Technical Advisory Council
Federal Communications Commission
Summary of Meeting
September 23rd, 2013

The Technical Advisory Council (TAC) for the FCC was convened for its tenth meeting at 1:00 P.M. on September 23rd, 2013 in the Commission Meeting Room at the FCC headquarters building in Washington, DC. A full video transcript of the meeting is available at the FCC website at http://www.fcc.gov/encyclopedia/technology-advisory-council together with a copy of all materials presented at this meeting. In addition, all materials presented at this meeting are included in electronic form in an Appendix to this document.

In accordance with Public Law 92-463, the entire meeting was open to the public.

Council present:

Shahid Ahmed, Accenture	Kevin Kahn, Intel Corporation
John Barnhill, Genband	Gregory Lapin, Independent Consultant
Mark Bayliss, Visual Link Internet, Lc	Brian Markwalter, Consumer Electronics Association
Nomi Bergman, Bright House Networks	Milo Medin, Google, Inc
Peter Bloom, General Atlantic	
Mark Bregman, Neustar	Lynn Merrill , NTCA
Ed Chan, Verizon	Vish Nandlall, Ericsson North America
John Chapin, DARPA	Jack Nasielski, Qualcomm, Inc.
David Clark, MIT	Ramani Pandurangan , XO Communications
Lynn Claudy, National Association of Broadcasters	Mark Richer, Advanced Television Systems Committeee, Inc.
Brian Daly, AT&T	Dennis Roberson, Illinois Institute of Technology
Pierre Devries, Silicon Flatirons Center for Law, Technology, and Entrepreneurship University of Colorado at Boulder	Jesse Russell, incNetworks
Adam Drobot, OpenTechWorks	Marvin Sirbu, Carnegie Mellon University

Brian Fontes, NENA	Kevin Sparks, Alcatel-Lucent
Dick Green, Liberty Global, Inc	Paul Steinberg, Motorola
Russ Gyurek, Cisco Systems	David Tennenhouse, Microsoft
Dale Hatfield, Silicon Flatirons Center for Law, Technology, and Entrepreneurship University of Colorado at Boulder	Jack Waters, Level 3 Communications LLC
Theresa Hennesy, Comcast Corporation	Joe Wetzel, EarthLink, Inc.

FCC staff attending in addition to Walter Johnston and Julius Knapp included:

Michael Ha, FCC	Henning Schulzrinne, FCC
Gregory Intoccia, FCC	David Valdez, FCC
Ahmed Lahjouji, FCC	Henning Schulzrinne, FCC
Robert Pavlak, FCC	David Valdez, FCC

Meeting Overview

Dennis Roberson, TAC Chairman, began the asking the TAC members to introduce themselves. He noted that we needed to continue to focus on actionable recommendations and that had lots of material to review. He added that Marty Cooper was unable to attend the meeting as he was on his way to Italy to receive the Marconi Prize. He next introduced the new TAC members: Theresa Hennesy, Comcast; Lynn Merrill from NCTA which had merged with OPASTCO, and John Barnhill from Genband. The Work Group chairs next made their presentations, a copy of which is attached herein. Dennis Roberson concluded the meeting by asking people to begin to think about next year's program.

TAC Agenda

- Spectrum Frontiers Workgroup
- Spectrum Receiver Workgroup
- Resiliency Workgroup
- Communications Infrastructure Security Workgroup
- Wireless COTS Workgroup

Technological Advisory Council

Spectrum Frontier Working Group

23 September 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

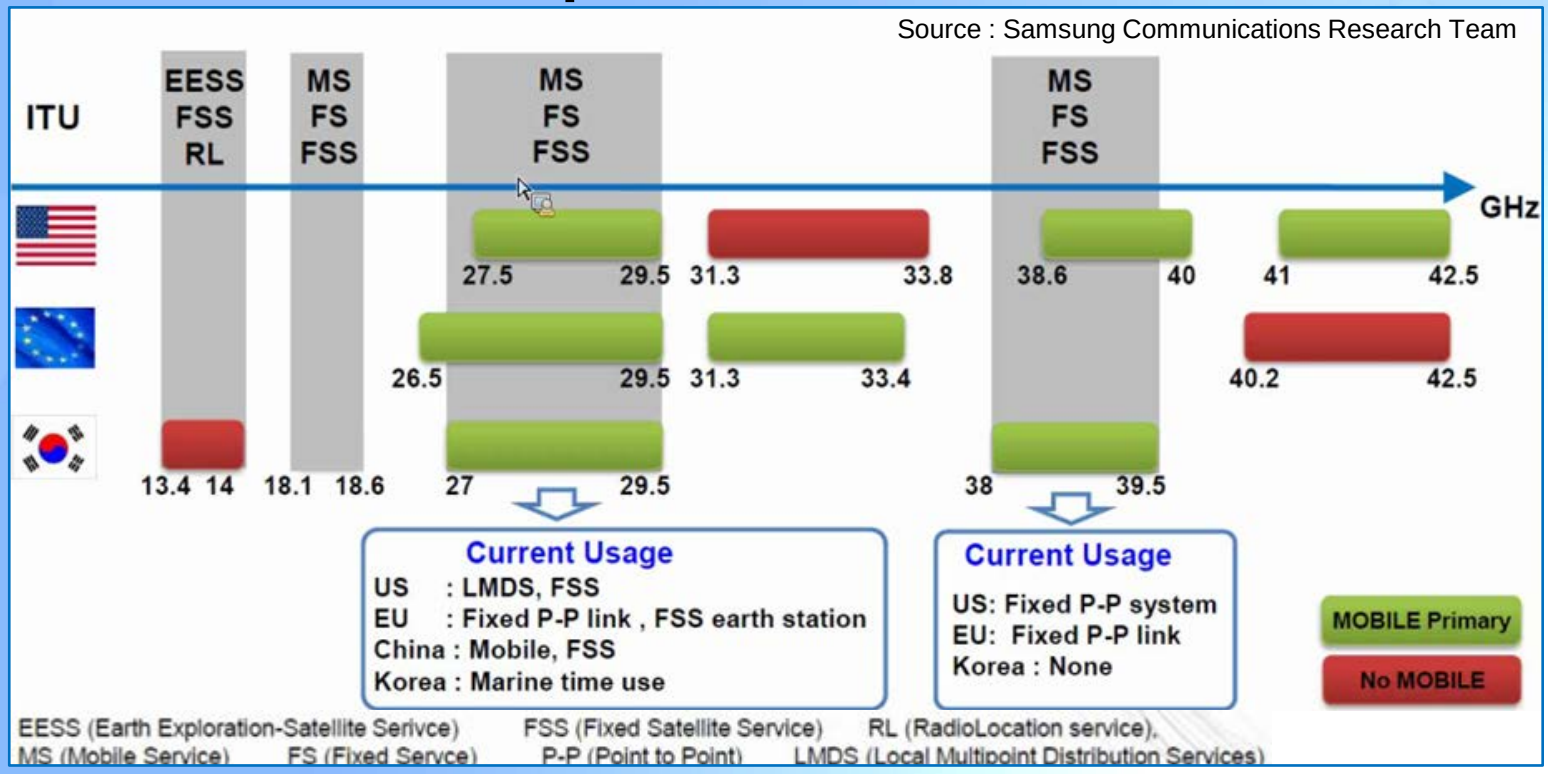
- Chair: Brian Markwalter, CEA
- FCC Liaisons: Michael Ha, John Leibovitz

- Mike Bergman, CEA
- Ed Chan, Verizon
- Bill Stone, Verizon
- John Chapin, DARPA
- Lynn Claudy, NAB
- Marty Cooper, Dyna LLC
- Adam Drobot, OpenTechWorks
- Milo Medin, Google
- Ramani Pandurangan, XO Communications
- Eric Miller, XO Communications
- Paul Steinberg, Motorola Solutions
- Bruce Mueller, Motorola Solutions
- Shahid Ahmed, Accenture
- Dale Hatfield, Silicon Flatiron
- Mark Bayliss, Visual Link Internet
- Jesse Russell, incNetworks
- Marvin Sirbu, Carnegie Mellon University
- David Tennenhouse, Microsoft
- Brian Daly, AT&T
- Mark Richer, ATSC
- Kevin Kahn, Intel

Overview

- June Meeting Recap
  - Presented the overview of higher frequency bands
  - Reviewed the key FCC allocations in mmW bands
  - Discussed Broadband activities in the lower mmW band
- Updates between June-September, 2013
  - 60GHz R&O: Allows higher power for outdoor application in the 60GHz unlicensed band
- This presentation explores:
  - 30-40GHz mmW activities review and WG recommendations
  - 95-275GHz band findings and planned activities
  - Terahertz band proposed applications and next steps

30-40GHz mmW – Spectrum Overview



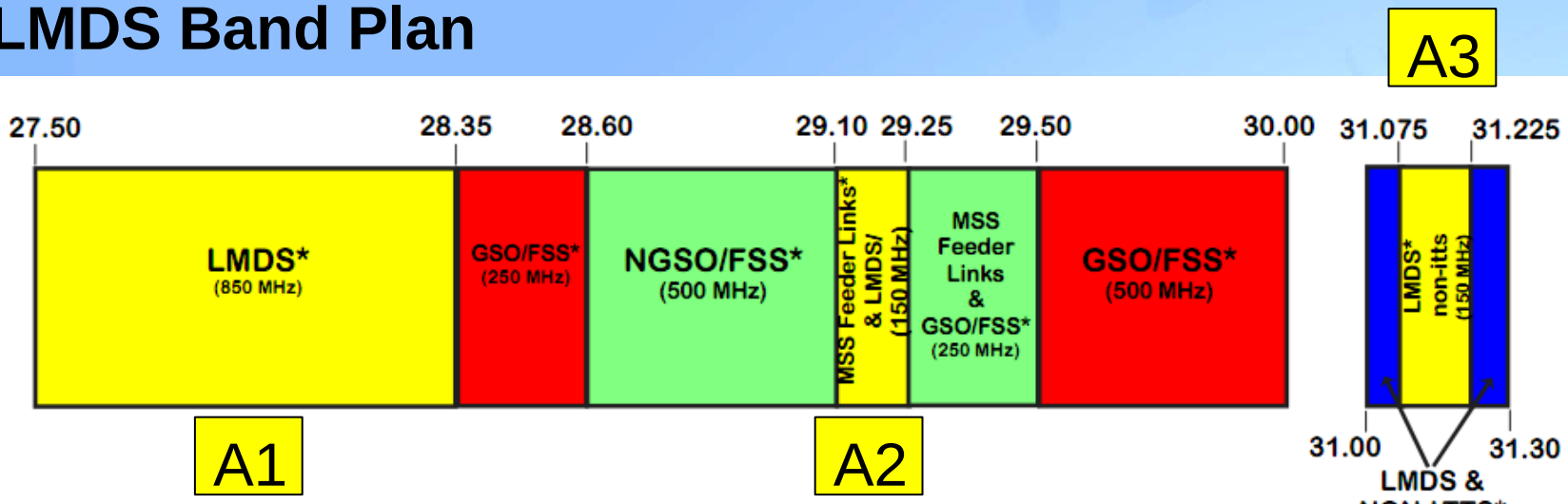
- Note: The Commission's Fixed Microwave (Part 101) and Satellite Communications (Part 25) service rules govern most of US Mobile allocations shown above

30-40GHz mmW – Current Activities

- LMDS (27.5-28.35, 29.1-29.25, 31.075-31.225, 31-31.075 & 31.225-31.3GHz)
  - 1.3GHz total spectrum, with a maximum of 850Mhz in one contiguous block
  - Governed by Fixed Microwave (Part 101) Service Rules
  - BTA licenses with coordination requirement
  - Mostly used for wireless backhaul
  - Certain licenses have been returned

- V-Band (37-38.6GHz, 38.6-40GHz, 42-42.5GHz)
  - Mixture of Fixed Satellite Service and Fixed Service
  - Services both Federal Government and non-Government entities
  - 3rd NPRM released on May 2004 and is still active

LMDS Band Plan



Two LMDS Licenses per BTA

Block A - 1150 MHz:
27,500-28,350 MHz
29,100-29,250 MHz
31,075-31,225 MHz

Block B - 150 MHz:
31,000-31,075 MHz
31,225-31,300 MHz

Legend

"*" - Primary Service
FSS - Fixed Satellite Service
GSO - Geostationary Orbit
NON-LTTS - Non-Local Television Transmission Service
MSS - Mobile Satellite Service
NGSO - Non-Geostationary Orbit

30-40GHz mmW – LMDS Application

- Most major market LMDS licenses were retained, particularly A-band.
- Majority are in A1 band (850 MHz contiguous).
- 1000+ links are in service nation-wide, primarily in the “NFL” markets.
- Applications: Cell tower backhaul (PTP); also fiber extensions, redundancy circuits
- Also: Interest for small cell backhaul; several links have been deployed in LA and operate in a non-line of sight environment.
- Returned licenses were typically in rural markets and/or B-block licenses.
- There are very few deployments in the A2, A3 and B1/B2 bands.
- There are limited Point to Multipoint deployments, primarily by ISPs.

30-40GHz mmW – Technology Enablers/Market Pull

- Smart Antenna Technologies
  - Beamforming with various sizes of array antenna has been proposed
  - Spatial Division Multiple Access (SDMA) and Spatial multiplexing can compensate for propagation deficiencies in these bands…
  - …but still challenged to overcome absorption issues such as rain and non-line-of-sight objects
- Silicon Technologies
  - RF components that enable mmW communications becoming more common
- Scalable Network Architecture
  - To interoperate with already deployed and planned networks for functions such as backhaul, short range, local access and direct cellular or nomadic services.
- Market Application
  - Growing demand for mmW links for redundancy to fiber backhaul.

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
  - Get on WRC-15 agenda for conclusion at WRC-18

95-275 GHz mmW – Intermediate Findings

- *Beamforming:* Physics leads to *beam shaping and steering* requirements. Solutions are in transition from R&D to commercial use.
  - "Basic" application is for fixed high-gain P2P antennas. Beam steering is used to locate and compensate against vibration and sway
  - "Advanced" application is mobility, compensating for barriers and for UE movement
- *Altitude Sharing at mmW:* Could separate out low altitude ("streetlight") and high altitude ("rooftop") licensing to enable sharing
- *Component Limits and Spectral Efficiency:* Clock speed cannot keep up with carrier frequency. Modulation must be done at a lower relative frequency; this yields a lower bits/Hz efficiency.

95-275 GHz mmW – DARPA 100Gb/s RF Backbone (100G)

- Military requires fiber-optic-equivalent capacity usable anywhere within their area of responsibility
- The program goal is a 100 Gb/s airborne-based communications link for 100-200 km range from high altitude in all weather
- Satisfying the DARPA RFP is likely to require an 80-120GHz solution.
- If the military adopts such technology, commercialization becomes much more likely
- However, the 100G project is a DARPA research activity; civilian commercialization is still years away.

95-275 GHz mmW – Planned Activities

- *Further investigation:*
  - Briefing by Dr. Dick Ridgway, DARPA Program Manager for the 100G RF backbone program
  - Discussions with manufacturers and industry players (commercialization, timeframes)
  - Discussion with Radio Astronomy community
- *Under consideration:*
  - Working group is aware of IEEE petition related to service rules above 95GHz
  - Continue investigation of technologies applicable above 95 GHz
- *For December:*
  - Provide an assessment of the expected applications and commercialization timeline and how they might relieve congestion in lower frequencies

Terahertz Envisioned Applications

- Small Cell
  - Cells covering 10's of meters, pedestrian on the street application
  - Track UE with highly directional antennas
  - Technology not ready
- Wireless Kiosk
  - Sync-N-Go application, 10 Gbps, less than 1 m
  - Already served by 802.11 and 60 GHz
- Wireless Data Center
  - Switched P2P 40-100 Gbps data distribution within data center
  - Range up to 100 m
  - Expect 10's of mW power with 20 dB gain antennas
  - Current project of the IEEE THz Study Group

IEEE 802.15 SG100: THz Study Group

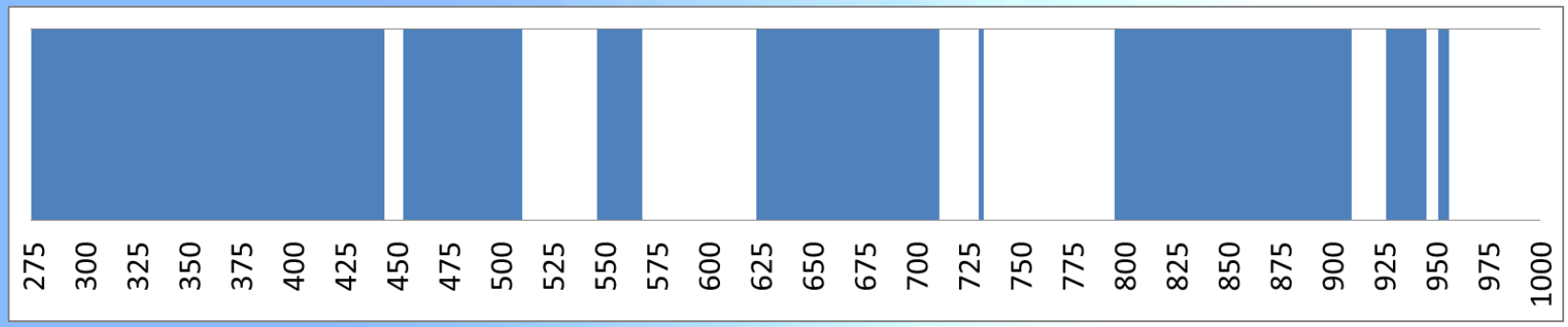
- Dr. Thomas Kürner, chair of THz SG, gave overview
- Formerly an Interest Group, in July it became Study Group (SG 100G)
- Motivated by familiar march to higher data rates
- Issues to consider
  - Cost of components, commercial viability
  - Antenna technology, especially beamforming
  - Interference with passive services
- Next step
  - The SG will develop the THz Wireless Data Center concept
  - Homepage : http://www.ieee802.org/15/pub/SGthz.html

ITU Radio Regulations Footnote 5.565

The frequency band 275-1000 GHz may be used by administrations for experimentation with, and development of, various active and passive services.

- Radio astronomy service: 275-323 GHz, 327-371 GHz, 388-424 GHz, [...]
- Earth exploration-satellite & space research service 275-277 GHz, 94-306 GHz, 316-334 GHz, [...]

Administrations are urged to take all practicable steps to protect these passive services from harmful interference.



Significance of Footnote 5.565

- As written allows:
  - Transmission in free parts of spectrum; or
  - Coexistence with radio astronomy and earth exploration

- Barrier to commercial use of passive bands may not be as high as it seems. Allocations can change as commercial interest becomes more specific.

- IEEE THz SG is following coexistence path for following reasons
  - Insufficient contiguous “free” bands
  - Coexistence practical for terrestrial short range applications like data centers
  - Physics of these frequencies conducive to coexistence

Further Consideration

- Support FCC, as needed, in pursuit of three recommendations for 30-40 GHz range
- Provide an assessment of the expected 95-275 GHz applications and commercialization timeline and how they might relieve congestion in lower frequencies
- Understand passive services and how future commercialization and allocations will work

Technological Advisory Council

Spectrum / Receiver Performance

Working Group

23 September 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

- Implementation of Interference Limits Policy
- Multi-Stakeholder (MSH) Groups
- Radio Service Standards Knowledge Base
- Emerging Technologies
- Interference Resolution and Enforcement

Piloting Harm Claim Thresholds

- 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 Not-In-My-Back-Yard (NIMBY)
  - 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
- **Recommendation**
  - **FCC should encourage formation of a multi-stakeholder group to investigate interference limits and the use of harm claim thresholds in the 3.5 GHz band**
- Recap
  - Interference limit policies: “ways to describe the environment in which a receiver must operate without necessarily specifying receiver performance”
  - Harm claim thresholds: “in-band & out-of-band interfering signals that must be exceeded before a system can claim that it is experiencing harmful interference”

Why 3.5 GHz?

- Advantages
  - Explicit or implied support for interference limits approaches in various comments/replies, and overlap in filers on Interference Limit PN and 3.5 GHz NPRM
  - Some technical data on receiver characteristics already on the record, e.g. from Content Companies, Baron Systems, Google
  - Indications of unselective receivers in-band and adjacent band
- Disadvantages
  - DoD incumbents in-band and adjacent
  - Diversity of coexisting systems, e.g. radar / comms best practices still under development in other venues

Use of Harm Claim Thresholds (HCT) in 3.5 GHz

- Three protection tiers proposed in NPRM: Incumbent Access (Tier 1), Priority Access (PA)(Tier 2), General Authorized Access (GAA)(Tier 3)
- Protection of incumbents
- HCTs explicitly defines protection Tier 1 needs from Tier 2 and 3 services
  - Provides basis for defining operating rules for Tier 2 & 3 services, either in rules and/or ad hoc using spectrum access database
- Additionally: HCTs for Tier 2 services can be used to
  - Optimize PA deployment by defining what protection they need from each other
  - Define interference protection Tier 2 requires from Tier 3
  - Provides basis for defining operating rules for Tier 3 services, either in rules and/or ad hoc using spectrum access database

Stakeholders: Likely Players in MSH Process

- In-band and adjacent incumbents
  - Federal: DoD
  - Non-federal: fixed satellite services, both comms downlinks and content companies
  - 3650-3700 “light licensed” operators
- 3.5 GHz new entrants
  - Commercial cellular operators and vendors
  - Electrical utilities
  - Unlicensed operators, vendors and interest groups
  - Hospitals / Public safety
  - Others?

Multi-stakeholder (MSH) Organizations

- Current study items and status
  - Compare and contrast MSH and other regulatory approaches
    - MSH versus rulemaking, negotiated interference, FACA approaches
  - Explore levels of increasing guidance from the MSH as outlined in TAC White Paper
    - Examined appropriate level of FCC participation for best results
  - Scenario descriptions for MSH use at candidate band/allocation boundaries
    - Examining the process in detail

General Advantages of Using MSH Organizations

- Flexibility allows for tailored approach to specific issues
- Informal process allows fast responses
- Collegial approach fosters collective problem solving
- Powerful tool in clarifying relevant assumptions and identifying legitimate disagreements

Possible Disadvantages of Using MSH Organizations

- Lack of single authority opens possibility of intractable disputes that stall progress
- More powerful stakeholders may dominate discussion
- Potentially diminished disclosure
- Agreement requires additional process to gain force of law
- Difficult to represent nascent or diffuse interests

Disadvantages of Other Potential Methods for Developing Harm Claim Thresholds

- Notice and Comment Rulemaking
  - Slow, not flexible, can be complex
- Federal Advisory Committee
  - Recommendations require additional process to implement, full representation of stakeholders challenging
- Negotiated Rulemaking
  - Sensitivity of absent parties, has not been successful in practice

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

Appropriate Level of Involvement of FCC in Multi-Stakeholder (MSH) Organizations

- FCC supervised process:
  - Effectiveness of MSH is hampered – similar to slow notice and comment rulemaking
- No FCC input:
  - Effectiveness of MSH is hampered – disagreement among marketplace competitors may stall decisions
- Encouragement by FCC and monitoring role:
  - Effectiveness of MSH is maximized with optimized level of government involvement
  - Highlight bands where multi-stakeholder process may be useful
  - Highlight questions and topics where multi-stakeholder input could assist (or obviate) rulemaking

Potential Process and Structure for a MSH Organization

- Initiating involvement
  - “Signal” from FCC that input from the MSH would be welcome in recommending harm claim thresholds in a particular frequency band
- Potential structure of MSH Organization
  - Non-profit corporation independent of federal government
  - Widely balanced stakeholder groups represented
  - Technology-focused
  - Open and transparent process
  - Funded from membership dues
  - One umbrella organization with sub-groups or separate organizations for different situations?

Radio Systems Standards Knowledge Base

- Purposes:
  - To inform system and receiver developers of standards applicable to devices that may be found in adjacent bands and changes to their potential RF operating environment based on those devices.
  - To serve as a resource to regulators in deciding on assignment of compatible adjacent services.
- How can we develop a sustainable standards knowledge base?
  - TAC cannot maintain a knowledge base and keep it up to date.
  - FCC unlikely to have sufficient resources to maintain such a knowledge base, given the high volume and rate of change of standards specs
  - Many standards are not readily available without purchase or subscription.
  - Many **S**tandards **D**evelopment **O**rganizations have been identified.

Radio Systems Standards Knowledge Base

- **Recommendation: FCC Should Issue a Notice of Inquiry (NOI) to initiate SDO action**
  - Prompt standards organizations to volunteer to maintain a standards knowledge base
  - 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
  - Does NIST figure in to this type of effort?
- The end result will be a Knowledge Base
  - SDOs maintain lists of standards associated with each FCC Rule Part, Rulemaking Proceeding and/or Frequency Band
  - References to SDOs maintained by FCC OET in document form
  - Possible Spectrum Dashboard references
  - Other references when no standards exist

Emerging Technologies

Goal:

- To investigate receiver and transmitter design techniques that improve efficient use of the spectrum, and related policy implications

Product:

- List of techniques being researched that show promise in improving spectrum efficiency often by increasing interference tolerance
- Assessment of related policy and regulatory implications

Results to date:

- Identified key technologies, including:
  - Software defined receivers and transmitters
  - Interference cancellation and coordination methods
  - Advanced receiver technologies (e.g., high dynamic range A/D and RF front-end)
  - Advanced antenna and multi-carrier technologies (e.g., MIMO, carrier aggregation)
  - RF MEMS and dynamically tunable front-end filters
- Tentative analysis of policy implications (see Background Slides)

Interference Resolution and Enforcement

Goal:

- Recommend policies to establish standardized procedures for interference resolution and enforcement in an increasingly complex spectrum environment

Product:

- Issue 4Q'13 TAC report on the issues and scope of FCC work for interference resolution and enforcement in a spectrum sharing environment

Background:

- Historical incidents (e.g., "garage door opener" issue)
- Government and commercial spectrum user needs (federal and non-federal)
- Legislative and policy actions (e.g., CSMAC, PCAST, GAO, FCC PN, etc.)
- Spectrum sharing, increasingly crowded / dynamic environment, heterogeneous systems & standards, advancing technology, reduced budgets
- Need for coordinated practices, tools, for resolution and enforcement

Interference Resolution and Enforcement

Results to date:

- Background review, including:
  - Analysis of FCC rulemaking; use of statistical and deterministic worst case assessments of interference
  - Definitions of types of interference
  - Traditional enforcement tools, interference resolution and enforcement steps
  - Risks and challenges associated with evolving technology
  - Limitations and opportunities for advancing tools and processes
- Identified key success factors (CSMAC and TAC), including:
  - FCC enforcement tools for new forms of spectrum sharing
  - Methods of FCC and NTIA coordination when both federal and non-federal users are involved
  - Mitigation measures prior to resolving source(s) of interference
  - Technical compliance showings to facilitate enforcement measures

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 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	

Table of contents

COTS Working Group Mission Statement

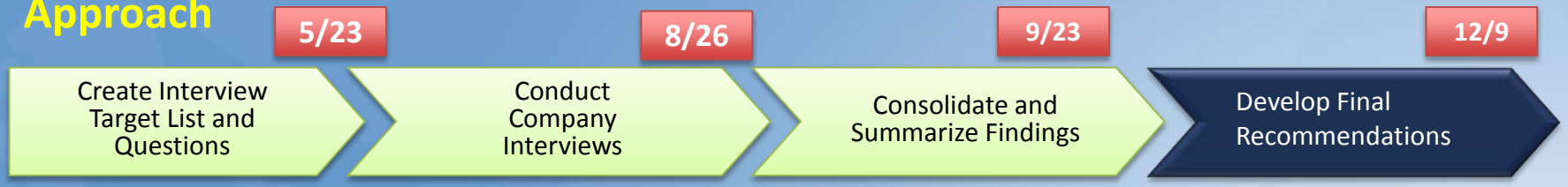
Find ways to leverage technical and commercial benefits of scaled wireless solutions to:

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

Our Preliminary Recommendations

1. Formalize a Commission COTS definition for ‘Commercial-Off-The-Shelf’ technologies and services

2. Identify spectrum sharing opportunities in under built commercial areas

3. Workshop on Enterprise Services in Broadband Network

Preliminary 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 industry, leading to costly solutions that are not interoperable between industries (i.e. Pubic Safety and Utilities)
- **Recommendation**
  - Formalize a Commission definition that defines COTS from a service and technology view point
  - Work with the Industry, Service Providers and Technology Vendors on developing a 'COTS' Program per Industry Sector
- **Complexity/Timeframe to Implement**
  - **Long Term**

Preliminary Recommendation 2: Identify spectrum sharing opportunities in under built commercial areas

- **Situation**
  - Given disparity in the service areas covered by Organizations and Service Providers, the former 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**
  - Cover Spectrum Sharing as part of a broader workshop that that discusses Enterprise requirements for Wireless Broadband Services (as described in Preliminary Recommendation #1).
- **Complexity/Timeframe to Implement**
  - **Short-term**

Preliminary Recommendation 3: Workshop on Enterprise Services in Broadband Network

- **Situation**
  - Organizations across industries have concerns about Service Providers not providing the quality of service 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**
  - Hold 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
- **Complexity/Timeframe to Implement**
  - **Short Term**

Next Steps

1. Further define preliminary recommendations
2. Collect feedback and agreement from workgroup
3. Present final recommendations at TAC meeting on 12/9

Appendix

#	Key Themes	Importance
1	Security	Security remained consistent among interviewees as the top risk of using COTS based products. Security vulnerabilities in COTS products can introduce significant risk into an organization's network. *(Southern Company - most COTS products go through additional security hardening to meet corporate infrastructure security requirements).*
2	Cost	Interview participants agreed that COTS products reduce cost and time to market, allowing for a broader vendor ecosystem and lower refresh/development cycles. Conversely, OEMS are leveraging COTS implementation to multiple verticals with the same product lines. *(Samsung – Develops consumer products and replicates the products for enterprise based customers. For example, Galaxy S4 devices are now being equipped with chip-based security mechanisms to accommodate multiple vertical market applications – i.e. Government)*
3	Reliability	Reliability is viewed as the top gating factor for using COTS based products in the Utility industry. The majority of the products that are deployed to the field are COTS-based. Therefore, they are required to be harden and resilient. *(Southern Company – Challenge: Carriers provide public networks (non-resilient, mission critical, or hardened) and Public Safety always has priority 1 over the network in mission critical response. This puts Utility industry in a priority 2 situation for communication services.)*

#	Key Themes	Importance
4	SLA / QoS	Commercial network's business models are not SLA-driven. Thus they can not ensure service delivery for some critical vertical market applications and functions (e.g. PTT or Mission Critical Data). OEMs recognize that and are using COTS technologies to circumvent the networks and allow for service delivery to be controlled by the user. *(Qualcomm – Development of LTE-direct will allow a COTS product, such as a smartphone to use COTS technologies – LTE – to communicate directly with other devices using a standards-based stack)*
5	Interoperability	Using a COTS technologies based on global standards (i.e. 3GPP) allows for greater interoperability at lower costs. Seamless interoperability can enable specific vertical markets to leverage commercial networks to a greater extent, while using private COTS implementations to provide specific applications or features. *(Qualcomm – LTE Direct, Air-to-Ground Communications and private Small Cell deployments allow for industries to leverage COTS to provide industry-specific applications over COTS technologies or commercial networks)*
6	Data privacy	Customer Data Privacy issues when using COTS technologies and commercial networks were raised from the industry-specific OEMS. As customer data gets placed on shared infrastructure, ownership and use of that data becomes a risk. *(Ford – Significant risk for using commercial networks to send in-vehicle and customer data to the cloud is around ownership of the data. Is this data owned by the vehicle OEM or by the service provider?)*

- Other Key Themes
  - Spectrum
  - Availability
  - Enterprise Needs vs. Individual Communication

TAC Resiliency WG

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

Resiliency WG

September 23, 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)

WG Summer Actions

- 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
  - Intent statement
- Liaison with Security team, and emergency services
- Weekly/regular sub-group meetings
- Regular all-hands meetings to share data
- Whitepaper outline, start of detailed information (*special thanks John Barnhill)*

The IP Transition – *It's the Power Supply*

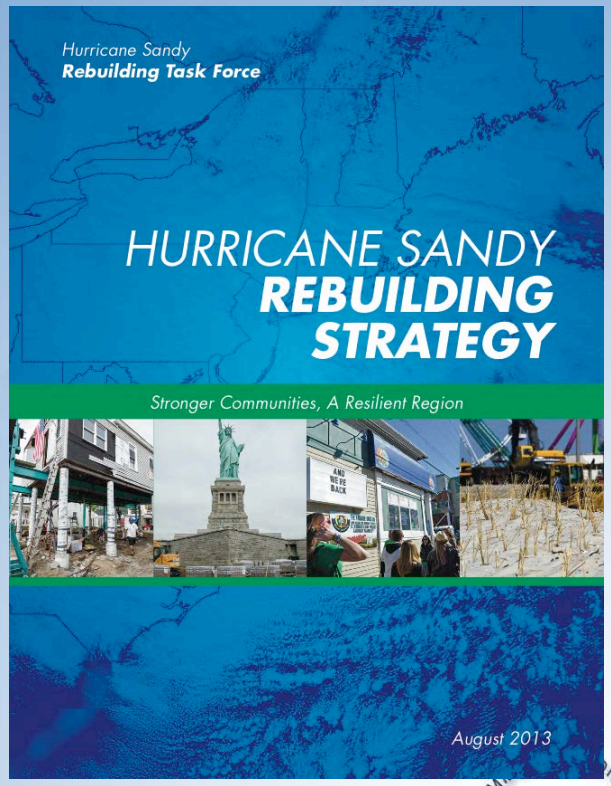
- Power availability has emerged as the single most-impactful issue tied to resiliency
  - -48v CO Powered vs Premise Powered
    - the network has evolved
  - Consumer devices: broadband modems/routers, PCs, tablets & smartphones
  - Service Provider: broadband access elements, NIDs, pedestals, wireless towers, routers etc.
  - Application Service Provider
    Network applications infrastructure.
  - Coming Impact of Internet of Things (M2M)
    - Payments, monitoring, additional power requirements

Hurricane Sandy Rebuilding Task Force – 19 Aug 2013

- RECOMMENDATION 16

  "Develop a resilient power strategy for wireless and data communications infrastructure and consumer equipment."

- Network Infrastructure
  - Function Thru Electrical Grid Outage
    - Cellular towers (antennas), Data Centers, and Other Critical communications
- Consumer Equipment
  - Encourage stored power (i.e., batteries) for consumer broadband equipment

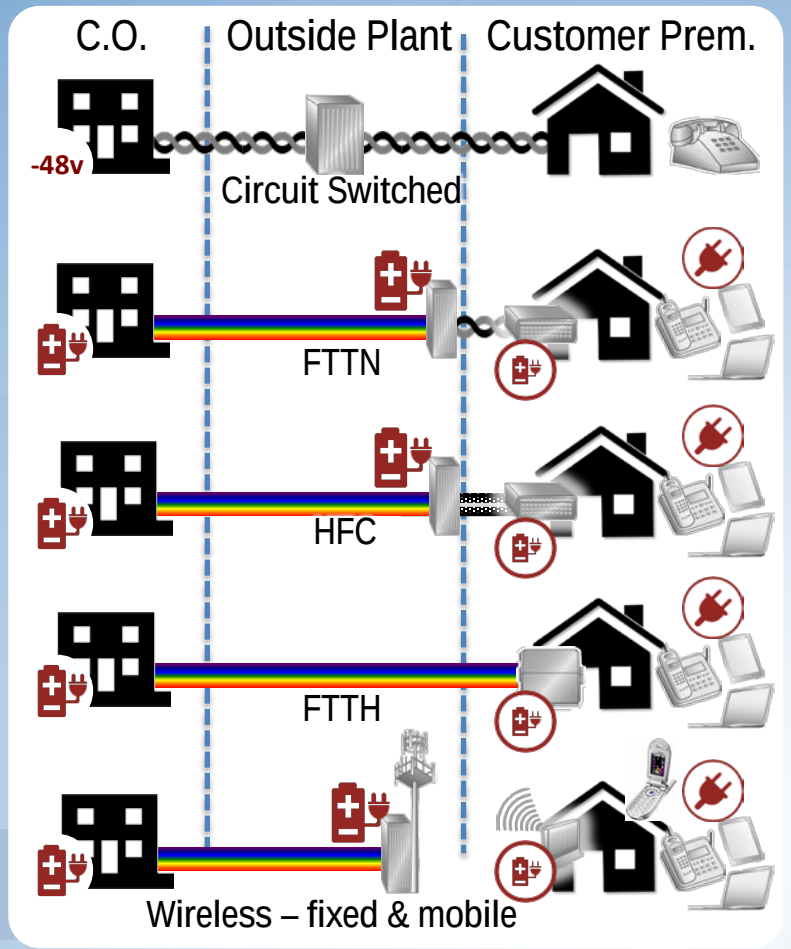


http://portal.hud.gov/hudportal/documents/huddoc?id=HSRebuildingStrategy.pdf

Dept. of Energy and NTIA prime to work with FCC on plan

Physical Plant

- Common theme: Power reliability & availability
- Issues Summarized in 3 Areas:
  - Consumer CPE: Little or No Battery Backup
    - Power reliability is critical, many devices
    - Line power is now the exception
    - Some Service Providers provide batteries, but maintenance is consumer dependent
  - Distribution/Last Mile: Limited Power Backup
    - Varied architectures: FTTH, FTTN, HFC, xDSL, etc
    - Cell Sites and Small Cells
    - Power practices vary widely by service provider
  - Wire Centers / Head-ends
    - Normally equipped with Battery or Generator Backup and can self-power
    - Power back up practices vary by service provider



Physical Plant – Assessment

- Power oversight is outside of FCC control
- No formal FCC liaisons to FERC or other power regulations groups
- Lack of shared priorities between power companies and providers
- Although some best practices, no uniform or common program in place, no back-up power rules
- Priority of restoration is lacking. hospitals, PS/E911, critical businesses, consumers
- “Clear-cutting” by power companies removes working plant
- Regional and Local peering issues- single points of failure

Services Substitution

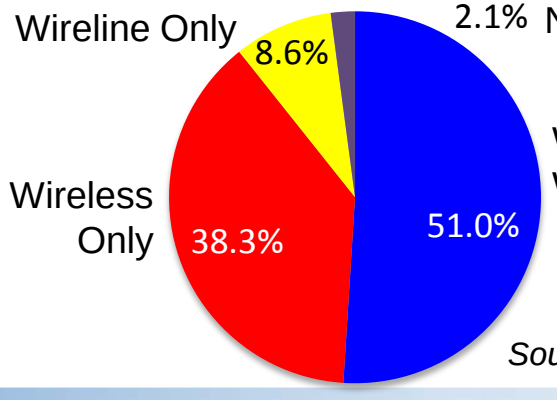
Impact on Household Communication Resiliency

Multiple Service = Higher Availability

- Availability of diverse services creates higher potential household resiliency
  - Growing deployments of Wireless, VoIP and Broadband households
    - 89.3% of Households have wireless phone.
    - 80% have either fixed BB or a smartphone
      - Educational Attainment, Age and Income are most likely predictors of adoption
  - New/ Growth of overlay networks
    - Wireless and Muni Wifi are recovery options (>160k hotspots to date)

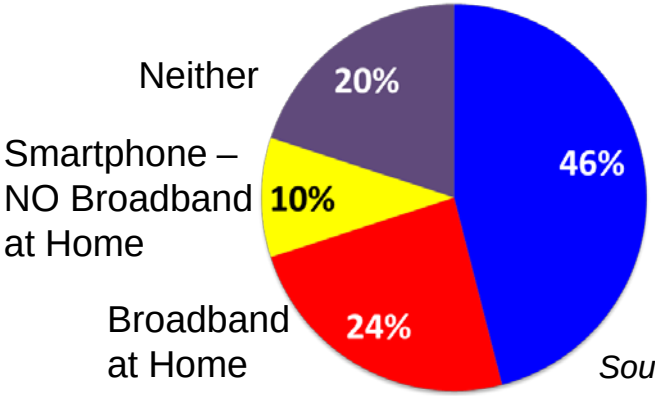
Most Americans have more than one way to communicate

Voice Deployment (% of US Households)



Source: CDC

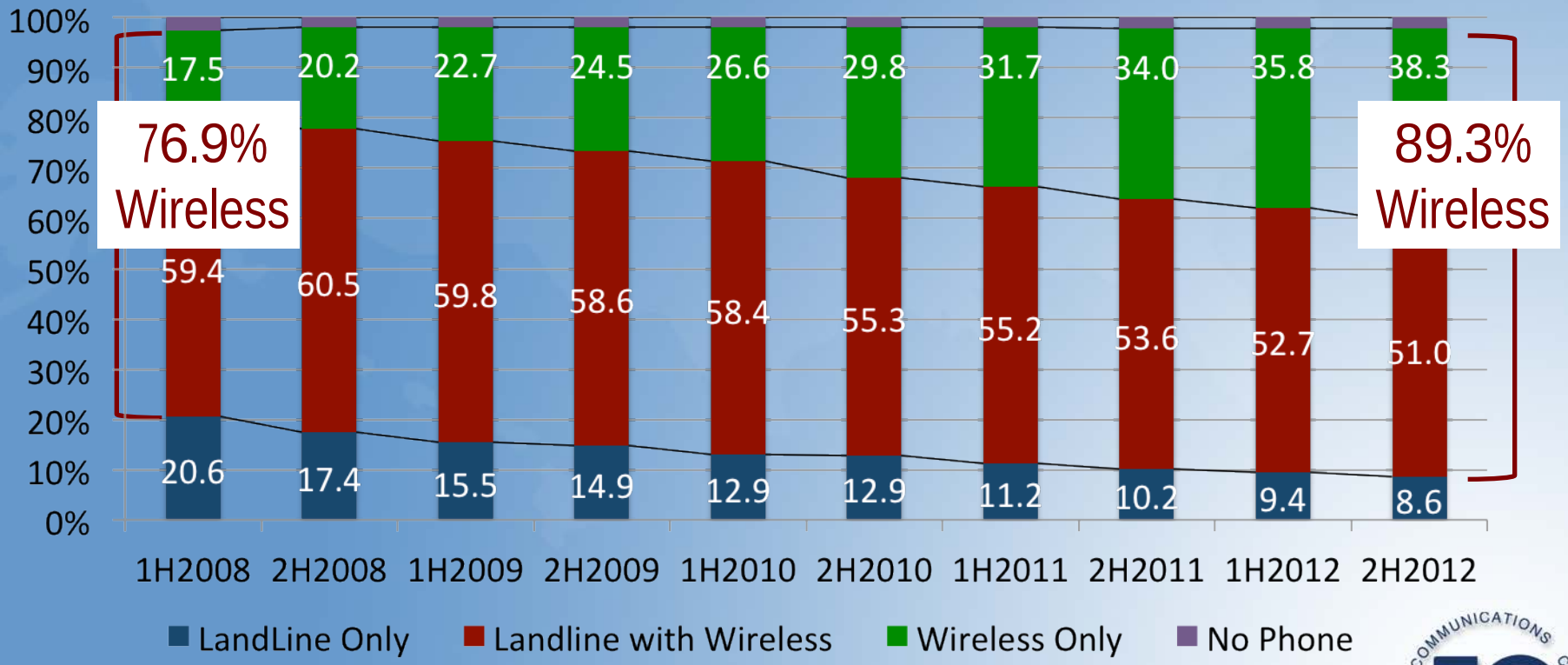
Broadband Deployment (% of US Adults)



Source: Pew Center

Household Resiliency Trend

% of US Households by Communications (Voice) Modality



Blumberg SJ, Luke JV. Wireless substitution: Early release of estimates from the National Health Interview Survey, July – December 2012. National Center for Health Statistics. June 2013. Available from: http://www.cdc.gov/nchs/nhis.htm.

Industry Recovery Options

Emergency Restoral

Best Practices

Industry Provided Disaster Resources

- Mobile Incident Command
- Human Needs Trailers
- Emergency Communications Equipment (e.g. COLT)
- Restoration Equipment
- Wireless &Muni Wifi

- CoLTS & COWS, Mobile Wifi Trailers available
- Recovery: Industry best practices are emerging
  - Roaming agreements
  - Opening wifi to all during restoration

Infrastructure Sharing: CableWiFi

- Major infrastructure sharing initiative being driven by providers
  - A coordinated, shared network during restoration
- Began in 2012 with 50,000 hot spots, a joint venture between:
  - Bright House Networks, Cablevision, Comcast, Cox Communications Time Warner Cable
- Collaboration with state and local governments is expanding reach
- Customers potentially have access to over 165,000 hot spots nationally, and growing daily
- Available in larger cities/metro areas, typically
- Able to offload 4G cellular services
- Use Case: during hurricane Sandy Comcast opened up network

R^3 = **R**esiliency, **R**esponse, **R**estore

- Cellular/wireless networks may be more resilient than landline (fewer elements in access network)
- Cell Sites – Battery or generator backup
  - Policy varies by service provider
- Cells-on-Wheels (COWs), Cell-on-Light-Trucks (COLTs) & Repeaters on Trailers (RATs)
  - Full functioning generator powered cell sites can enhance or replace network coverage and capacity in an area.
  - Used in emergency response situations – enhance communications between firefighters in remote areas.
  - Examples: recent CAL wildfires, OK hurricanes, super-storm Sandy

Reporting, Metrics & Forecasting

How to move from “Forensics” to “Predictability”

Reporting, Metrics, Forecasting

- **General reluctance to re-create circuit-switched era metric reporting for VoIP**
  - Avoid placing administrative burden on service providers for data requests
  - FCC requires outage information from Interconnected VoIP providers – with exceptions
  - No reporting is currently required for underlying broadband infrastructure.
- **Guiding questions on principles for data collection:**
  - What is desired goal/outcome of data collection?
  - Is the right data being collected to achieve the stated goals?
  - How will regulatory bodies use the collected data?
  - Will data be public or private?
  - Will data be used to establish a service baseline for comparison?
- **Providers proactively gather extensive internal data to manage their own network performance**
  - Is there a way to tap or utilize this data for disaster resiliency?

Reporting, Metrics, Forecasting

Proposed statement of intent for 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**.*

Preliminary Recommendations & Next Steps

WG activities Oct-Dec:

Actionable Recommendations

Physical Plant Team – *Preliminary* Recommendations

- **Formal Consumer Education & Responsibility program** *Workshop*
  - service options/substitution
  - power back up options
- **FCC & Power Industry Regulators** *Summit*
  - Leverage Hurricane Sandy Rebuilding Strategy Action Report
  - National program on collaborative restoration. Coordination between regulatory organizations
  - FCC liaison to state PUCs and power regulations groups
- **Providers: a leadership role**
  - CPE: Product design requirements to CPE vendors: efficiency, chaining, service labeling (back-up)
  - CPE: Take part in consumer education through service labeling, backup options
  - Power: Providers actively monitor power supplies throughout distribution network (CO/Headend to CPE)
  - CPE WiP: http://www.ncta.com/news-and-events/media-room/article/2453
- **CEA: Labeling and Efficiency** *Workshop*
  - FCC can play a role to accelerate implementation

Preliminary Policy Recommendations

- **Data Exchange**: Creation of a common or shared database among the key infrastructure providers.
  - Leverage the power monitoring capability of the providers
- **Joint Policy** with power providers required: the national communications system is highly dependent on reliable power.
  - FCC to lead alliance with Power industry/regulators
- **Provider Restoration Sharing Policy**
  - Prioritization
  - Coordination during restoration process
  - Regional and local peering options

Reporting, Metrics, Forecasting

- Preliminary Recommendations
  - FCC to develop Data/Analytics ability; for current and added contextual data
  - FCC to leverage DIRS and NORS outage data
  - Leverage FCC MBA program for broadband data sources
  - Partner with Power, CDC, DHS, FEMA, E911, etc for data access/sharing,

Areas for the WG to Explore

- Power back-up recommendations for various active network points
- Applying metrics to the underlying network for VoIP services
- Explore ways to modernize data collection/analysis, set baseline-NOI?
- Data exploration by academics and industrial researchers
- Disseminate reliability data to consumers on services
- MBA program as source of BB resiliency data; greater penetration for localized data capability
- CEA, Broadband Forum, CableLabs, etc create labels, a standard CPE plug related to power
- Provider labeling of equipment to provide consumer awareness

Comments and Feedback

Resiliency WG

Back-up Material

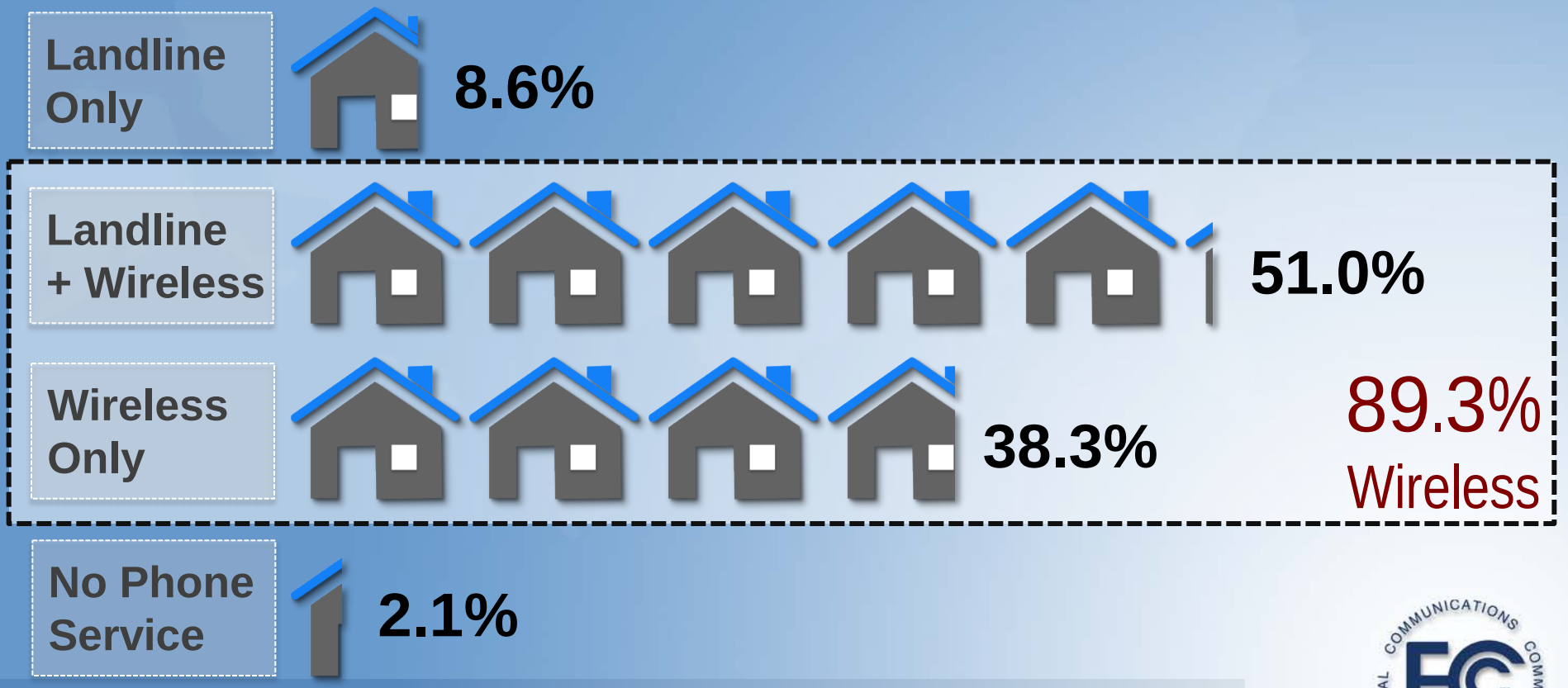
Physical Plant: *Proposed Events*

- **Workshop #1: Consumer Awareness**
  - The FCC host to foster and create educational material on guidelines for consumers in relation to power back up
- **Workshop #2: CEA & other relevant parties**
  - CEA: FCC to promote labeling, efficiency, ease of design
- **Physical Infrastructure Reliability Summit:**
  - Leverage Hurricane Sandy Rebuilding Strategy Action Report
  - FCC to lead collaboration with other government entities wrt to power reliability and restoration

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, plus local and regional peering
- Specific issues for rural infrastructure

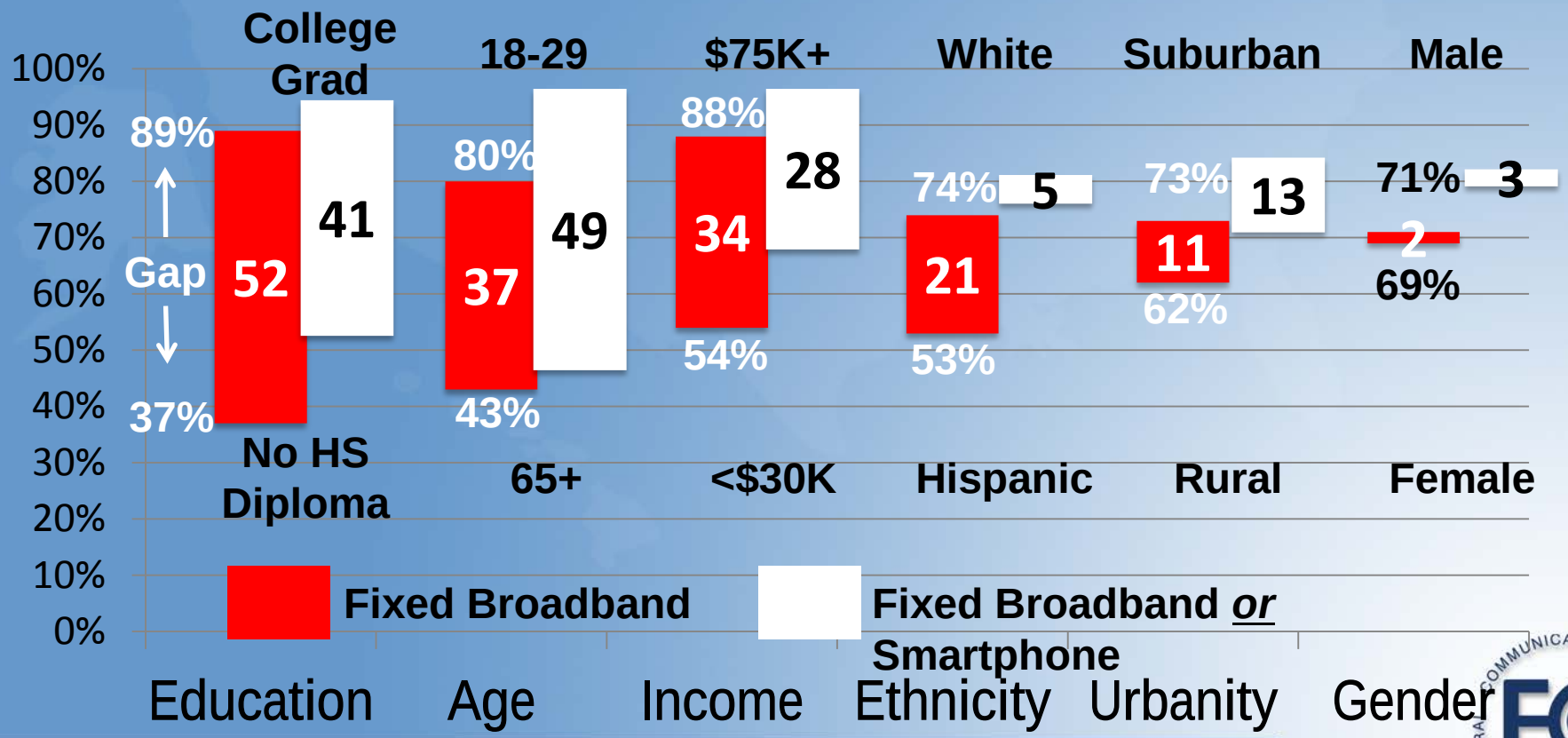
Wireless Dominates Household Communication



Blumberg SJ, Luke JV. Wireless substitution: Early release of estimates from the National Health Interview Survey, July – December 2012. National Center for Health Statistics. June 2013. Available from: http://www.cdc.gov/nchs/nhis.htm.

Broadband Gap Demographics

% of US Adults



Source: Pew Research Center's Internet & American Life Project Spring Tracking Survey, April 17 – May 19, 2013

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?

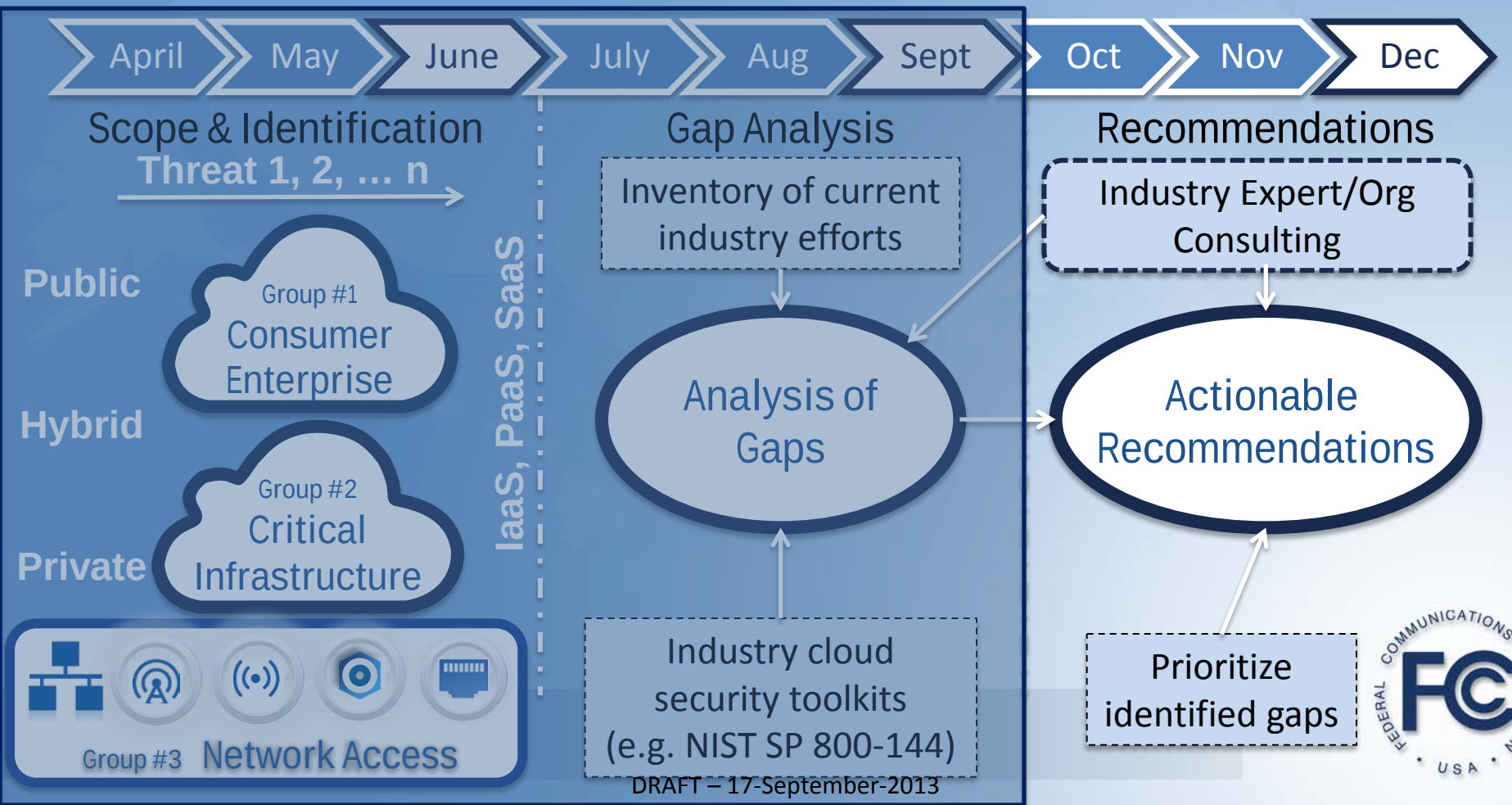
Mission Statement Key Objectives

- 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)
  - 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



Work Group Summary

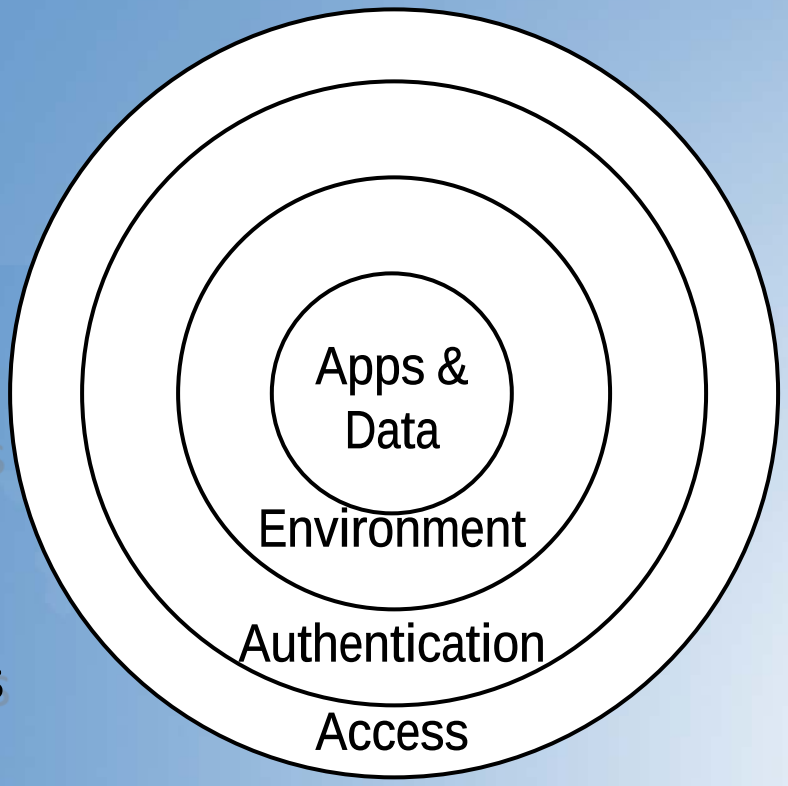
- Operated as Parallel sub-groups
  - WG #1: Consumer/Enterprise, Public Cloud Topologies
    - Leader: Joe Wetzel, with Mark Bayliss, Peter Bloom, Dick Green, Deven Parekh, Jesse Russell and David Tennenhouse
  - WG #2: Critical Infrastructure, Private Cloud Topologies
    - Leader: George Popovich, with Adam Drobot, and Paul Steinberg
  - WG #3: Network Access
    - Leader: Harold Teets, with John Barnhill, Lynn Merrill, Mike McNamara, G (Ramani) Pandurangan, Donald Tighe, Joe Wetzel
- Conducted Industry Research to Ascertain Key Cloud Use-cases and Associated Security Issues
  - Expert Interviews across a wide range of disciplines and roles
  - Industry Research into other entities operating on cloud security
- Outputs
  - Ascertained common themes and issues (across multiple WGs)
    Identified some Common themes from Mobile Device Security work of TAC 2012
  - Developed [intermediate] Whitepaper documenting key Use-cases and Gaps
  - Developed prioritized Cloud Security Gap list for development of recommendations

WG #1: Consumer/Enterprise Cloud Security

Consumer & Enterprise Cloud Implementation

Approach

1. Understand total Security Context
2. Study Industry efforts & talk to various constituents
3. Form hypothesis regarding gaps
4. Recommend actions to address gaps



Use of the cloud is just a part of how to implement Applications for Businesses & Consumers

Consumer & Enterprise Cloud: Exemplary Use Cases

- Enterprise IT Group outsources Desktop productivity apps to a SaaS provider within a public cloud environment. Accountability for data and application security is joint between the cloud SaaS provider and the customer
- Within the Enterprise Environment, a non-IT group creates a productivity application and launches it via a public cloud
- A consumer chooses to back up their private data in a public cloud environment

Consumer & Enterprise Cloud Implementation

Sources of Input

- 1 Govt Agency
- 2 Cloud Consulting Groups
- 2 Enterprise Business Cloud/ Network Providers
- 20+ Standards/ Industry forum reviews

Observations

- Mature IT Orgs. are better equipped to understand their risks and to make deployment decisions
- Many less mature IT shops don't have the ability to deploy the entire secure solution, rather aim to deal with specific pain points
- The language around security is not uniformly understood
- All pieces of the security picture need to be addressed when moving apps to a public cloud

Gaps

- Audit of application software before moving to the cloud
- Clear Accountability for security functions
- Cloud provider audit with enough uniform detail to be helpful to small IT shops that can't do extensive due diligence.

WG #2: Critical Infrastructure Cloud Security

Group 2: Research Methods and Results

Approach

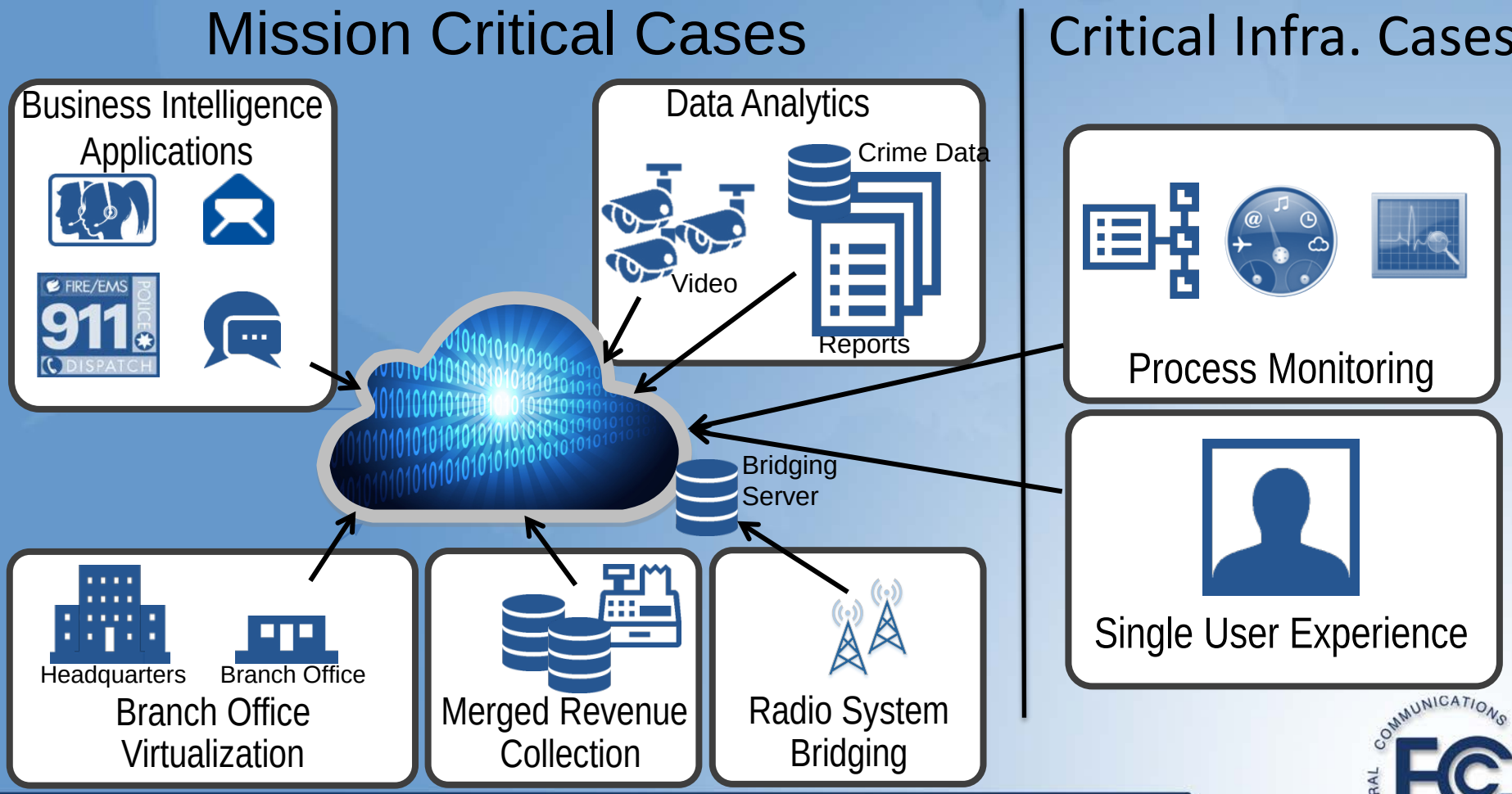
- Standards Document Scans
- Industry Use Case Scans
- Certification Bodies Research
- Trade Magazine Articles
- Industry Forums

Solicited Feedback

- State CIOs
- Public Safety Professionals
- CJIS Application Hosting Experts
- Corporate IT Specialists
- Cloud Consortiums
- Public Safety Applications Experts

Discussion Take Aways

- **Education to help agencies understand what the cloud is and how it can be used**
- **Guidelines for small to mid-sized agencies need to be developed (certified vendors)**
- **Mission critical apps require private/community clouds**
- State/local agencies need help to support auditing efforts
- SLA templates are needed to help define and capture responsibilities between user and provider
- Public safety is concerned about data privacy and physical location
- Security is the responsibility of both user and provider
- In Europe, clouds are considered Critical Infrastructure
- CJIS Policies will impact usage for users of CJI data


Mission Critical Cases
Critical Infra. Cases
Business Intelligence Applications
FIRE/EMS
911
POLICE
DISPATCH
Data Analytics
Crime Data
Video
Reports
Process Monitoring
Bridging Server
Single User Experience
Headquarters
Branch Office
Branch Office Virtualization
Merged Revenue Collection
Radio System Bridging

Mission Critical and Critical Infrastructure Gaps

- **Education**
- **Identity and access management**
- **Cloud certification programs**
- SLA contract language
- Clean Room Sponsors
- Advanced Persistent Threats
- Privacy and Transparency
- Data classification
- Cloud exit strategies

WG #3: Network Access Cloud Security

Industry Experts

- Group discussions held with experts to discuss gaps / issues around Network Access to Cloud Infrastructure with respect to security
- Focus of the discussions centered around Public and Hybrid Clouds
  - Private Clouds typically have dedicated, secure access
- Experts included members from:
  - Network & Security equipment manufacturers
  - Cloud and Managed Services providers
  - Network Access providers focused on various access methods
  - Industry Groups primarily charged with cloud security and data protection
- Methods of Network Access ranged from:
  - Over The Top (Internet Access)
  - Virtual Private Networking (VPN) / Tunneling / Secure Shell (SSH) Protocol
  - Dedicated Access Service

Observations

- The following themes were heard throughout the discussions:
  - Adoption of Cloud for streamlining IT-like functions growing as price models for compute & storage infrastructure continue to decrease
  - Pressure mounting for decreasing consumer time-to-market as well as fewer needs for dedicated IT-staff driving outsourcing to Cloud
  - Consumers have a wide range of expertise in the areas of IT, security, and data protection (ranging from a little to a lot)
  - Consumers may assume the Cloud Operator has more knowledge on these subjects and, in turn, may be less concerned with security
  - Cloud Operators looking to maximize return on investment of infrastructure and do offer security / protection as an "add on" – but not required
  - Cloud Carrier responsible for securing their networking infrastructure to ensure no unauthorized access
  - Access to data is only as strong as the weakest link in the chain

Concerns / Gaps

- Number One: Ultimate End-to-End Accountability - Who has it?
- No standard of measurement for Cloud Providers
- Networking Threats (DNS redirect, BGP spoofing, Man-in-the-Middle, etc.)
- Need further research into:
  - Visibility for Consumers and how their data is handled / protected
  - Service Level Agreements (SLA) with basic language on data protection / performance by the Cloud Provider
  - Ubiquitous communication & preventative / proactive tools of known vulnerabilities / security breaches to reduce "I don't know what I don't know" perception
- Some enterprise CIOs take the approach of "Don't tell me what's wrong – I may have to act"
- Ensure all Cloud Providers are utilizing best practices Cloud Security Alliance best practices (such as Cloud Control Matrix) to disclose data handling practices
- Evolving technologies (e.g. Network Functions Virtualization) will require new security / protection considerations

Common Gaps / Forward Focus

- Accountability
- Education
- Industry Collaboration
- Certification
- Auditing

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

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.

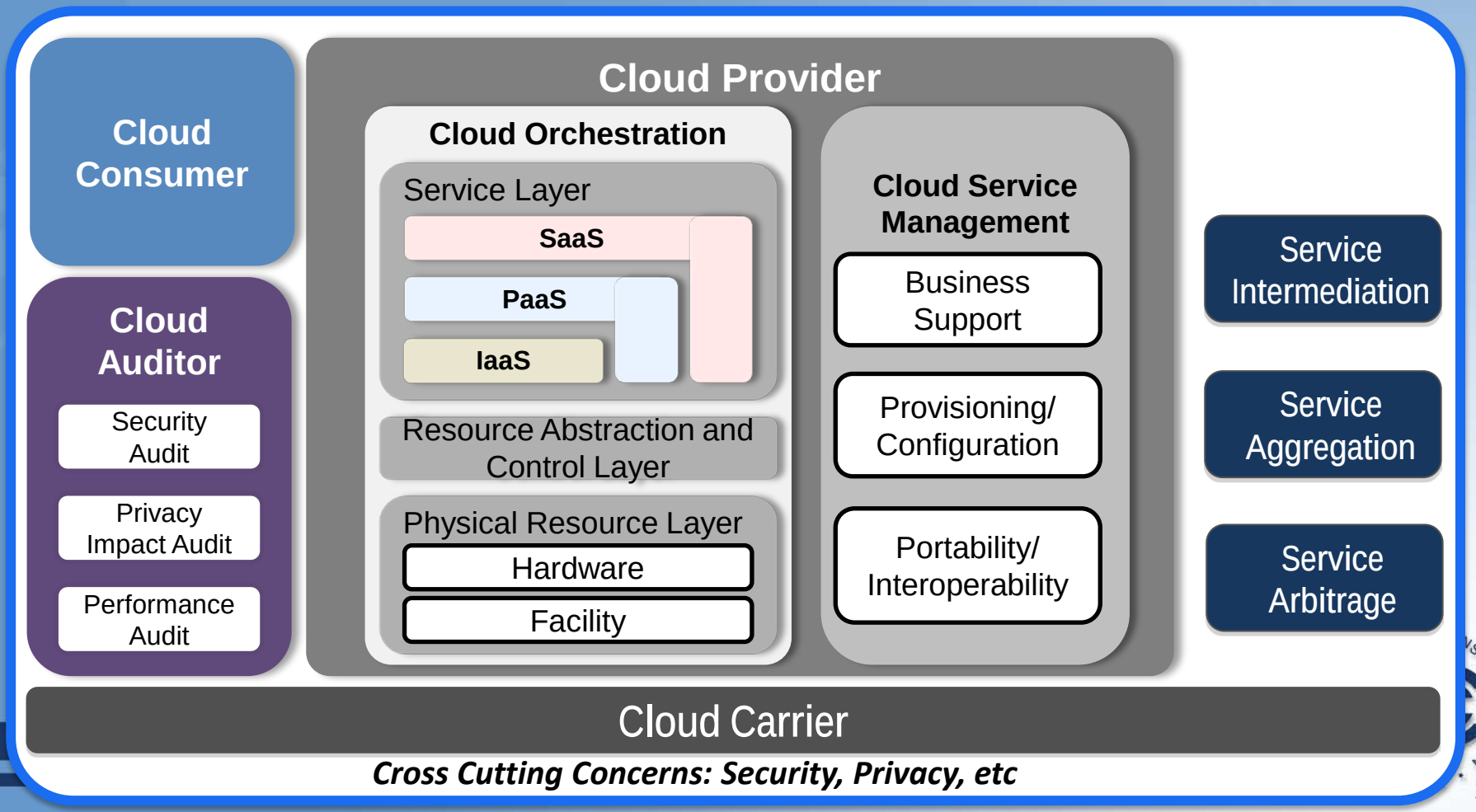
CSCC, OGF, ARTS, Openstack, OMG, CSA, W3C, OCC, PCISSC, Oasis, SNIA, IETF, OSLC, TM, SIIA, DMTF, TIA, IEEE, ETSI, ATIS, AICPA, GICTF, Open, Group, NDIA, ISO, MPAA

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

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.gov
• Department of Homeland Security Office of Cyber-Security and Communications	http://www.dhs.gov
• 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.dodcio.defense.gov
• 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.siia.net
• 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