed Scope

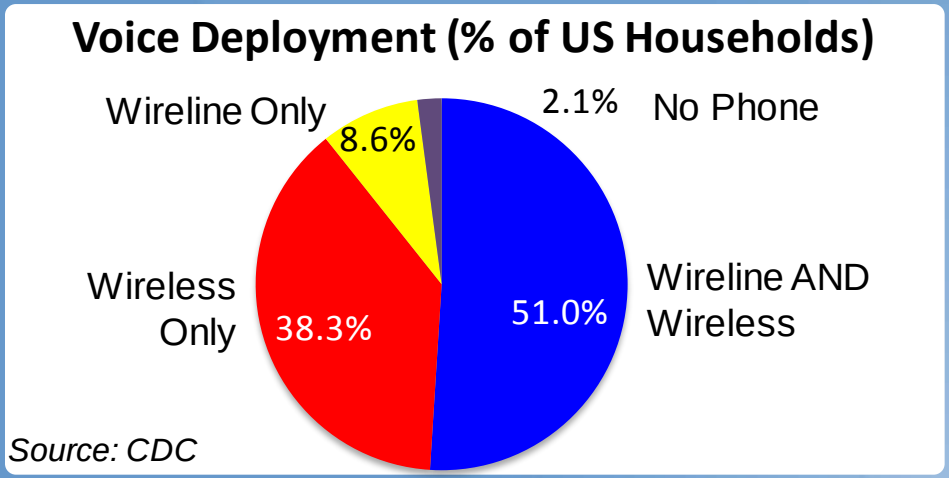
- Define ***resiliency*** relative to communications networks
- Focus on: Disasters: avoidance, recovery, substitution
- WG to focus on "distribution" part of network
  - Rationale: there is redundancy in core
- Emerging Trends review and relevant points of consideration
  - Cloud, SDN, NfV
- Metrics and Data collection
- Industry best practices

WG Actions 2013

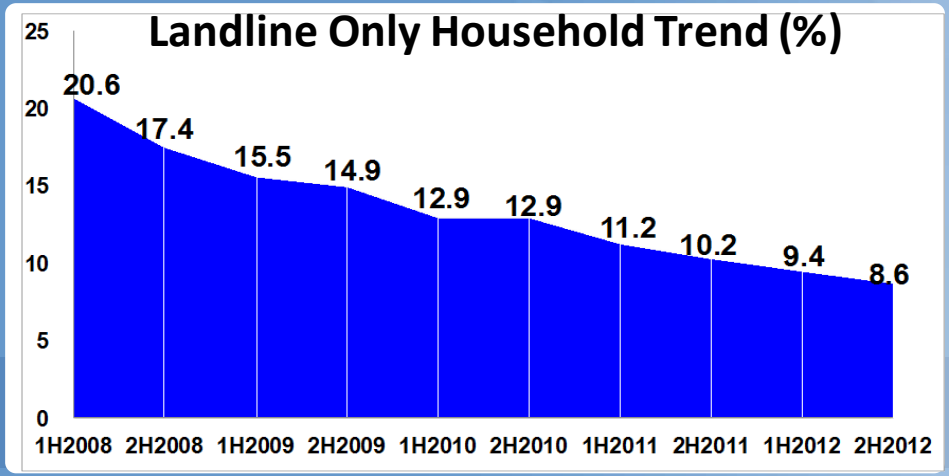
- Formed three sub-groups within WG to focus on main areas
  - Physical Plant Team (*special thanks Doug Jones*)
  - Investigate Policy, current Regulations, and Priorities (*special thanks Mark Bayliss*)
  - Reporting, metrics, forecasting, and service substitution/diversification
- Met a number of industry experts/stakeholders
- Liaison with FCC on existing resiliency data- John Healy
  - Intent statement
- Liaison with Security team, and emergency services
- Whitepaper (*special thanks John Barnhill)*

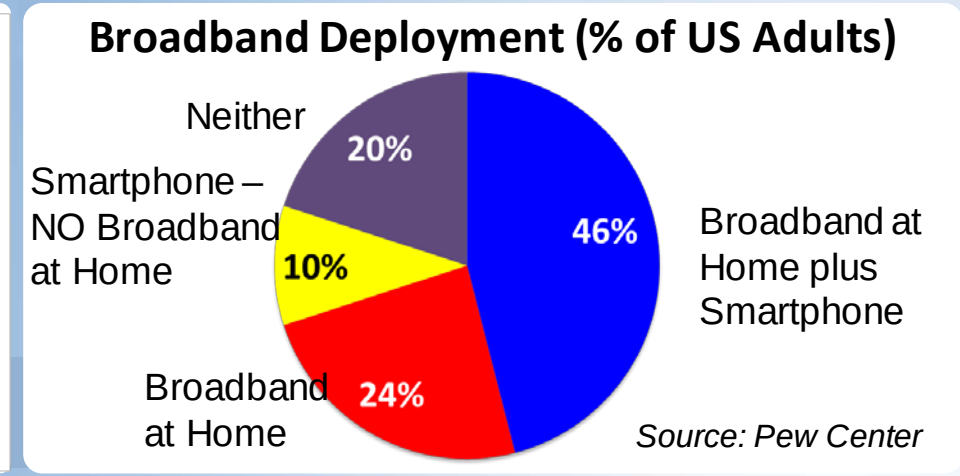
TODAYS NETWORK OF RECORD

Multiple Services = Higher Availability



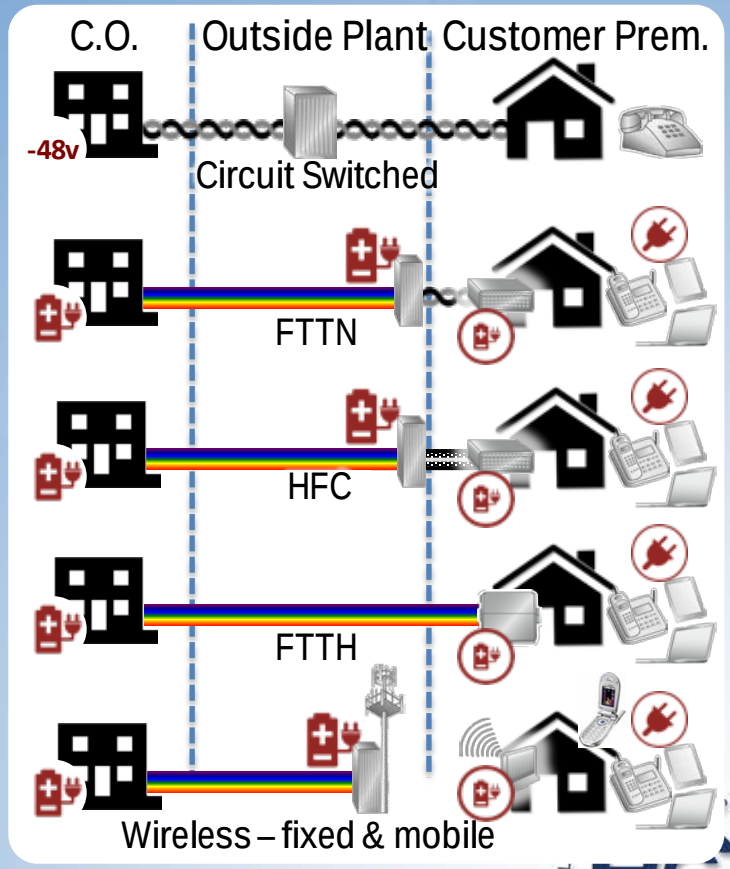
- Availability of diverse services creates higher potential household resiliency
  - Wireless now Dominant Voice Service
  - VoIP and Broadband households
  - 89.3% of Households have wireless phone.
  - 80% have either fixed BB or a smartphone





PSTN Transition = Powering Transition

- Power availability has emerged as the single most-impactful issue tied to resiliency
  - IP Transition: -48v CO Powered vs Premise Powered
  - Muti-modal communication, Multi-power needs:
    - Consumer devices: broadband modems/routers, PCs, tablets & smartphones
  - Service Provider impact: broadband access elements, NIDs, pedestals, wireless towers, routers etc.
  - Next Wave is Coming: The *Internet of Things* (M2M)



Industry Initiated **R³** = **R**esiliency, **R**esponse, **R**estore

Industry best practices are emerging and adapting to the new "Network of Record" driven by increased Competition as well as Cooperation among Network Providers

- Mobile Response Command Trailers
- Cells-on-Wheels (COWs), Cell-on-Light-Trucks (COLTs) & Repeaters on Trailers (RATs)
  - **Used to quickly enhance or replace network coverage and capacity in an effected area**
  - **Recent examples: CAL wildfires, OK hurricanes, super-storm Sandy, major sporting venues**
- CableWi-Fi hotspots. Major infrastructure sharing initiative by providers (Bright House Networks, Comcast, Cox, Optimum, Time Warner Cable)
  - **A coordinated, shared network used during super-storm Sandy restoration**
  - **Other providers offered non-coordinated Wi-Fi**

Value of Data

Proposed statement of intent- data collection:

Network Performance measurements serve multiple complementary purposes:

- *Data gathered over extended periods of time can help industry, government and researchers identify **performance trends**, **root causes** and **correlations** of network outages, particularly as the underlying network technologies, operational practices and organizational structures change.*
- *Data collected in real time during outages improves **situational awareness**, facilitates focusing on **critical needs** and identifies where **additional resources** or **alternative** means of **communications** are most urgently needed.*

*Long term goals would include **better forecasting, predictive modeling and planning for various outages**.*

WG Output & Actionable Recommendations

Resiliency Team

FCC- TAC 2013

Post-PSTN Public Communications Resiliency

FCC Technological Advisory Council:
Communications Resiliency Working Group

ABSTRACT

The purpose of this paper is to provide a detailed overview of the communications network, as it relates to resiliency. The paper identifies areas of concern, and related recommendations.

Detailed Whitepaper on Resiliency

-Network Transition
-Overview of Networking
-Communications Resiliency
-Disaster Planning and Response
-Resiliency for Public Safety
-Reporting and Metrics (Data)
-Regulatory & Agency Cooperation
-Recommendations
-Conclusions

- RECOMMENDATION: The FCC sponsor industry collaboration to create educational material/guidelines for consumer backup power associated with their broadband communication services.
  - Explore leveraging DHS, FEMA, and the Ad Council to establish a fund to create and promote consumer awareness.
  - Collaborate with Service Providers and Consumer Electronics manufacturers to document power consumption for devices in the communications chain.
  - FCC to promote the development of a CPE efficiency and "plug" program to create a common power plug for back-up power.
  - Establish a challenge.gov challenge to develop creative solutions to maintain customer communication services for at least 24 hours during power outages.
  - FCC to recognize there is an existing and evolving voluntary telecommunications industry agreement focused energy efficiency (http://www.ncta.com/news-and-events/media-room/article/2453).

- Optimize restoration process: FCC National program on a collaborative restoration approach in response to outages, disasters to increase resiliency and long-term reliability. Additionally, a reduction in damage to communications networks during the restoration process post disasters.
  - Explore creating a “data exchange” for various utility/communication providers to share data with each other for greater efficiency and optimization of restoration process
  - Providing estimated time to restore electrical service, by area, to communications companies
  - Providing communications companies with power crew work locations so that efforts can be coordinated
  - Instruct clearing and tree removal power crews not to cut any communications cables; call providers for quick removal of any cables in the way
  - Place communications technical facilities at risk, and outside plant locations critical to public and private sector entities on priority restoration lists

- Reliability/Resiliency: The FCC act as a catalyst and work closely with the Power industry to encourage continued improvements to reliable commercial power architectures to assist the communications service providers in developing resilient power strategies for critical network infrastructure.
  - FCC to work with FERC and other power industry agencies.
  - Explore the impact of long term use of back-up and diverse power sources.

- "Dig Once Policy": Building on the 2011 Executive Order -- Accelerating Broadband Infrastructure Deployment, FCC to Encourage Dig Once policies be enacted at local, state and federal levels to facilitate co-installation of communications networks during public works and utility construction
  - Dig Once policy would minimize the disruption to citizens by consolidating utility work among different companies. Potential to reduce facility cuts. Longer term greater reliability of network through UG installations of physical plant
  - Work with the *Inter-government advisory council*

- **Data collection and Metrics: Use network data sources to better track, predict, and plan network resiliency for disaster preparedness. To baseline and measure resiliency improvement over time.**
  - FCC to work collaboratively with providers to establish a data/analytic ability and/or expertise to use existing data sources, including existing NORS/DIRS data, for greater predictability and analysis of resiliency, and creation of a "Reliability Baseline" as a reference for future comparisons and metrics, working voluntarily with industry.
  - FCC to partner with CDC to update current data gathering process to get more specific information relating to availability of multi-modal communication options, clarifications between VoIP, VoIP OTT, and traditional wireline voice services for better reliability reporting and planning capability.
  - Leverage MBA data sets. Determine what data could be of value for reliability in the long term goals of the MBA program.
  - FCC to work with providers, determine what additional data is a meaningful indicator of reliability; develop a voluntary "crowd sourcing" data collection model to gather data in a manner that protects provider and consumer privacy and proprietary needs.
  - Create annual network reliability baseline update

FCC Sponsored Workshops:

- Workshop: Consumer Awareness

  The FCC host to foster and create educational material on guidelines for consumers in relation to power back up and services impact

- Workshop: CEA & other relevant parties

  FCC to promote labeling, efficiency, ease of design for CPE. Attendees to include: CEA, CPE vendors, SP's, Consumer advocacy groups.

- Physical Infrastructure Reliability Summit/Workshop:

  Leverage Hurricane Sandy Rebuilding Strategy Action Report

  FCC to lead collaboration with other government entities wrt to power reliability and restoration

Measuring Underlying VoIP Network

No Consensus from TAC

Viewpoint A: Market factors will drive service providers to deliver excellent service. A new requirement to report network performance would have little value in that other relevant service metrics would not be reported.

Viewpoint B: Accurate Data on performance of the communications network as a whole is required to ensure consumer protection and public safety.

This issue is discussed in more detail in the Resiliency Whitepaper

Comments and Feedback

Technological Advisory Council

Spectrum / Receiver Performance

Working Group

9 December 2013

Working Group Members

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

* FCC Liaisons

2013 Mission

- The working group will provide support as the Commission considers TAC recommendations related to the proposed interference limits policy.
- The working group will make recommendations in areas focused on improving access to and making efficient use of the radio spectrum from a systems perspective. Specific problem areas include:
  - Clarifying spectrum access rights and the limits of interference between receivers and transmitters
  - Explore methods to motivate receiver performance improvement

Working Group Areas of Focus

- Interference Limits Policy
- Multi-Stakeholder Organizations
- Radio Systems Standards Knowledge Base
- Emerging Receiver Technologies
- Interference Resolution and Enforcement

Implementation of Interference Limits Policy

- Published Interference Limits Policy White Paper
  - FCC issued Public Notice and collected Comments
- Recommended FCC to encourage multi-stakeholder (MSH) group to pilot interference limits policy in the 3.5 GHz band

Implementation of Interference Limits Policy

- Comments on Public Notice re Interference Limits Policy (docket 13-101)
  - Broad support for defining the environment in which receivers need to operate, though details need to be worked out and commenters generally supported concept more for services by others rather than their own service
  - Broad support for using multi-stakeholder organizations, but detail needs to be developed, and not one-size-fits-all
  - Support for FCC to encourage industry action in pilot project

Possible Activities of MSH Organizations

- Frame general principles
  - Use of worst case vs. probabilistic interference analysis, whether/how to reflect current or future signal environment, transition mechanisms?
- Identify threshold parameters
  - Determine which parameters are required, how many measurements, resolution in space/time/frequency, setting confidence levels?
- Determine parameter values
  - Develop methods to determine harm claim threshold values for the above parameters, e.g. how to take existing transmissions and receivers into account, to what extent & how to characterize existing interference environment, protocol for making techno-economic trade-offs?
  - Using these methods, determine consensus parameter values
- Define enforcement mechanisms

Radio Systems Standards Knowledge Base

- Enlisted the cooperation of the Spectrum Wiki website (www.spectrumwiki.com)
  - Exploring sharing standards on this website as a central repository of links
  - Exploring development of links between this site and the FCC Spectrum Dashboard
- Exploring organization of a FCC / NTIA / NIST workshop of radio system standards researchers and practitioners

Radio Systems Standards Knowledge Base

Recommendation: FCC Should Issue a Notice of Inquiry to initiate Standards Development Organization action

- Prompt standards organizations to volunteer to maintain a standards knowledge base
- Ask for comments on the relationship between existing standards and the development of interference limits policies
- Ask for a list of minimum receiver performance specifications (*i.e.*, the necessary parameters that should be included in every standard)
- Ask receiver developers their needs for parameters
- Ask for conformance testing requirements and specifications for each technology type

Emerging Receiver Technologies

Technology Notes targeted for January 2014

- Receiver hardware technology
  - Improvements in linearity (IIP3); dynamic front end filtering
- Dynamic interference cancellation
  - Using phased antennas and (echo-like) interference cancellation
- Software defined radio (SDR) technology
  - Moving ADC toward the front end enhances linearity & selectivity; future-proofing hardware with field upgradability
- Dynamic spectrum allocation and coordination
  - Coordination between users allows more effective spectrum sharing

Interference Resolution and Enforcement Actions and Recommendations

- Broad white paper draft targeted for January 2014
- Release additional information on interference complaints and investigations
  - Recommendation: The Commission should take early steps to release publicly in summary form information on interference complaints and investigations, including ones that are voluntarily resolved by the affected parties

Interference Resolution and Enforcement Actions and Recommendations

Recommendation: The Commission should convene a workshop of (a) academic researchers and their funding agencies working in the field of interference resolution and enforcement and (b) practitioners and other experts in the field of interference resolution and enforcement from within the Commission itself and other federal government agencies (e.g., the National Telecommunications and Information Administration)

Recommendations for TAC 2014 Work

(Continuing Spectrum & Receivers Working Group)

- Publish two papers in January 2014
  - Emerging receiver technologies for improving spectrum efficiency
  - Interference resolution and enforcement policy recommendations
- Develop scope and initial charter for interference limits MSH group in 3.5 GHz band

Recommendations for TAC 2014 Work

(New working group proposals)

- Interference resolution, enforcement, and noise
  - Investigate the costs and benefits of a Public-Private Partnership to voluntarily share information on interference incidents in a systematic fashion
  - Identify, analyze and recommend new strategies for interference resolution and enforcement in an increasingly challenging interference environment
  - Investigate noise floor and impact on services
  - Are changes needed in emission limits?

Recommendations for TAC 2014 Work

(New working group proposals)

- Advanced sharing technologies and support
  - FCC support for “Test City”
  - Evaluate agile technologies for sharing and co-existence
  - Federal / non-federal spectrum sharing

THANK YOU

Technological Advisory Council

Spectrum Frontier Working Group

9 December 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

- Chair: Brian Markwalter, CEA
- FCC Liaisons: Michael Ha, John Leibovitz

- Mike Bergman
- Ed Chan
- Bill Stone
- John Chapin
- Lynn Claudy
- Marty Cooper
- Adam Drobot
- Milo Medin
- Ramani Pandurangan
- Eric Miller
- Paul Steinberg
- Bruce Mueller
- Shahid Ahmed
- Dale Hatfield
- Mark Bayliss
- Jesse Russell
- Marvin Sirbu
- David Tennenhouse
- Brian Daly
- Mark Richer
- Kevin Kahn
- Michael Marcus

Overview

- September Meeting Recap
  - Presented the WG Recommendations on 30-40GHz mmW Band
  - Discussed intermediate findings on 95-275GHz Band
  - Presented research activities in the Terahertz Band
- Updates between September-December, 2013
  - IEEE-USA Petition: PN was released on October 31st
    - Petition for Declaratory Ruling Regarding Treatment of Rulemakings and Waivers Related to New Equipment and Services at Frequencies Above 95GHz
- This presentation explores:
  - Update activities on 30-40GHz mmW Band
  - 95-275GHz band findings and WG recommendations
  - Terahertz band research activities and WG recommendations

30-40GHz mmW – Recommendations

- WG recommends the Commission to take action which may include an NOI to evaluate mobile broadband feasibility and adoption of appropriate service rules to encourage further investment in key technologies and promising services.

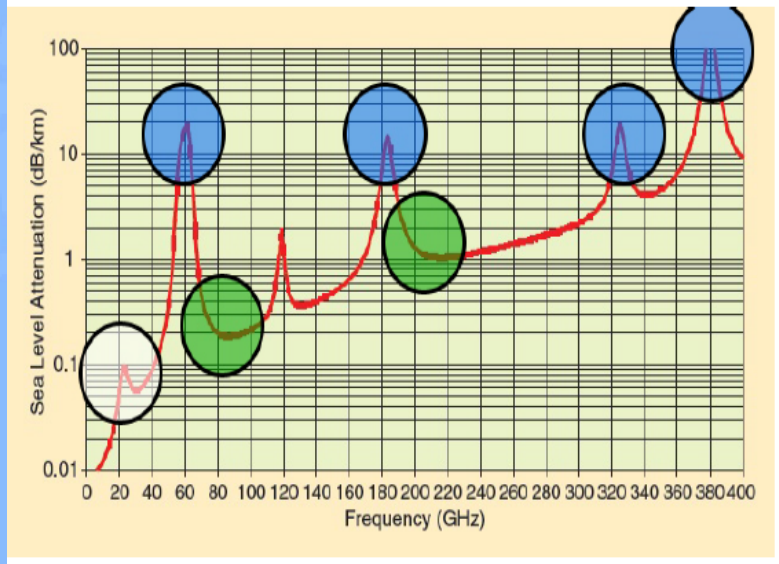
- WG recommends the Commission to hold a workshop with industry experts to discuss:
  - Enabling Technologies for Mobile Broadband
  - Potential Global Harmonization and Economies of Scale

- WG recommends the Commission to take a leadership role in the relevant ITU discussions without compromising other key US positions and objectives
  - Use WRC-15 discussion to get this item on WRC-18 agenda

30-40GHz mmW – Market Updates

- ITU Updates
  - Current effort has been on the WRC15 agenda formulation, for items to be discussed during the WRC18
  - Key discussion/debate is on identifying IMT bands at mmW bands
- Key Players and Activities
  - Samsung continues to promote 5G using mmW technologies and participates in various industry conferences (TIA Workshop in Nov, IWPC in Dec, etc)
  - Intel's efforts on WiGig at 60GHz is expanding to 30-40GHz bands and expects to unveil chipsets in 2014
  - T. Rappaport of NYU is actively engaged in mmW band propagation measurements and recently published a paper on 5G mmW in IEEE Access (May 2013)
  - Nokia Solutions and Networks and NYU are jointly organizing early 2014 5G Summit which considers 3-100GHz spectrum band
  - METIS (Mobile and Wireless Communications Enablers for the 2020 Information Society) of Europe is laying the foundation of 5G. METIS is coordinated under the auspices of the Seventh Framework Programme for research and development (FP7)
- Desire for higher speed for 5G (i.e. >1Gbps) makes mmW band very attractive but there are ample technical challenges to discuss

Atmospheric Attenuation: mm-waves



- 0.012 dB over 200 m at 28 GHz
- 0.016 dB over 200m at 38 GHz

- White
  - Current cellular frequencies and low mm-wave
- Blue
  - Short-range indoor communications, whisper radios of the future
    - Higher attenuation
- Green
  - Future backhaul and cellular frequencies
    - Low atmospheric attenuation
    - Multi-GHz Bandwidth
    - Directional Antenna Arrays with Beamsteering
    - CMOS: cost-effective with high frequency limits
    - Atmospherics are challenging

T. S. Rappaport, J. N. Murdock, and F. Gutierrez, "State of the Art in 60-GHz Integrated Circuits and Systems for Wireless Communications," Proceedings of the IEEE, vol. 99, no. 8, pp. 1390–1436, August 2011.

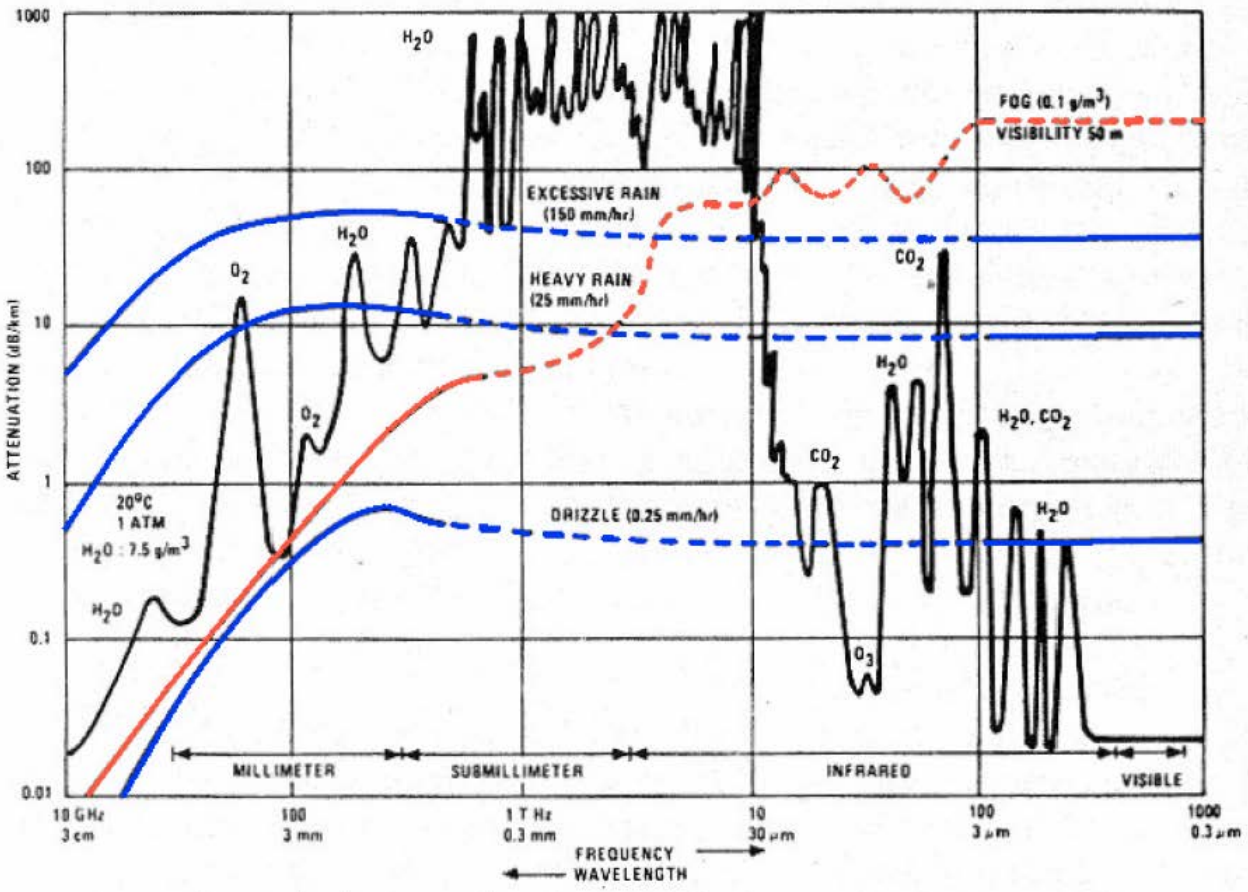
Your mileage may vary:

Foliage loss at 80 GHz and 10m penetration = 23.5 dB (15dB higher than @ 3 GHz)

Heavy rain in 70/80/90 GHz band results in 10 dB/km fade

Source: Samsung

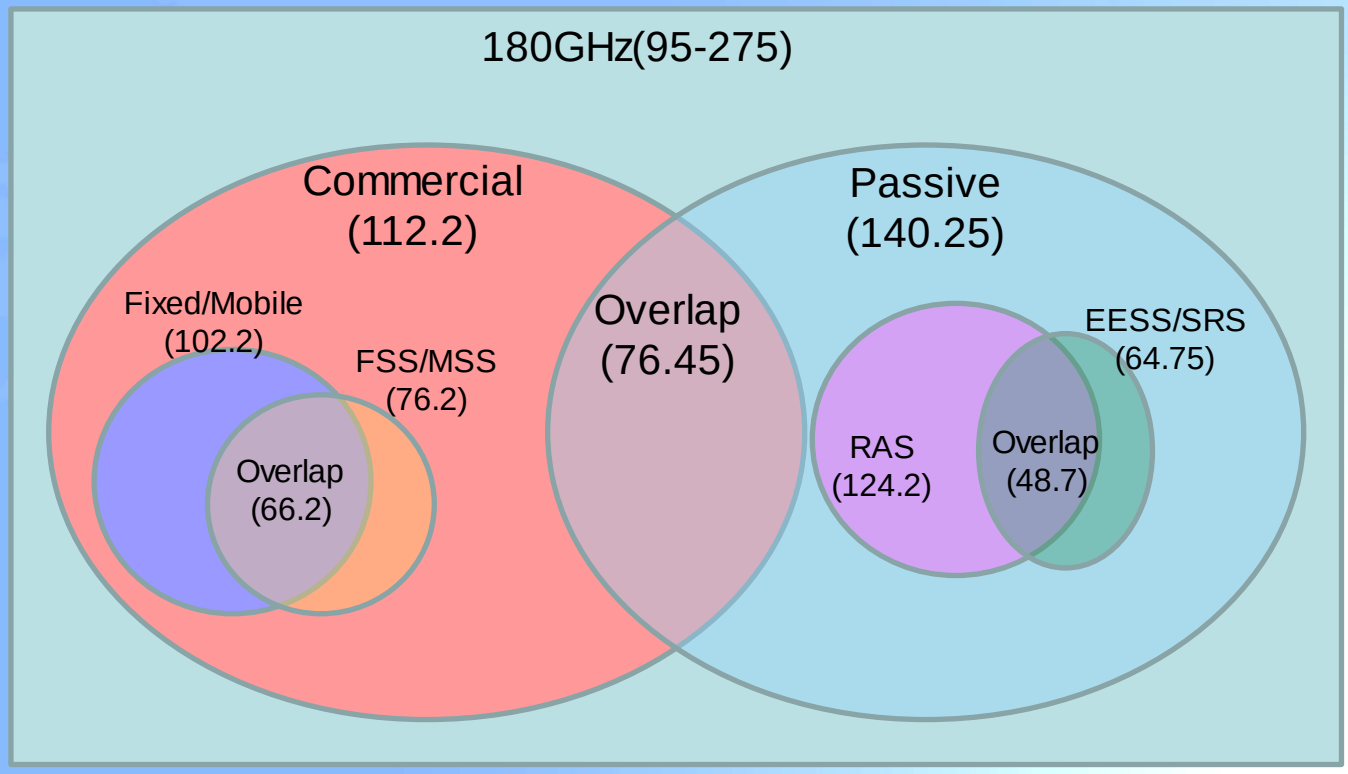
Source: IEEE ICC Plenary Presentation by Prof. T. Rappaport, 6/2013



Atmospheric attenuation characteristics for wavelengths 3 cm to 0.3 μm.

Source: Seashore, C., "Millimeter-Wave Integrated-Circuit Transducers," in K. Button, ed., "Infrared and Millimeter Waves" Volume 14 Millimeter Components and Techniques, Part V, (1985, Academic Press, Orlando, Fl.)

95-275GHz Allocation Summary



RAS: Radio Astronomy Service
MSS: Mobile Satellite Service
FSS: Fixed Satellite Service
EESS: Earth Exploration Satellite Service
SRS: Space Research Service

Note: Ovals representing frequency totals are not to scale

There are 31.5GHz of allocation for other active services including RNS, RNSS, Amateur, AMSAT, ISS.

Coordination with Passive Services

- Over 60-70% of spectrum over 100GHz ~ 1THz bands is allocated for passive services
- Radio Astronomy Space Research (RAS) service has demonstrated sharing potential with commercial services
  - RAS operates in 15 sites around the country below 100GHz and 3 sites above 100GHz (Hawaii, Arizona and California)
  - RAS already shares 70/80/90GHz band with microwave services
- Sharing with airborne/satellite-based Passive Services is more challenging
  - Both a Single User and Aggregate Interference cases may become a concern
- Mass market services/devices are concerns for RAS and other Passive Services
- It is difficult to assemble actual/planned use of passive services

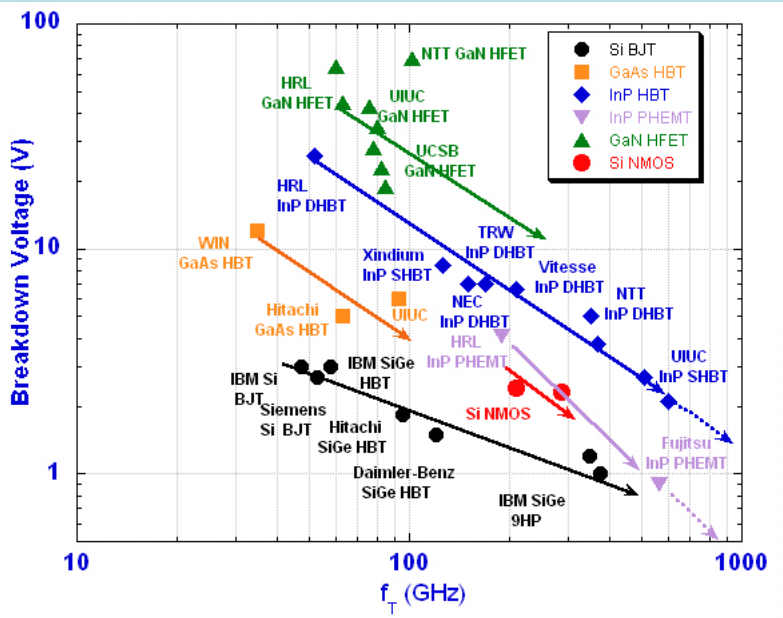
DARPA 100G Program *(100Gbps)*

- Design, build and test an airborne-based communications link
  - High capacity (fiber-optic-equivalent)
  - Long reach (200km air-to-air; 100km air-to-ground)
  - High spectral efficiency, +20bps/Hz
- Announced December 2012
- First phase of contracts were awarded to six companies in September 2013
  - Silvus Technologies, Northrop Grumman, Raytheon, Battelle, Trex Enterprises, Applied Communication
  - Total contract amounts to $21M

95-275 GHz mmW – Commercialization and Technologies

- Near 95GHz
  - There are a number of companies in 70/80/90GHz, but most at 70/80
  - 71-76GHz / 81-86GHz pairing is more useful than 92-94GHz / 94.1-95GHz

- Above 95GHz, propagation is well understood; some applications and technology exist
  - CMOS Silicon works above 95GHz to a point—then must transition to SiGe, GaAs, other technologies…but the cost goes up significantly.
  - Spectral efficiency degrades at higher frequencies when traditional radio techniques are scaled up, but optical techniques hold promise of significant improvement



Source: M. Feng, S. Shen, D. Caruth, and J. Huang, Proc. IEEE, Feb., 2004

95-275 GHz mmW – Driving Commercialization

- Two factors to drive more products and systems above 95 GHz:
  - Demand factor: Demand drives semiconductor re-investment and advancement cycle, but this cycle is not there yet for non-silicon ICs needed above 95 GHz.
  - Certainty factor: Service rules or other regulatory clarity above 95 GHz would accelerate commercialization and investment.
- Facts can be found to support both points
- Balance of these factors can be seen in recommendations

95-275 GHz mmW – Opportunities and Challenges

"More Certainty is needed"

- Larger bandwidth at higher frequency presents opportunities for ultra high-speed communication (+10Gbps)
- Adoption of service rules or regulatory certainty by FCC may facilitate capital investment in new technologies
  - US is lagging in technology private investment in higher frequencies
  - Market demand and technology maturity will come along as investment follows certainty and new applications and services are developed

"Demand cycle isn't ready"

- Capital investment is at an early stage
  - Ample investments in R&D (i.e. DARPA)
- Technology is not mature for commercialization
  - CMOS has limitations in higher frequencies
  - Alternative technologies (i.e. SiGe, GaAs) do not offer the cost structure for mass market
- Market demand isn't there yet
  - 70/80/90 band is available for point-to-point services
  - 60GHz unlicensed band can offer higher power services for outdoor use

95-275 GHz mmW – Risk/Benefit Assessment of +95GHz Service Rules

Risks	Benefits

▪ Early technology may not serve the mass market
▪ Prematurely licensed/unlicensed spectrum in high frequency band may not best serve the public interest
	▪ Early technology movers may benefit in terms of:
	  ▪ Capital Investment
	  ▪ A large amount of high frequency spectrum being licensed

95-275 GHz mmW – WG Recommendations

- The Commission should take an active role to establish a framework for co-existence with passive services

- The Commission should carefully balance the benefit/risk of adopting service rules in this band
  - Monitor progress & await petitions
  - Host a workshop or technology day on >95 GHz to understand developments
  - Engage in the international activities for this band and evaluate the applicability for US market as appropriate

Terahertz Research Activities

- Terahertz sources and detectors
- Materials research
- Imaging and tomography
- Wireless Applications
  - Short Range, Ultra High-Speed Data Communications
- Security Imaging/Sensor
- Medical/Industrial Applications
- Space Science

- Why THz is hard to do…
  http://spectrum.ieee.org/aerospace/military/the-truth-about-terahertz

Terahertz Recommendations

- Continue to monitor the commercial developments and R&D in the Terahertz space
- Non-telecom applications should be included in the Commission's effort on this band
- Desire for large passive allocation in 275 GHz-1 THz is likely trigger a similar sharing discussion and should be considered in the coexistence study recommendation of 95-275 GHz band.

Technological Advisory Council

Wireless COTS Working Group

COTS working group members:

Name	Company	
Shahid Ahmed	Accenture	Workgroup Chair
Mark Bayliss	Virginia ISP Association	
Nomi Bergman	Bright House Networks	
Ed Chan	Verizon	
Diane Wesche	Verizon	
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	

Table of contents

COTS Working Group Mission Statement

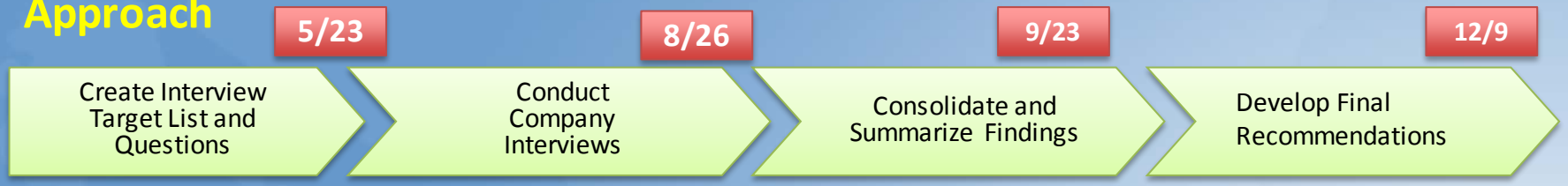
Find ways to leverage technical and commercial benefits of scaled wireless solutions to:

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

Objective

Collect empirical data from industry interviews to determine lessons from industries where COTS has worked and focus on a 2-3 specific use-cases where COTS is a common platform. Some examples include: Military use of LTE, Spectrum sharing, Smart Grid, and LTE for Public Safety.

Approach



- DOT
- Qualcomm (Small Cells / LTE ATG
- Samsung
- Nest
- Ameren
- Southern Company
- Ford
- Wireless Policy OSD

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

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

- Present final COTS models and recommendations
- Final presentation on 12/9

Recommendation 1: Formalize a Commission COTS definition for 'Commercial-Off-The-Shelf' technologies and services

- **Situation**
  - Loose definition of what COTS means and what the term applies to (e.g. commercial services, technology standards) leads to inconsistent interpretations from Organizations, Service Providers and Technology Vendors
- **Complication**
  - Some Organization believe that some non-standard solutions are COTS given their wide availability within their (vertical) industry, leading to costly solutions that are generally not interoperable between industries (i.e. Pubic Safety vs Utilities, Telematics vs Home Automation)
- **Recommendation**
  - Formalize a Commission definition that defines COTS from a service and technology view point
  - Work with the Verticals, Service Providers and Technology Vendors on developing a 'COTS' Program per Industry Sector
- **Complexity/Timeframe to Implement**
  - **Short-term**

Recommendation 2: Identify spectrum sharing opportunities in under built commercial areas collaboratively with Industry Stakeholders

- **Situation**
  - Given disparity in the service areas covered by Service Providers, certain verticals cannot rely on commercial networks for Mission Critical business functions. As a result, these Organizations move towards private network build-outs that require dedicated spectrum.
- **Complication**
  - Private network build-outs require Organizations to make costly investments in spectrum to fill coverage holes in areas where Service Providers could extend their services.
  - Use of dedicated spectrum and private networks adds complexity to Interoperability efforts that are crucial during Emergency Scenarios.
- **Recommendation**
  - Work collaboratively with industry stakeholders in a workshop to cover spectrum sharing options as part of a broader workshop that discusses Enterprise requirements for Wireless Broadband Services (as described in Preliminary Recommendation #1).
  - Explore possibilities for public safety/emergency service usage of private networks
  - Look at evolving technologies that support sharing
- **Complexity/Timeframe to Implement**
  - **Short-term**

Recommendation 3: Workshop on Enterprise Services in Wireless Broadband Network

- **Situation**
  - Organizations across industries have concerns about Service Providers not providing the quality of service (e.g. latency) and service guarantees appropriate to meet their Mission Critical business requirements. As a result, these Organizations end up deploying costly private solutions.
- **Complication**
  - Congestion in Service Provider networks during Emergency Scenarios makes them unreliable in the view of certain Organizations
- **Recommendation**
  - Organize a workshop to discuss Enterprise requirements for Wireless Broadband Services
  - Encourage Enterprise support by Service Providers and gain a better understanding of what the technical issues, limitations and potential is in having these Service Providers offer specialized Enterprise Services. For example, Mining, Oil, and Gas
  - Identify potential regulatory / policy issues associated with Quality of Service
- **Complexity/Timeframe to Implement**
  - **Short Term**

Use Case	Industry	Description
Armed Forces Networks	Defense	The armed forces or other defense organization could use commercial LTE or wireless equipment to provide private wireless networks supporting training facilities and deployed forces.
Public Safety	Public Safety	Public safety personnel can use commercial networks for emergency communication or can build private networks using commercial wireless technology.
Emergency 911	Consumer	Communities can use COTS/Private networks for 911 calls that will extend emergency services to unserved areas.
Utility Monitoring & Communications	Utility	Utilities can use COTS technology to provide wireless communications where no viable commercial service exists, monitor consumer and business power usage, and monitor utility networks.
In Transit Remote Communications	Transportation	Commercial wireless service can be used by airlines, railways, and other transportation companies to provide data access to customers where viable commercial service does not exist.
Aviation Telemetry Platform	Aviation	Due to increased use of drones by civilian and military users and the high bandwidth requirements for telemetry and control, there is a need for a unified wireless aviation telemetry and control platform that could be developed and shared among the many future users.

Full Use Case Collection

Next Steps

1. Update recommendations based on feedback

2. Schedule a workshop with key stakeholders regarding COTS definition and broadband services for enterprises

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?

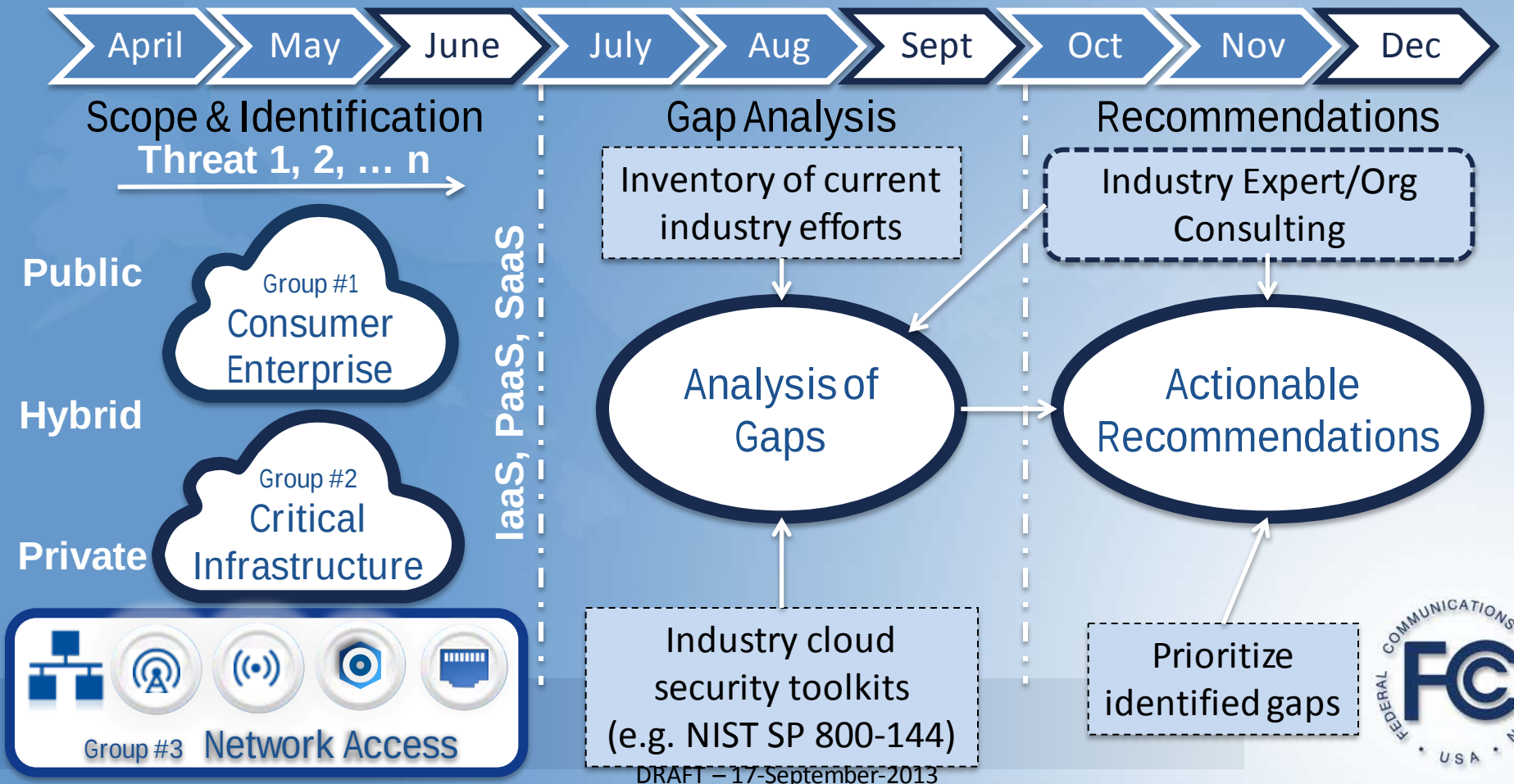
Mission Statement Key Objectives

- 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
  - Peter Chronis, Earthlink
  - Dick Green, Liberty Global
  - John Howie, Cloud Security Alliance
  - Lynn Merrill, 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
  - Joe Wetzel, Earthlink

2013 Work Group Plan



2013 Work Group Plan

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

Identified areas of Concern (From Sept-2013 Report)

- Education (Lynn, John)
- Accountability (Ramani, Harold/Mike)
- Industry Collaboration (Donald, David)
- Certification
- Auditing

} (George, Pete)

Work Products

- Short and Long Term Recommendations for the FCC
- Whitepaper: "FCC TAC Communications Infrastructure Security Working Group Report: CLOUD SECURITY ANALYSIS AND RECOMMENDATIONS" (Dec – 2013)
- Whitepaper: "FCC TAC Communications Infrastructure Security Working Group Supplemental Report: Expanded findings Around Mission Critical and Critical Infrastructure Cloud Usage: A More In-Depth look at the Relevant Use Cases and Areas of Concern (Dec-2013)
- Recommendations for Future (e.g. 2014 TAC) Further Study Items

Education

Lynn Merrill

Education: Description & Background

- **Education is the cornerstone to expand the use of the cloud and to protect the security of the networks**
- All actors need to make informed decisions about the cloud in order to advance cloud computing
  - Actors include providers, consumers, regulators, etc.
  - In order to make an informed decision, education and awareness materials are required
  - Smaller Government Agencies, Enterprise Companies and Individuals will benefit most from concise educational material
- We did a high-level review of the current state of education and awareness in the industry today
- There is a role for the FCC in promoting education and awareness to government, industry, and consumers (both enterprise and SMB/individual)

Education and Awareness: Best Practices

- There is a lot of material published today which can be used
  - Some of it is marketing and hype more than reality, and some is very high level
  - An overload of information makes it difficult for small users to locate pertinent resources for Cloud uses and Security
- NIST has contributed greatly to education and awareness
  - SP800-145, SP500-292 and Draft SP500-299, are readily available and consumable by all actors and stakeholders, not just USG (SP800-145 is de facto world standard)
- There are several 'trusted', objective sources for educational material
  - Industry associations such as the Cloud Security Alliance, Open Data Center Alliance and others, whose goal is to produce independent guidance and best practices
  - Government agencies in other countries and communities, e.g. European Network and Information Security Agency (ENISA)
  - Some industry players have produced reasonably independent material (Microsoft, Google and Amazon included)
  - Academia is creating Undergraduate and Master degrees as well as certificate programs

Education and Awareness: Analysis of the Current Landscape

- Much of the guidance published is high-level, service specific or has a marketing focus
- Material tends to be vendor specific
- Earlier-published material, which are relied upon or referenced by others, is not being kept up-to-date
- Collaboration of best practices and case studies are not understandable or available to the general user
- Volume of information available makes consumption largely impracticable

Education and Awareness: Recommendations

- **General Takeaways**
  - Education is one of the best tools to use and in the long run will provide the greatest awareness for cloud security issues
  - Small enterprise users will benefit the most from the targeted education and awareness campaign
- **Near-term**, FCC can collaborate with industry and academia to identify best E&A materials from sources publicly (and freely) available
  - Material should be evangelized
  - Small investments by government and industry could be made to update older material to make it relevant
    - Investment need not be 'cash', but labor
  - FCC could incorporate materials from others into its own portfolio
  - Materials published to include a website reference for small business

Education and Awareness: Recommendations

(continued)

- **Long-term**, FCC can work with others to identify gaps in E&A material focused at, or about, cloud carriers and develop its own materials
  - Still a lot of work to be done, and FCC is best placed to lead this work
    - Include topics such as carrier security, routing, DNS, etc..
  - Hold Workshops to increase Education and Awareness
    - Work with industry and associations to create a long-term strategy for the development and sustainability of ones' own published material
  - Public Awareness
    - Continue investment in the evangelizing of material to promote adoption
    - Develop liaisons with other governmental agencies to have recently created material posted on websites, updated and disseminated to users
      - (i.e., SBA, USDA, NTIA, Cloud Providers, Industry Associations, Smart Communities and Broadband Providers)
  - Provide information to Cloud and Broadband Providers to place on websites for consumer's use

Accountability

Mike McNamara

Accountability: Description & Background

Description:
"An essential concept in the protection and security of electronic information whereby every individual that works with an information system should have specific responsibilities for the assurance and integrity of the information.

- Accountability Goals: (Security is TAC focus)
  - Define responsibilities of each party ***(Consumer, Provider, Carrier, Auditor)*** per Service Model (***IaaS, PaaS, SaaS)***
  - Ensure protection methods across services (IaaS, PaaS, SaaS, Storage, etc)
  - Baseline Certification & Auditing methods of compliance
  - Drive consistency of environment measurement and assurance for consumers
- Increased adoption of outsourcing IT-like functions and responsibilities accompanied by increased threats in data hijacking & theft warrant greater knowledge of data protection & validation of roles & responsibilities

Accountability : Best Practices

- Existing industry Best Practices for guidance:
  - NIST SP500 (Information Technology) & SP800 (Computer Security)
  - NIST SP500-292 Cloud Computing Reference Architecture
  - Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0, Cloud Security Alliance 2011
  - Practical Guide to Cloud Service Level Agreements Version 1.0 Cloud Standards Customer Council, April 10, 2012
  - Specifics publications:
  - SP800-144 Guidelines on Security and Privacy in Public Cloud Computing
  - SP800-146 Cloud Computing Synopsis and Recommendations

- Cloud Security Alliance – highlights best practices for Cloud Computing security assurance
- Larger enterprises have purchasing leverage to negotiate Service Level Agreements (SLA) to ensure better protection, performance, and stronger accountability if issues arise

Accountability: Analysis of the Current Landscape

- Knowledge or understanding of limited / undefined Accountability when outsourcing data to the Cloud
- Lines of Accountability are unclear and finding information on best practices is cumbersome
- Certain network access methods are more secure and less vulnerable to MITM (Man-In-The-Middle) attacks such as DNS Spoofing and BGP Hijacking
- Data Protection parameters such as PCI, HIPPA focus on specific industries / data types
- In the area of auditing and SLA, many documented challenges have come not from a cloud provider's ability to service a customer, but the ability of the customer's systems to interface properly with the cloud
- In the area of BC / DR, It is common to see a false sense of security among cloud consumers regarding disaster recovery planning

Accountability: Recommendations

- General Takeaways
  - Security is as strong as the weakest link in the end-to-end ecosystem of actors
  - Accountability ***of*** various actors in the ecosystem depends on the Service Model
- Short Term Recommendations
  - Develop easy-to-access and easy-to-understand content to make Cloud Consumers aware of
    - the need for and attributes of various domains of an SLA between ecosystem players and dependency on the service model, since Accountability (expectations and recourse) is captured in SLA [1,2]
    - the need to evaluate suitability of cloud for their business needs and to conduct due diligence to evaluate security capabilities (e.g. compliance certificates, audit reports, BC / DR) of cloud ecosystem players for all the layers of the "stack" for migrating to the cloud, being in the cloud and exiting from the cloud
- Long Term Recommendations
  - Study any specific recommendations that may need to be developed for Critical Infrastructure cloud services
  - Extend the scope of Accountability beyond security to other areas such as availability and performance
  - Study the impact of new SDN / NFV technologies on Cloud security implications and update these recommendations

[1] *Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0, Cloud Security Alliance 2011*
[2] *Practical Guide to Cloud Service Level Agreements Version 1.0 Cloud Standards Customer Council, April 10, 2012*

Industry Collaboration

Donald Tighe

Industry Collaboration: Description & Background

- Industry collaboration functions as a central tenet in the multi-stakeholder approach to Internet governance
- With 95% of the nation's critical infrastructure owned and operated by the private sector, industry collaboration on network access, resiliency, and cyber security is essential
- Industry collaboration takes three primary forms:
  - Industry-to-industry collaboration, industry-organized, & industry-led
  - Industry-sponsored collaboration that funnels guidance to government
  - Government-sponsored entities that foster/facilitate industry input

Industry Collaboration: Best Practices

- Industry collaboration contributes standards and certification requirements to three crucial priorities: network access, resiliency, and cyber security
- Progress stems from Industry-government cooperation and collaboration
- Recent network access and security initiatives by government have supplemented ongoing private sector collaboration initiatives, and include:
  - 2007, Government establishes Trusted Internet Connection (TIC) program
  - 2009, President establishes first-ever Federal Chief Information Officer (CIO)
  - 2010, Federal CIO establishes Federal Data Center Consolidation Initiative (FDCCI)
  - 2011, OMB launches "Cloud First" initiative prioritizing info security, access, and $ savings
  - 2012, Government expands "Bring Your Own Device" initiative for data access, security
  - 2013, President releases Executive Order 13636, "Improving Critical Infrastructure Cyber Security, including NIST-led industry collaboration for access & security standards

Industry Collaboration: Best Practices in all 3 models

- Industry-to-Industry Collaboration:
  - Information Technology Industry Council (ITI) links policymakers, companies, and non-governmental organizations to advance standards, cooperation, and interoperability.
  - TechAmerica fosters comprehensive global, national, and regional advocacy and high-level policy and technology collaboration establishing standards and transparency in the ICT industry.
- Industry-sponsored collaboration that funnels guidance to government:
  - Sector Coordinating Councils (such as the IT-SCC) that develop standards and foster peer review and transparency standards for Service Level Agreement elements such as access & up-time
  - Information Sharing & Analysis Centers (ISACs) that facilitate the exchange of both classified and unclassified cyber security information including known threats and detection techniques
- Government-sponsored entities that foster and facilitate industry input
  - Presidential advisory panels such as National Security Telecommunications Advisory Council (NSTAC), with recent reports on Cloud Security, FirstNet, and Secure Gov't Communications
  - National Institute for Standards & Technology (NIST), currently leading industry collaboration efforts for standards and incentives ensuring network access and security

Industry Collaboration: FCC TAC Recommendations

- Existing best practices can be supported, enhanced by FCC; legislative and Executive Branch policy puts jurisdiction elsewhere, but the FCC can build and nurture industry collaboration among key stakeholders
  - FCC has unique convening capability to facilitate collaboration, cooperation
  - The TAC recommends incorporating network access and security education and awareness "toolkit" information into 2014 FCC meetings with industry partners
  - The TAC recommends the FCC consider holding public-private partnership workshops in 2014 that gather and disseminate network & access standards
  - The TAC recommends the FCC partner with other gov't entities overseeing these issues (DHS, NIST, WH/OMB) to ensure industry participation & adoption (e.g., promote the use of NIST's Cyber Security Framework)
  - The TAC recommends an FCC-convened "clean room" for info sharing

Certification & Audit

George Popovich

Certification & Auditing: Description & Background

- Description: *Attaining an accreditation attesting that any vendor's solution does what the vendor claims.*
  - This is not limited to initial environment validation but includes ongoing auditing of the environment to assure continuous compliance to the original attestation.
  - This accreditation can be in the form of third party assessments or self assessments.
  - Recommendations herein are scoped to security certification and auditing in cloud environments.

- Why this matters: Smaller entities cannot afford the due diligence to navigate the complexity of selecting the best cloud providers for their needs.
- Scope: enterprise/consumer, mission critical/critical infrastructure, cloud network access
- Certification & Auditing Goals:
  - Gain and maintain subscriber trust in the solution
  - Provide transparency
  - Reduce costs of evaluation
  - Drive consistency of environment measurement
- Take-away: Cloud audit and certification programs are new, continue to evolve, and often overlap existing certification/compliance schemes

Certification & Auditing : Best Practices

- Enterprise/Network Access: best practices via CSA STAR/AICPA SOC2
  - CSA STAR Self Assessment/ Certification /Attestation/ Audit
    - Self assessment based on questionnaire and/or Cloud Control Matrix (CCM).
    - New third party assessment based on CCM and ISO27001/2 or AICPA SOC2.
  - AICPA SOC 2 control area scope: security, availability, processing integrity, confidentiality, privacy
- Consumer
  - Federal level privacy rules/regulations focused on financial/healthcare, child online privacy; patchwork of state legislation
  - 3rd Party AICPA GAPP certifications are rare, TRUSTe self-certifications are becoming more common
- Federal Government
  - FedRAMP Authority to Operate for CSPs (Cloud Service Providers)
  - CSPs must attain FedRAMP certification to sell services to the federal government.
- Mission Critical & Critical Infrastructure
  - NIST Cyber Security Framework will likely become the minimum standard
  - IACP published Guiding Principles in Cloud Computing for Law Enforcement
  - Critical Infra. security controls include NERC-CIP and NISTIR 7628, but not focused on the cloud

Certification & Auditing: Analysis of the Current Landscape

- Cloud certification & audit frameworks are relatively new and continue to evolve (e.g. NIST, SOC2, CSA STAR)
- Certification/audit programs are generally rigorous and complex and favor large enterprise/government
- Federal agencies are covered by FedRAMP today
  - Authority to operate (ATO) only extends to moderate impact data, per FIPS 199 definitions
- Area of focus for non-federal agencies - not covered by FedRAMP
  - Lack of transparency leads to mistrust , need state and local endorsements
  - Feedback from external discussions, need organized at federal level
- Mission Critical & Critical Infrastructure
  - Need data classification standard for CJI data (e.g. FIPS 199)
  - CJIS Data not covered by any cloud certification body (i.e. high impact data)
  - Public Safety believes certification is needed
  - SCADA Data will have limited movement to public clouds, due to the inherent risks
- Enterprise/Consumer
  - Many solutions are more commonly being delivered using a mix of different cloud solutions – shared security model is not addressed

Certification & Auditing: Recommendations

- General Takeaways
  - There is not a “one size fits all” solution for cloud services
  - There are existing certifications and requirements that need to be leveraged where possible (described on the following slide)
  - Enterprise Cloud customers should leverage the newly evolving CSA Open Certification Framework to enhance the cloud vendor selection process.
    - Multi-layered structure – based on customer needs
    - Three levels (tiers) defined within the CSA Open Certification Framework (OCF)

Certification & Auditing: Recommendations

Short Term Recommendation	FCC Action
As a recommended best-practice, all enterprises and organizations should conduct an application audit concurrent with moving to the cloud.	FCC sponsored workshop to explore public/private partnership to promote application security in the cloud, enhanced application security in the cloud translates to fewer targets for hackers, cleaner network traffic, fewer threats to critical infrastructure

Leverage existing standards for certification, and existing certification bodies, to help educate potential cloud service consumers.	Provide guidance and education on the following:
	• Security controls and guidance documents
	  • NIST SP 500-292 and NIST SP 500-299
	  • NIST SP 800-53 and FIPS 199/200
	• Certification standards
	  • AICPA SOC2
	  • ISO 27001, 27002
	• Certification bodies
	  • FedRAMP
	• Certification frameworks
	  • CSA Open Certification Framework

Certification & Auditing: Recommendations

Long Term Recommendations	FCC Action
Closely evaluate existing certification standards for security gaps.	Collaborate with the CSA to drill down on security standards to address any gaps that may exist as a 2014 standards
Leverage the FedRAMP certification process for state and local agencies	Reach out to FedRAMP to expand coverage to state and local agency certifications.
Create certifications for CJIS data service providers	Reach out to FedRAMP to expand coverage for CJIS and High Impact Data coverage Alternatively, address high impact needs via the sponsoring of Community Clouds for PS/State/Local
Create a Certification Body that cover NERC-CIP requirements for CI	Reach out to NERC to extend compliance standards to cloud providers for CI data

Conclusions and Next Steps

- The future impact of cloud computing cannot be overstated
  - Rapidly progressing and evolving with considerable complexity
  - Cloud Security and Cloud Resiliency have significant bearing on the economic viability of the country and the safety of our citizens
- The FCC is wise to consider implications of cloud computing but (as always) must strike the balance of how it acts
  - Cloud provides accessible/affordable professional services for entities with limited (private) means – the rising tide.
  - Because of newness and significant leverage of the paradigm, the stakes are much higher overall for failures and missteps (e.g., EU considers cloud CI)
- Future Suggested Activities (e.g., TAC 2014)
  - Expand the analysis to include Cloud Resilience, Availability and Performance
  - Focus additional security analysis around Critical Infrastructure usages of Cloud
  - Help the FCC create alliances and joint forums with industry / government partners