
FCC Technological Advisory Council

April 1st, 2014



Agenda

- Opening Remarks
- Chairman's Overview
 - TAC Contributions
 - Staff Response to 2014 Recommendations
 - MDTP Expectations
- Mobile Device Thief Prevention
- Cybersecurity
- Spectrum and Receivers
- Form 477
- Roadmap for Future Unlicensed Services
- Next Generation Internet Services
- Game Changing Technologies
- Closing Comments and directions for 2015 meetings
- Adjourn

Technological Advisory Council Actionable Recommendations - 2014

- TAC workgroups provided recommendations to FCC staff in 2014
- FCC staff reviewed recommendations in context of Bureau/Office responsibilities
- Bureaus/Offices established objectives based on these recommendations
- Progress on objectives will be tracked on continuing basis



WTB/OET/CGB

- Smart Phone Theft
 - Establish FCC inter-Bureau Smartphone Theft Working Group to combat mobile device theft as evolving challenge to consumers/industry/law enforcement
 - Underway in 2015
 - Work with industry in 2015 for specific commitments to:
 - Continue to improve phone security
 - Improve industry database approach to theft deterrence and mitigation; and improve reporting capability for stolen devices
 - Increase effectiveness of consumer outreach by industry/law enforcement
 - Consumer awareness of theft problem, importance of security, awareness of mitigation solutions, actions to be taken if phone is stolen



WTB

- Advance Sharing
 - Identify additional target spectrum bands for sharing
 - Communicate TAC's recommendations in this area to NTIA (PPSG)
 - Work with NTIA/PPSG to identify target band(s)



OET/EB/WTB

- Near term
 - Work with CSMAC to incorporate TAC recommendations on transmitter identifiers and emission designators into “Straw-Man” enforcement proposal
 - Develop FCC briefing paper on current use of emission designators in licensed and unlicensed services
- Long Term
 - Move towards risk-informed interference assessment by:
 - Increasing agency knowledge/expertise in quantitative risk assessment
 - Developing pilot proposals in low risk situations



WCB

- Transition to IP
 - Use rural service providers as test bed for technologies and/or cost models
 - FCC implemented work group in 2013 based on earlier TAC recommendation for IP Transition
 - In 2014 FCC initiated program to provide \$100M for rural technology trials
 - Incent construction of efficient middle mile networks
 - Work with rural service providers to provide better deployment cost and operational models for a future evolvable IP environment
 - Maintain a regulatory environment supporting broadband deployment



Technological Advisory Council

Mobile Device Theft Prevention WG

April 1st, 2015



Agenda

- Mission
- Recap of MDTP Findings & Top Priority Recommendations
- Progress on MDTP
- MDTP working Group Plan for 2015



MDTP WG Mission

- TAC workgroup will continue from 2014
- Emphasis will be on longer term initiatives that will combat more sophisticated theft scenarios
 - Developing recommendations on next generation anti-theft features
 - Processes including recommendations for hardening of existing device identifiers and the possible need for new, more secure identifiers
 - Security mechanisms with higher consumer acceptance (e.g. biometrics)
 - More focused analysis of analysis overall theft ecosystem including how stolen devices are re-entered into the marketplace (e.g. recycling industry)
 - Further recommendations on improved reporting mechanisms
- Consideration will also be given to the efficacy of extending theft prevention mechanisms to other classes of devices.
- Provide an assessment of progress made in the area of device theft prevention as some of these recommendations have been applied



WG Participants

- Co-Chairs:
 - Brian Daly, AT&T
 - Rob Kubik, Samsung
- FCC Liaisons:
 - Walter Johnston
 - Charles Mathias
 - Elizabeth Mumaw
- Dennis Roberson, FCC TAC Chair
- Alan Bersin, DHS
- Asaf Askenazi, Qualcomm
- Ayal Yogev, Lookout
- Adam Drobot, OpenTech Works
- Ben Katz, Gazelle
- Brad Blanken, CCA
- Chris Bender, Motorola Mobility
- Christian Schorle, FBI
- Craig Boswell, Hobi
- David Strumwasser, Verizon
- Deepti Rohatgi, Lookout
- DeWayne Sennett, Editor (AT&T)
- Eric Feldman, ICE/Homeland Security Investigations
- Gary Jones, T-Mobile
- Greg Post, Recipero
- Ian Robertson, Motorola Mobility (Lenovo)
- Irene Liu, Lookout
- Jake Laperruque, Center for Democracy and Technology
- Jack Nasielski, Qualcomm
- James Moran, GSMA
- Jamie Hastings, SME (CTIA)
- Jason Novak, Apple
- Jay Barbour, Blackberry
- Jeff Brannigan, DHS
- Joe Heaps, National Institute of Justice
- John Foust, Metropolitan Police, Washington, DC
- John Marinho, CTIA
- Kirthika Parmeswaran, iconectiv
- Les Gray, Recipero
- Mark Romer, Asurion
- Matt Rowe, Gazelle
- Mike Rou, eBay
- Maxwell Szabo, City and County of San Francisco
- Shelley Gu, Microsoft
- Ron Schneirson, Sprint
- David Young, Verizon
- Samuel Messinger, U.S. Secret Service
- Sang Kim, LG



Recap of 2014 MDTP Findings

No common national framework for smartphone anti-theft mitigation

No current official national or international smartphone theft statistics

- Industry database has only been operational in the U.S. for the past few years
- Large number of law enforcement agencies makes aggregation of mobile device theft data a significant challenge
- Improved data collection is necessary to understand if measures being implemented are effective

MDTP Working Group obtained preliminary data from 22 police jurisdictions supporting the view that smartphone theft is a major issue in the U.S.

Destination of the millions of stolen smartphones is unknown



Recap of 2014 MDTP Findings (continued)

Industry groups (e.g., CTIA, GSMA-NA) have developed voluntary commitments and best practices on smartphone theft mitigation

- Major manufacturers and OS providers have committed to providing device-based solutions by July 2015 (CTIA)
- Not all mobile service providers have adopted these commitments
- Best practices need to be enhanced over time

No “silver bullet” that will eliminate smartphone theft

- A complementary suite of technical and operational mitigation techniques must be made available and applied to gain additional impact to mobile device theft
- There is evidence that implementation of specific solutions is impacting criminal activity
- Secure technology solutions are required to ensure unique device identifiers on all smartphones



Recap of 2014 MDTP Findings (continued)

Law enforcement needs a better understanding of anti-theft tools available to aid theft investigations; more user-friendly anti-theft tools for law enforcement will be a critical component of a successful solution

Consumers must understand the benefit to broadly adopt phone theft deterrent measures – “opt-out” solutions should be the norm going forward

The most effective anti-theft messaging comes from local law enforcement

- Service provider and manufacturer outreach is needed to supplement this effort



Review of Top Priority Recommendations (December 2014)

National Framework

Deploy and Continue to Evolve Technology Solutions

Engaging Consumers

Engaging Law Enforcement

Engaging the International Community



Progress on MDTP

- Industry wide recognition of mobile device theft and solutions being implemented
- MDTP solutions take into account interests of consumers, industry, public safety
- Progress to prevent mobile device theft is being made
 - New Data Reveal Thefts Down 40% In London; 22 % In San Francisco; And 16% In New York City
 - <http://www.ag.ny.gov/press-release/ag-schneiderman-london-mayor-johnson-and-da-gasc%C3%B3n-welcome-dramatic-global-drop>

MDTP Plan for 2015 – Immediate Objectives

- Develop recommendations to achieve a national template geared toward on-device features like password protection and remote wipe/lock for Mobile Device Theft Prevention:
 - Reduce complexity, significantly increase consumer use and reporting of theft
 - Address issue of WiFi only device use
- Device Identifier Hardening
 - Assess obstacles to and make recommendations for near term action
- Industry stolen device database
 - Develop specifications for an effective database supporting:
 - Comprehensive listings for stolen devices on a national/regional basis
 - Effective reporting/use by key stakeholders
 - Scaling to all service providers
 - Broadest range of future devices
 - Off-net use of stolen devices

Cybersecurity Working Group

Chairs: Paul Steinberg, Shahid Ahmed
Vice Chair: Ramani Pandurangan
FCC Liaisons: Jeffery Goldthorp, Lauren Kravetz

1-April-2015



Working Group Members

- WG Chair: Paul Steinberg, Motorola Solution
Shahid Ahmed, Accenture
- Vice Chair: Ramani Pandurangan, XO Communications
- FCC Liaisons: Jeffery Goldthorp, Lauren Kravetz
- Members:
 - John Barnhill, Genband
 - Mark Bayliss, Visualink
 - Nomi Bergman, Brighthouse
 - Nneka Chiazor, Verizon Wireless
 - Brian Daly, AT&T
 - John Dobbins, Earthlink
 - Martin Dolly, AT&T
 - Dale Drew, Level 3 Communications
 - Adam Drobot, Open Tech Works
 - Dick Green, Liberty Global
 - Russ Gyurek, Cisco
 - Theresa Hennesy, Comcast
 - Farooq Kahn, Samsung
 - Tom McGarry, Neustar
 - Paul Misener, Amazon
 - Jack Nasielski, Qualcomm
 - George Popovich, Motorola Solutions
 - S Rao Vasireddy, Alcatel Lucent
 - Jack Waters, Level 3 Communications
 - David Young, Verizon Wireless



FCC Requested Analysis Topics

- 1. Simplifying Smartphone Security (Martin Dolly)**
- 2. Securing IoT Consumer Products (George Popovich)**
- 3. Securing SDN (Ramani Pandurangan)**

Definition: Topic 1 - Simplifying Smartphone Security

Today, configuring a device to minimize security and privacy risks can be tortuous and the impacts are not well understood by most consumers. Last year, the Commission asked the Consumer Advisory Committee to recommend a series of questions that could be presented to consumers by way of their smartphones. The answers to these questions would be used by an app resident on the device to configure the device's security and privacy settings to the user's liking. We originally had in mind that the Smartphone Security Checker could be a platform for presenting the questions to users, but we have turned our attention to apps produced and marketed by NQMobile (a CSRIC member) and LookOut. We recommend that the TAC be asked to provide us with a set of recommended generic requirements that we could seek comment on, thereby promoting the availability of features in such apps that converge on a set of common security and privacy concerns.

Work plan: Topic 1 – Simplifying Smartphone Security

- **Proposed scope/direction**

- Develop platform agnostic baseline security controls, recommended settings and common vernacular for reporting on device security and application permissions.

- **Tentative key deliverables**

- **June 2015:** Analysis / Discovery
 - Platform agnostic application permissions definitions including risk of enabling each permission.
 - Baseline security controls recommendations, methodology for testing and common reporting
 - Recommendations on handling alternative application sources (e.g. “unknown sources” on Android and Enterprise or developer delivered on iOS)
 - Clear statements on dangers of jailbreaking or rooting devices and recommendations on detection capabilities for such in any bolt-on security solutions
- **September 2015:** Tentative suggested feature list that promote device security/privacy
- **December 2015:** Recommended requirements for capabilities/features that promote device security/privacy that the FCC could seek comment upon



Work plan: Topic 1 – Simplifying Smartphone Security (cont.)

- **Potential key sources of input – *preliminary list***
 - Device Vendors – Samsung, Sony, HTC, Apple, LG, etc.
 - Platform representation – Google / Android, Apple / iOS, RIM / Blackberry, Microsoft / Windows Phone, alternative mobile OSs – e.g. FireOS, Sailfish, Firefox OS, Ubuntu, Tizen
 - Carriers
 - Security Solution providers – Lookout, NQ, Symantec, Intel
 - Device OEMs– Broadcom, AMD, Qualcomm, TI, Freescale, Marvell

Definition: Topic 2 - Securing IoT Consumer Products

The WG will examine the special cybersecurity challenges posed by the emerging Internet of Things, and suggest actionable recommendations to the FCC with particular focus on the security and protection of IoT consumer products.

Questions:

- What are the underlying technologies (e.g., WiFi, ZigBee, GPRS, LTE) that dominate the IoT space? and what security vulnerabilities and challenges do they present in the IoT environment?
- What other security challenges face IoT consumer products?
 - For example, to what extent does lack of physical security pose a threat to unsupervised IoT devices? Explain.
- What is the industry doing to secure and protect battery-operated and resource- constrained (i.e., minimum computing power and memory) M2M devices, which cannot encrypt its data?
- How are the IoT/M2M stakeholders addressing those security challenges and vulnerabilities, and what are the gaps?
- What is the potential impact of these security challenges on the future of IoT/M2M industry, the end user and the economy, especially when IoT devices become fully integrated in all of our systems, including our critical infrastructures?
- What role could the FCC play in facilitating positive changes in the security, privacy and resiliency of M2M/IoT devices and systems?

Work plan: Topic 2 – Securing IoT Consumer Products

- **Proposed scope/direction**

- Start by leveraging the valuable work produced by the 2014 TAC IoT Working group
- Examine the cyber security challenges posed by the emerging Internet of Things, and suggest actionable recommendations with particular focus on the security of IoT consumer products.
- Understand IoT security challenges, e.g. securing unsupervised and resource constrained devices
- Investigate how stakeholders are addressing security challenges today, identify the gaps, and understand the potential impact of these challenges to the future of the IoT industry where IoT devices become fully integrated in all of our systems, including our critical infrastructures

- **Tentative key deliverables**

- **June 2015:** Perform and deliver a survey of the industry landscape, including existing best practices, standards, consortium efforts, and leading technology solutions
- **September 2015:** Communicate the current security gaps in the IoT space, and how technology advancements may address these gaps
- **December 2015:** Propose a FCC role in facilitating positive changes in the security, privacy and resiliency of IoT devices and systems



Work plan: Topic 2 – Securing IoT Consumer Products (Cont.)

- **Potential key sources of input – *preliminary list***

- **NIST cyber-physical systems public working group (CPS PWG)** – looking to develop and implement a new cyber security framework dedicated to cyber-physical systems (also known as Internet of Things)
- **FTC Office of Technology Research and Investigation (OTRI)** - examining the privacy and security measures of rapidly expanding technologies such as IoT
- **Industrial Internet Consortium (IIT)** – establishing a security framework to ensure sufficient cyber security and privacy for the various users of the industrial Internet
- **Thread Group** – a non-profit organization looking at better ways of connecting products in the home
- **OWASP Internet of Things Top Ten Project** – helping vendors and consumers understand IoT security issues
- **Leading vendors** in the IoT technology space, e.g. Intel, Microsoft, Windriver, HP, Thingworx, Cisco, Broadcom, GE, IBM

Definition: Topic 3 - Securing SDN

There are clear signs that the telecommunications market is standing at the cusp of a significant paradigm shift in how computer networks of the future will be designed, controlled, and managed. One of the key technologies at the heart of this transformation is called Software Defined Networking (SDN) architecture. According to ONF, this new approach to designing, building, and managing networks make it possible for enterprises and carriers to gain unprecedented programmability, automation, and network control, enabling them to build highly scalable, flexible networks that readily adapt to changing business needs. The way this is accomplished is by decoupling the control and data planes, logically centralizing network intelligence and state, and abstracting the underlying network infrastructure from the applications.

SDN is sometimes considered to carry significantly more cyber risk than traditional network architectures. Therefore, the need to secure both SDN's centralized network's control plane and distributed dataplane seem essential. It would be worthwhile considering how to build in security as opposed to retrofitting it, and seeking to apply lessons learned from the long running efforts to secure existing control plane protocols such as BGP, and DNS.

Definition: Topic 3 - Securing SDN (cont.)

Questions:

- What are the key security challenges that SDN architectures present? And how is the telecom industry addressing them?
- What measures could be employed to make networks deploying SDN applications resilient and secure?
- What is the trust model that should be applied between devices and controllers, and between controllers?
- What, if any, high-assurance approaches may apply to SDN?
- What specific lessons can we extract from the long running efforts to secure existing control plane protocols -- such as BGP and DNS – to benefit SDN-based networks?
- What are the pros and cons of embedding security within the network, as opposed to embedding it in servers, storage and other computing devices?
- What are the strengths and weaknesses of Software Defined Security (SDSEC)?
- What role could the FCC play in facilitating positive changes in the security, privacy and resiliency of SDN?

Work plan: Topic 3 – Securing SDN

• Proposed scope/direction

- Study the state of the SDN / NFV architectures and associated flexibility to dynamically steer flows through physical and virtual security functions, and security challenges presented by this architecture
- Lessons learned from attempts to secure existing control plane protocols, such as BGP and DNS
- Research strengths and weaknesses Software Defined Security(SDSEC) and current industry best security practices to make SDN networks resilient and secure
- Investigate relative merits of embedding security within the network vs. in servers, storage and other computing devices
- Identify any possible gaps and examine approaches to ameliorate
- Explore FCC role in enhancing the security, privacy and resiliency of this evolving network architecture

• Tentative key deliverables

- **September 2015**
 - Industry landscape of the evolving network architecture and related security approaches and challenges
 - Currently available industry best practices
- **December 2015:** Recommended roles which could be played by FCC and actions to facilitate enhancing security, privacy and resiliency of this evolving network architecture

Work plan: Topic 3 – Securing SDN (cont.)

- **Potential key sources of input – *preliminary list***
 - NIST
 - Leading Vendors (e.g. ALU, Cisco, Cyan, Ericsson, Genband, HP, Juniper, Windriver) in the different layers of the SDN / NFV ecosystem
 - Ongoing work in Standards Development Organizations (e.g. 3GPP, ATIS, ETSI, IEEE, IETF, ISO)
 - Industry Consortia and communities (e.g. ONF, OpenDaylight, OPNFV)
 - Current and planned security strategies by Service Providers

APPENDIX



Technological Advisory Council

Spectrum and Receiver Performance

Working Group

April 1 , 2015



2015 Mission

- **Make recommendations in areas focused on improving access to and making efficient use of the radio spectrum from a system and receiver perspective**
- **Provide support as the Commission considers TAC recommendations related to the statistical aspects of interference**
- **Conduct analysis and make recommendations related to enforcement issues in a rapidly changing RF environment**



Working Group

- **Chair:**

- Lynn Claudy, NAB
- Greg Lapin, ARRL

- **FCC Liaisons:**

- Julius Knapp
- Uri Livnat
- Bob Pavlak
- Matthew Hussey

- **Participants / Contributors:**

- Dale Hatfield, University of Colorado
- Pierre de Vries, Silicon Flatirons
- Brian Markwalter, CEA
- David Gurney, Motorola Solutions
- Geoff Mendenhall, GatesAir
- Robert Dalglish, Ericsson
- Robert Miller, incNetworks
- Patrick Welsh, Verizon
- Bruce Judson, Qualcomm
- Marc Richer (ATSC)



Working Group Areas of Focus

- **Develop recommendations about statistics of interference and risk-informed decision making**
- **Recommend strategies for interference resolution and enforcement in a changing RF environment**
- **Propose methods for characterizing the operational impact to receiver performance from interference**



Risk-Informed Interference Assessment

- **Goal: Find quantitative ways to reason about the risks of harmful interference due to changes in radio service rules, e.g. new allocations, rule changes, and waivers**
- **‘Introduction to Risk Informed Interference Assessment’ paper**
 - **Comments**
 - **Acceptance of the paper by the full TAC for publication on the website**



Interference Resolution and Enforcement

- **Goal: Recommend strategies for interference resolution and enforcement to address changing RF environment**
- **Coordinate with CSMAC in the development and recommendation of enforcement strategies for a shared spectrum environment with federal incumbents**
- **Enforcement ‘White Paper’ and ‘Straw-Man’ proposal**
- **Use of emission designators and transmitter identifiers in classifying and identifying sources of interference**



Characterizing Receiver Performance

- **Goal : Develop methods for characterizing the operational impact to receiver performance from interference in shared spectrum environments**
- **Consider the balance between the input power limits of receivers (blocking) and the output power limits of transmitters (out-of-band emissions), interference margins and cost / benefit technical tradeoffs**



THANK YOU



FCC TAC: 477 Testing



477 Testing WG

April 1, 2015

- Steve Lanning (WG Chair)
- Tom Wilson
- Chris Feathers
- Chelsea Fallon (FCC)
- Kenneth Lynch (FCC)
- Others



Charter

- This working group will continue from 2014
- The goal is to validate the requirements developed for improved electronic collection of Form 477 data and test the computing platform developed to collect these data
- Development of this platform is dependent on IT funding
- A diverse range of service providers will participate
- Successful completion of the trial will allow the next phase of the Commissions' data collection infrastructure to be deployed, supporting the collection of broadband data



Key Areas of Focus

- Data accuracy
- Ease of use



Work Plan (first draft)

- Review requirements for the application
- Survey platforms used to make current 477 submissions
- Survey platforms available to run new 477 software
- Provide input on security and confidentiality issues
- Test early version of application
- Develop recommendations on how to collect subscribership data beyond counts by data rates
- Compare results to 477 submissions without application
- Compare results of testers to estimated households from Census



Logistics

- Periodic team meetings
- Work with FCC advisor on “requirements focus” for 477 Testing
- Draft of work plan by June TAC meeting



Comments and Feedback



Roadmap for Future Unlicensed Services Working Group

Chairs: Mark Bayliss, Milind Buddhikot
Vice Chair: John Barnhill
FCC Liaisons: Michael Ha

1-April-2015



Working Group Members

- WG Co Chairs: Mark Bayliss, Milind Buddhikot

- Vice Chair, John Barnhill
- FCC Liaisons: Michael Ha

- Members:
 - John Barnhill, Genband
 - Mark Bayliss, Visualink
 - Nomi Bergman, Brighthouse
 - Adam Drobot, Open Tech Works
 - Dick Green, Liberty Global
 - Russ Gyurek, Cisco
 - Theresa Hennesy, Comcast
 - Farooq Kahn, Samsung
 - Jack Nasielski, Qualcomm
 - George Lapin
 - Mark Racek, Ericsson
 - Brian Markwalter CE.org



Roadmap for Future Unlicensed Services

Unlicensed services have played an unexpectedly vital role in the evolution of communication capabilities and in providing a ‘wireless commons’ for innovation. It is critically important for the Commission to understand both the potential pathways for continued evolution of unlicensed services as well as potential threats to the continued viability of the ‘commons’. To that end, this workgroup will focus on number of key topics for future unlicensed services: (1) Evolving and novel applications (e.g. low power WANS, internet-of-things (IOT), unlicensed LTE). (2) new business models (e.g. managed vs. unmanaged vs. private, indoor-only services). (3) new candidate spectrum bands to increase available spectrum. (4) etiquettes for unlicensed service applications that will help protect the commons model and (5) the potential impact of present EMC limits for consumer and industrial devices on the continued growth and vibrancy of unlicensed services.

Work plan:

- **Potential key sources of input – *preliminary list***

Unlicensed Wireless equipment manufactures

Wireless Internet Providers. “Wisps”

Large scale deplorers of Unlicensed services, “Comcast, Verizon, Bright Networks, Bongo”

And new adopters and technology developers for unlicensed spectrum – Like “Ericsson, Alcatel-Lucent”

APPENDIX



Next Generation Internet Service Characteristics & Features Working Group

Chairs: Russ Gyurek

FCC Liaisons: Padma Krishnaswamy, Daniel Kahn,
Walter Johnston

1-April-2015



Working Group Members

- **WG Chair:** Russ Gyurek, Cisco
- **FCC Liaisons:** Padma Krishnaswamy., Daniel Kahn, Walter Johnston
- **Members**
 - John Barnhill, Genband
 - Mark Bayliss, Visualink
 - Nomi Bergman, Bright House
 - John Dobbins, Earthlink
 - Adam Drobot, OpenTechWorks
 - Andrew Dugan, Level3
 - Stephen Hayes, Ericsson
 - Theresa Hennesy, Comcast
 - Farooq Kahn, Samsung
 - Tom McGarry, Neustar
 - Milo Medin, Google
 - Lynn Merrill, NTCA
 - Paul Misener, Amazon
 - Jack Nasielski, Qualcomm
 - Ramani Pandurangan, XO Comm
 - Mark Richer, ATSC
 - Hans-J. Schmidtke, Juniper
 - Marvin Sirbu, Carnegie Mellon
 - Kevin Sparks, ALU
 - David Young, Vz



NG Internet Service Characteristics & Features Charter

The Internet continues to evolve: from a network that originally supported remote terminal access and email, later to web browsing and media transfer, now to the present environment where video streaming has become a dominant service. A ‘best effort’ network is evolving towards one where Quality of Service (QOS) is a growing concern and where the Internet assumes the role of critical infrastructure. The architecture of the Internet has adapted to better support these issues morphing from relatively simple backbone/access network architecture to a more complex environment of dedicated links, Content Delivery Networks (CDNs), specialized routing/peering arrangements, etc. The transition to IP (‘the death of the PSTN’) will further hasten this evolution to an environment wherein IPv6 is the underlying addressing scheme. This work group will seek to **assess future service requirements** for the Internet driven by the need to provide critical infrastructure services, the transition of services from the PSTN to an IP based platform, the expected impact of IOT, cybersecurity needs, governance models and other factors. The work will examine efforts within relevant standards and governance bodies to frame these issues as well as look at potential architectural changes driven by these **service needs** for public safety, **QOS metrics for end/end and network/network interfaces** and new technologies such as 5G.

The work group will also seek to make recommendations on benchmarks that could serve to better inform policy makers on the health and status of the Internet.

NG Internet Service Characteristics & Features

Topics of Focus

Examples of Areas to explore service needs & Requirements:

- 5G
- Video: 4K, 8K, 16K
- CDN
- IPv6 migration/impact
- Deterministic Ethernet
- CyberSecurity
- IoT applications
- Data Virtualization, Cloud, Distributed services
- Privacy
- End to end encryption
- Caching

NG Internet Service Characteristics & Features Activities

- Ideation/Start: March 2015
- Team Meeting March 30, 2015
- FCC Advice meeting, March 2015
- Planning session (in DC) April 1
- TAC Guidance April 1, formal TAC meeting

NG Internet Service Characteristics & Features

Prior, Current, and Related Work

- Previous “Transition” WG: detailed analysis on QoS for Access
- Cybersecurity Working Group efforts
- Previous “IoT” Working Group analysis of requirements
- Other FCC groups: BITAG
- FCC programs: “Measured Broadband America” (MBA) program
- Standards efforts: IEEE, IETF, ITU, etc.
- Current Working Group on “Future Game Changing Technologies”

NG Internet Service Characteristics & Features

Open Questions...

- What is the meaning of the Internet today
- What are the expectations for the future of the Internet
 - QoS or no QoS
- How will the Internet be consumed [services]
- Should we distinguish between the Internet and Specialized Service
- Impact of new Business models → this is not a purely technical issue
- Scenario planning: 3 year, 5 year, 10 year, beyond

NG Internet Service Characteristics & Features

Proposed Efforts

- **QoS wrt TAC focus**
 - Services requirements will drive the teams efforts
 - What are implications
 - Voice & Video → Real-time communications (Today)
 - NG: 5G, other
 - Distinction between Access and End-to-end
 - Interconnection element
 - The Internet, is it more than just “best effort”
 - New disruptive services(s)
 - Beyond Bandwidth: BW alone does not solve all problems, especially in access
 - Implications for what is minimum “broadband” requirements
 - Cloud services impact
 - Other metrics to consider: jitter, delay, and loss

Future Game Changing Technologies Working Group Proposed Plan

Actions:

1. Define QoS, capacity needs, BW, etc., for effort
2. Standards, Government Bodies- Existing efforts
 - Quick Taxonomy- define focus
3. Service and Architectural Impact
4. Recommendations

Our Guidance: *What the commission should encourage*



NG Internet Service Characteristics & Features

Input and Discussion

Future Game Changing Technologies Working Group

Chairs: Nomi Bergman, Adam Drobot
FCC Liaisons: John Leibovitz, Nnake Nweke,
Walter Johnston

1-April-2015



Working Group Members

- WG Chair: Nomi Bergman, Bright House Networks
Adam Drobot, OpenTechWorks

- FCC Liaisons: John Leibovitz, Nnake Nweke, Walter Johnston

- Members:
 - Kumar Balachandran, Ericsson
 - John Barnhill, Genband
 - Mark Bayliss, Visualink
 - John Chapin, DARPA
 - Lynn Claudy , NAB
 - Brian Daly, AT&T
 - John Dobbins, Earthlink
 - Paul Devries, Silicon Flatirons Center
 - Jeffrey Foerster, Intel
 - Dick Green, Liberty Global



Working Group Members Cont'd

- Members:

- Mark Gorenberg, Zetta Ventures
- Russ Gyurek, Cisco
- Farooq Kahn, Samsung
- Gregory Lapin, ARRL
- Brian Markwalter, CEA
- Tom McGarry, Neustar
- Paul Misener, Amazon
- Jack Nasielski, Qualcomm
- Bruce Oberlies, Motorola Solutions
- Ramani Panduragan, XO Communications
- Michael Roman, NTCA
- Mark Richer, ATSC
- Marvin Sirbu, SGE
- Paul Steinberg, Motorola Solutions
- Hans-Jurgen Schmidke, Juniper Networks
- Kevin Sparks, ALU
- Sanjay Udani and David Young, Verizon



Future Game Changing Technologies Working Group Charter

- The workgroup will seek to identify technologies with the potential to radically change communication infrastructure and business models across a broad range of fronts. The intent is to identify seminal technologies and concepts that the Commission should understand and possibly include in its considerations. The workgroup will seek to identify these catalysts and assess their potential impact. The group will be chartered to scan across a wide breadth of technical areas, identify areas of potential promise, and organize them in the context of synergies and potential impacts.



Future Game Changing Technologies Working Group Charter

- Examples of areas that could be examined include 5G, Massive MIMO, millimeter wave devices, bidirectional channel sharing, interference cancellation technology, space-based free space optical systems, cube-satellites, low earth orbit satellites, fiber enhancements, the use of crowd sourced measurement techniques, software defined networks, radar/radio spectrum sharing, etc.

Future Game Changing Technologies Working Group Activities

- Request for Ideas 3/8/2015 **
- First WG Call 3/24/2015
- Planning Session – additional ideas, WG organization, and plan for deliverables 4/1/2015

** The original submissions are available for sharing with the TAC and are abstracted later in this presentation. Kevin Sparks has provided a further refinement of the ideas and characterized their implication.



Future Game Changing Technologies Working Group Summary of Ideas - Examples

- Antennas and Signal Processing
 - Massive MIMO, Beam Forming
 - Adaptive Arrays
 - Advanced Waveforms
 - Vectoring
- Software Defined Networks - SDN
- Network Function Virtualization – NFV
 - Virtual RAN, Cloud RAN, Intelligent Multi-RAN
- 5G Technologies
- WebRTC

These technologies drive new architectures, spectrum efficiency, capacity, and communications bandwidth

Future Game Changing Technologies Working Group Summary of Ideas - Examples Cont'd

- Free Space Optical Communications
- Next Generation Passive Optical Networks
- High Bandwidth Satellites
 - GEO, MEO, and LEO
- IoT and M2M Technologies
 - Device-device communications
 - Network Coding
 - Edge Computing
- Artificial Intelligence
- Big Data

Swarms of airborne communications platforms (e.g., drones, cube-sats) are likely to be a game changer: fast, cheap, hard to control

Future Game Changing Technologies Working Group Summary of Ideas - Examples Cont'd

- Smart Cities
- Personalized Medicine and Telemedicine
- Augmented Reality
- Education
- Autonomous and Connected Vehicles
- Uniform National Public Safety Network
- Embedded and Distributed Intelligence

These applications will drive infrastructure, demand, business models, and along the way, new communications technologies

Future Game Changing Technologies Working Group Proposed Organization

The Team Discussed Forming Subgroups which would address technologies that:

1. Create Demand
 - Lead to New Capabilities and User Experiences
2. Increase Capacity and Coverage
3. Drive Architectural Discontinuities

Future Game Changing Technologies Working Group

Discussion

Next TAC Meeting Thursday, June 11, 2015

- New format for meeting
 - Spotlight topic discussions for specific work groups
 - Lightning status updates for remaining groups
 - Major topic discussions will rotate among work groups
- Extending Wednesday, December 9th, 2015 by starting at 12 pm

