Agenda

- Introduction
- 2016 Recommendations
- 2015 Recommendations Status
- Cybersecurity Work Group
- Mobile Device Theft Prevention Work Group
- Break
- Implications for Mass Deployment of Aeronautical/Space Transmitters
- Future Game Changing Technologies Work Group
- NG Internet Services Work Group
- Spectrum and Receiver Performance Work Group
- Wrap-up

2015 Recommendations

Recommendations

- **Mobile Device Theft Prevention Workgroup**
  - **Recommendation:** FCC to work with CTIA/GSMA/Carriers/LEA to implement MDTF features, improve process and outreach to consumers
  - **Status:** FCC staff currently engaged on a number of fronts implementing these recommendations
- **Future of Unlicensed Workgroup**
  - **Recommendation:** Accelerate search for unlicensed spectrum
  - **Status:** FCC staff engaged on a broad range of unlicensed spectrum issues and will continue to seek opportunities for unlicensed spectrum
  - **Recommendation:** In cooperation with industry, promote sharing of bands between licensed and unlicensed services
  - **Status:** FCC committed to establishing opportunities such as 3.5 GHz where licensed and unlicensed like services coexist; working with standards bodies and industry to resolve conflicts when they arise

Recommendations

- Cybersecurity
  - **Recommendation:** Work with other agencies on IOT security
  - **Status:** FCC working with other agencies towards common cybersecurity goals

  - **Recommendation:** Work with smartphone vendors to improve embedded cybersecurity mechanisms
  - **Status:** Under Consideration

  - **Recommendation:** For SDN, the FCC should work with industry on developing best practices for dominant scenarios
  - **Status:** FCC requested TAC develop further

Recommendations

- Spectrum Receiver and Performance Workgroup
  - **Recommendation:** Develop expertise on risk informed assessments of harmful interference
  - **Status:** Multiple FCC engineers took statistical analysis training

  - **Recommendation:** Future frequency allocations should be based on enumerated risk informed assessment principles
  - **Status:** Excellent paper & recommended principles. Assessing how best to proceed; considering opportunities for applying risk-based interference assessments; most focus is on new spectrum allocations

Recommendations

- Next Generation Internet Workgroup
  - **Recommendation:** Expand FCC network measurement program to gain better assessment of end to end broadband performance and enhance consumer awareness of QOS/QOE
  - **Status:** FCC working with industry and research community on best measurement practices. Evaluating proposal to include CDN and some gateway measurements.

- Future Game Changing Technologies
  - **Recommendation:** Assess impact of Programmable Network on current service rules and accelerate growth of SDN/NFV
  - **Status:** Working with industry to assess impact of programmable networks
  - **Recommendation:** Consider use of Universal Service Fund to support deployment of edge cloud infrastructure in rural areas
  - **Status:** FCC considering evolution of USF to support broadband deployment

Work Group Presentations

TAC 2016 Recommendations

- **Cybersecurity - 5G:** Leverage industry bodies (ATIS) and use the content and processes created and piloted by the TAC, to drive security by design principles into the 5G standardization process (3GPP).
- **Cybersecurity - Software Defined Networking:** Ensure industry support for security as a designed in principle for software defined networks by leveraging industry bodies (CSRIC) and using TAC recommendations to promote and drive best common practices across industry.
- **NG Internet - Public Notice on In-Home Networking Performance :** We recommend that the FCC issue a Public Notice on in-home networks and their contribution to overall Quality of Service/Experience.
- **NG Internet - Measuring QoS - Data Capture, Metrics and Reporting:** Expand the MBA program to add additional QoS and QoE measurements to include CDN performance and Interconnection health
- **Future Game Changing Technology :** The FCC should engage in an annual facilitated study exercise to gain essential insights on the impact of emerging technologies and innovations for disruptive change in the communications sector.
- **Future Game Changing Technology :** FCC should work closely with the Administration and Congress to ensure a flow of spectrum balanced across high, middle, and low spectrum. FCC should establish a 'technology watch list' (evolving 4G and emerging 5G) of priorities for the US market.
- **Mobile Device Theft Prevention :** The FCC TAC recommends that the FCC work with the U.S. State Department and Executive Branch of the government to lobby internationally for greater engagement on device theft issues.
- **Mobile Device Theft Prevention :** The FCC TAC recommends that the FCC work with State, Local, Federal, and Tribal Law Enforcement to assess the effectiveness of the mobile theft prevention measures implemented by the wireless industry.
- **Spectrum/Receiver Performance**: Direct the OET Lab to measure advanced lighting and switching power supplies on the market to ascertain if they meet regulatory noise limits; initiate enforcement if not. Issue NOI/NPRMs to gain more information about the advisability of rule changes to 1) deal with advanced lighting and switching power supplies and 2) to reduce noise in the spectrum.
- **Spectrum/Receiver Performance:** Implement and formalize the TAC's receiver recommendations and spectrum allocation principles as policies
- **Mass Deployment of Aeronautical/Space Transmitters:** TAC recommends the Commission to promote use of existing communications infrastructure whenever possible to support small UAS communications functions and avoid unnecessary costs and regulatory delays. TAC recommends the Commission begin a proceeding on service rules for Command and Control (C2) for large UAS, including HALE/MALE/HAPS, using ITU recommended L-band and C-band.

Cybersecurity Working Group

Chairs:	Shahid Ahmed, Paul Steinberg
FCC Liaisons:	Jeffery Goldthorp, Ahmed Lahjouji

7-Dec-2016

Topics

1. 5G Security (Chairs: Amit Ganjoo, Tom McGarry)
2. Securing SDN (Chair: Ken Countway)
3. Cyber Security - Software Configurable Radios (Chair: Mike Bergman)

2016 TAC Cybersecurity WG Recommendation Summary

- **5G:** The FCC should ensure proactive and broad industry support for 5G security by leveraging industry bodies (ATIS) and using the content and processes created and piloted by the TAC, to drive security by design principles into the 5G standardization process (3GPP).

- **Software Defined Networking:** The FCC should ensure proactive and broad industry support for security as a designed in principle for software defined networks by leveraging industry bodies (CSRIC) and using the content and processes created and piloted by the TAC to promote and drive best common practices across industry architectures and deployments.

- **Cybersecurity for Software Controlled Radios:** The FCC should incorporate the specific SCR (Software Configurable Radio) cybersecurity mechanisms identified the whitepaper into its current guidance.

* https://transition.fcc.gov/oet/tac/tacdocs/reports/2016/TAC-5G-Cybersecurity-Subcommittee-09-12-16.pdf

Topics

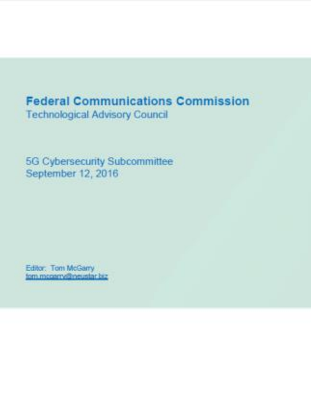
1. 5G Security (Chairs: Amit Ganjoo, Tom McGarry)
2. Securing SDN (Chair: Ken Countway)
3. Cyber Security - Software Configurable Radios (Chair: Mike Bergman)

5G Security Subcommittee

- Amit Ganjoo – ANRA Technologies (co-chair)
- Tom McGarry – Neustar (co-chair)
- Mike Bergman – CTA
- Brian Daly – AT&T
- Martin Dolly – AT&T
- Adam Drobot – Open Tech Works
- Alex Gerdenitsch – Echo Star
- Dick Green – Liberty Global
- Katrina Hardy – Verizon
- Soo Bum Lee – Qualcomm
- George Popovich – Motorola Solutions
- Brian Russell – Cloud Security Alliance
- Christoph Schuba – Ericsson
- Paul Steinberg – Motorola Solutions
- John Yeoh – Cloud Security Alliance
- Ahmed Lahjouji – FCC

2016 TAC 5G Security – Scope/Deliverables

- **Scope/direction**
  - Start by leveraging the valuable work produced by the 2015 TAC IoT Working group
  - Focus on IoT applications of 5G technology, which can be categorized as; Automotive, Smart Society, Smart Grids, Healthcare, Industrial, and Logistics/Freight Tracking
  - Create a list of key security principles that should be built into the 5G IoT ecosystem
  - Identify the SDOs most active in developing 5G IoT specifications
  - Develop an action plan to use the TAC's 5G IoT key security principles into the standards development process
- **Key deliverables**
  - **June 2016:** Identify the SDOs most active in 5G IoT specifications
  - **September 2016:** Communicate the current list of key security principles
  - **December 2016:** Propose an action plan for integrating the principles into the standards development process and the final key security principles



Federal Communications Commission
Technological Advisory Council

5G Cybersecurity Subcommittee
September 12, 2016

Editor: Tom McGarry
tom.mcgarry@neustar.biz

2016 TAC 5G Security – White Paper Status

- Issued the 5G TAC Cybersecurity White Paper of security recommendations on Sept. 12th, 2016
  - Received TAC approval at Sept TAC
- Compared recommendations to 3GPP TR 33.899
  - Recommendation #16 same as Key Issue 8.1 (network slicing)
  - Otherwise found similar, but not identical, requirements
- 5G TAC collaborated with ATIS PTSC to review and update White Paper and create an ATIS document
  - Final version approved at Nov. 30th, 2016 ATIS PTSC meeting
- 5G TAC will continue to collaborate with ATIS PTSC to create 3GPP Change Requests
  - Goal is to pursue broad industry support for submitting CRs at the Feb 2017 3GPP meeting

2016 TAC 5G Security – 5G SDOs

- **3GPP – primary SDO for 5G**
  - 3GPP is a partnership of seven standards bodies (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC) within the scope of the ITU to develop mobile communications network technologies
  - SA3 within 3GPP has the overall responsibility for security and privacy in 3GPP systems
    - Determines security and privacy requirements based on analysis of potential threats
    - Specifies security architectures and protocols
  - SA3's TR 33.899 will identify the threats, potential requirements and solutions for the security of 5G networks
    - It will form the basis for normative work and further study
    - Due to complete February 2017
    - It identifies 17 Security Areas and currently 57 Key Issues
  - SA3 will begin normative work after the TR is completed
    - New requirements can still be introduced during the normative phase
- **ATIS – supports US industry and TAC efforts**
  - ATIS PTSC driven by the 5G TAC is creating CRs related to cybersecurity
  - Other work as necessary, e.g., WTSC and BoD level

2016 TAC 5G Security – 5G SDOs

- **IEEE – just beginning 5G standards work**
  - Currently focused in three areas
    - 802 – LANs and WANs (802, 802.1, 802.1CF, 802.11, 802.15.6, 802.15.7, 802.22)
    - 1903 – Next Generation Service Overlay Network (1903, 1903.1, 1903.2, 1903.3, 1903-2011)
      - Value added converged web and telephony services
    - 1914 – Packet-based Fronthaul Transport (1914.1)
      - Transport between remote radio units and centralized baseband controllers
    - 1918 – Tactile Internet (1918.1)
      - IP network with low latency, high availability, short transit, high reliability and high level of security to enable applications like IoT
  - Bears further evaluation for cybersecurity requirements
- **ITU – little direct 5G standards development**
  - ITU-R does work on radio spectrum
  - ITU-T will issue 3GPP standard as an ITU document after it is complete
- **5G-ENSURE – not an SDO, but a similar goal to 5G TAC**
  - Part of the EU's 5G Public Private Partnership (5G PPP)
  - 5G-ENSURE will define a shared and agreed 5G Security Roadmap with various 5G stakeholders
  - They expect to create CRs for joint contributions to 3GPP
  - FCC TAC should continue to monitor their efforts given our similar goals

5G Subcommittee Recommendations

- **Recommendation**
  - The TAC recommends that the FCC ensure proactive and broad industry support for 5G security by leveraging industry bodies (ATIS) and using the content and processes created and piloted by the TAC, to drive security by design principles into the 5G standardization process (3GPP).
- **Background**
  - The October 21st IoT DDoS attack demonstrates the importance of securing the IoT environment. Given that one of the primary use cases of 5G is IoT, and 5G standardization was is in an early stage, the FCC requested the 5G Subcommittee to implement security by design into the standardization process.
  - The 5G Subcommittee created and published a series of security recommendations* for 5G on 9-12-16, and defined and piloted a repeatable process leveraging ATIS, to enable these recommendations to be injected into SDOs (3GPP in particular). The recommendations were submitted to ATIS PTSC to seek further industry and expert input. The 5G Subcommittee and ATIS will use the recommendations to create formal Change Requests (CR) with the goal of submitting them at the February 3GPP.
  - The next step is for the FCC to engage in an outreach effort to the industry to educate them on the CR development process and encourage broad support for submitting a joint CR to 3GPP.
- **Additional recommendation**
  - 3GPP standardization will continue through 2017 and into 2018. The FCC should continue to ensure broad industry support for driving security by design into 5G standardization. And the FCC should leverage the TAC to create additional high impact, security by design recommendations that can be standardized using the same industry process.

* https://transition.fcc.gov/oet/tac/tacdocs/reports/2016/TAC-5G-Cybersecurity-Subcommittee-09-12-16.pdf

Topics

1. 5G Security (Chairs: Amit Ganjoo, Tom McGarry)
2. Securing SDN (Chair: Ken Countway)
3. Cyber Security - Software Configurable Radios (Chair: Mike Bergman)

Securing SDN Sub-Working Group

- Ken Countway – Comcast (chair)
- Brian Daly – AT&T
- Chetan Desai – PWC
- Martin Dolly – AT&T
- Mike Geller – Cisco
- Kathrina Hardy – Verizon
- Dennis Moreau – VMWare
- Ramani Pandurangan – XO Communications

- Kevin Rossi - Genband
- Christoph Schuba – Ericsson
- David Tennenhouse – VMWare
- Shanthi Thomas – Motorola Solutions

- Padma Krishnaswamy – FCC
- Ahmed Lahjouji- FCC

FCC Direction: Cyber security - SDN

1. Identify existing BCPs that focus on securing programmable networks, particularly those that are based on SDN/NFV network architectures
2. Develop BCPs that close the gaps identified.
3. What effective mechanisms should be employed to keep these BCPs current, and relevant to the industry?
4. How should the FCC and the industry, together, promote adoption of these BCPs?
5. How should the FCC and the industry, together, assess the effectiveness of these BCPs?

Securing SDN/NFV

- **Scope / Direction**
  - For the TAC, last cycle, the Securing SDN group captured the industry landscape with respect to security challenges and opportunities, now we will build on that research to develop recommended best common practices based on our further analysis of the threat surface of SDN and NFV
  - We found it relevant and necessary to couple SDN and NFV together
  - Conduct research using industry resources (vendors, SPs, SDOs, Communities)
  - Consult - SDN / NFV Security SMEs from vendors, operators and communities (e.g. OPNFV, OpenDayLight)
- **Key Deliverables**
  - **June 2016:** a) Ecosystem Engagement and Strategy to Develop / Maintain BCPs with Industry, b) Confirm Prioritized Use Cases
  - **September 2016:** BCP Drafts developed for Prioritized Use Cases
  - **December 2016:** a) BCPs Finalized for Prioritized Use Cases, b) Promotion Activity

Securing SDN/NFV

- After considering multiple use cases which use general SDN/NFV principles SWG identified two candidates
  - SD-WAN (Software Defined WAN) representing "Security for SDN" category
  - DDoS Mitigation for the "SDN for Security" category
- Since SD-WAN has gained significant traction in the industry due to its potential for solving several challenges currently faced by Enterprises the SWG focused on developing BCPs for Enterprise SD-WAN. Future BCP's might focus on Service Provider use cases
- Several SD-WAN vendors as well as industry practitioners were consulted
- SD-WAN (and SDN/NFV more generally) present many opportunities to significantly improve both the efficiency and effectiveness of security (e.g. dynamics, context, agility, granular compartmentalization). Care should be taken in expressing current and future BCPs, so as not to prevent exploitation of such opportunities

Securing SDN/NFV

- Seventeen threats were identified; they were prioritized by the SWG and BCPs developed for the top five; BCP summary slide at the end of this section
- After considering a number of organizations SWG selected CSRIC for lifecycle management of the BCPs, as CSRIC has developed BCPs for other domains, has good industry representation and works closely with FCC
- In the future, as TAC develops BCPs for other threats for SD-WAN and other use cases such as SP / Operator SD-WAN, and using SDN / NFV for enhancing security, the BCPs can flow to CSRIC for maintenance , industry adoption and promotion
- SWG has developed a White Paper "Security BCP Recommendations for SDN/NFV" – *Soliciting TAC Approval for Inclusion into Proceedings*

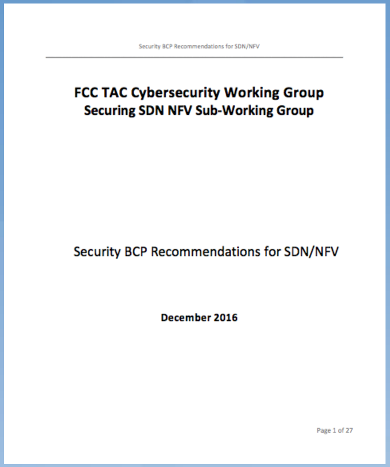
SDN Subcommittee Recommendations

- **Recommendation**
  - The TAC recommends that the FCC ensure proactive and broad industry support for security as a designed in principle for SDN and NFV by leveraging industry bodies (CSRIC) and using the content and processes created and piloted by the TAC to promote and drive best common practices across industry architectures and deployments.
- **Background**
  - The rapid adoption and application of software defined networks (SDNs) and network functional virtualization (NFV) poses a new and diverse set of cybersecurity considerations. As a follow up to the 2015 TAC recommendations* the FCC requested that the SDN Subcommittee develop best common practices (BCPs) for SDN/NFV and recommend ways to promote and sustain industry initiative around those BCPs.
  - The SDN Subcommittee evaluated a set of SDN/NFV applications and created and published a series of best common practice recommendations for SDN/NFV with initial focus on SD-WAN. The subcommittee will submit the SD-WAN BCP to CSRIC along with the prioritized list of other SDN/NFV applications and deployment architectures as input to future BCP development.
  - The subcommittee recommends that the FCC use CSRIC to promote BCPs across industry
- **Additional recommendation**
  - The subcommittee recommends a pipeline approach leveraging the TAC to develop future additional BCPs and transitioning them to CSRIC for industry promotion and life cycle management

* https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/2016/Securing%20-SDN-NFV%20-SWG-WP-Final.pdf

SD-WAN BCP Summary

Extract from White Paper…


Security BCP Recommendations for SDN/NFV

FCC TAC Cybersecurity Working Group
Securing SDN NFV Sub-Working Group

Security BCP Recommendations for SDN/NFV

December 2016

Page 1 of 27

Threat	Best Common Practice				
Manipulation of Information	Authentication of all network nodes	Establish network service directory with ACLs	Enable encryption/integrity protection of south-bound interfaces	Validation of flow table entries (detecting out of band change)	Encryption of persistent information
Software/Firmware Exploits	Isolation between SD-WAN Layers	SD-WAN Applications Isolated from the SD-WAN NOS	SD-WAN Exploit Detection and Prevention	TPMs, Secure Elements, UEFI Secure Boot – Roots of Trust	--
Denial of Service	DDoS mitigation appliance	Real-time monitoring & behavioral analytics	Cloud-proxy for traffic scrubbing	Proper configuration of Firewalls, IPS, DNS, NTP, OS	Action plan to handle an actual DDoS attack
API Exploitation	Encryption	Authorization	Distributed firewalls	DoS protection	Parameter and schema validation and white-hat testing
Unauthorized Activities	Authentication to physical SD-WAN resources	Authorization to software/firmware on SD-WAN resources	Host-based security	--	--

Topics

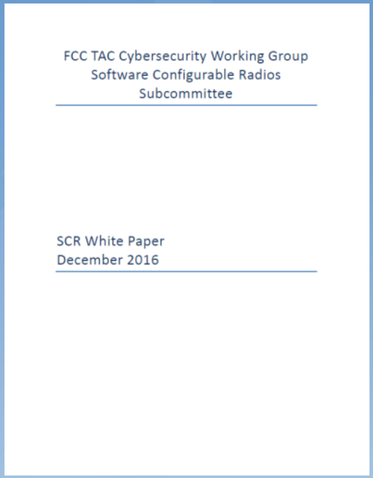
1. 5G Security (Leaders: Amit Ganjoo, Tom McGarry)
2. Securing SDN (Leader: Ken Countway)
3. Cyber Security - Software Configurable Radios (Leader: Mike Bergman)

Cyber Security - SCR Sub-Working Group

Mike Bergman – CTA (leader)
Alex Salvarani – Nokia
Amit Ganjoo – ANRA Technologies
Brian K. Daly – AT&T
Bruce Oberlies – Motorola Solutions
Christoffer Jerkeby – Ericsson
Dan Torbet – Arris
David Gurney – Motorola Solutions
David Kay – Netgear
Eric Schultz – prpl Foundation

George Popovich – Motorola Solutions
Martin C. Dolly – AT&T
Mike Geller – Cisco
Paul Steinberg – Motorola Solutions
Pierre de Vries - Silicon Flatirons
Richard Green – Liberty Global
Russ Gyurek – Cisco
Ahmed Lahjouji- FCC
Edna Prado – FCC
Rashmi Doshi – FCC

FCC Direction: Cyber Security - SCR



FCC TAC Cybersecurity Working Group
Software Configurable Radios
Subcommittee

SCR White Paper
December 2016

- FCC's Goal for the WG

  "How to strike the appropriate balance between embedding frequency security mechanisms into Software Configurable Radios while allowing innovation and the flexible addition of features."

- FCC's Questions
  1. Why don't (consumer) RF devices have the flexibility to allow 3rd party software upgrades while maintaining compliance related capabilities?
  2. Is there a model similar to that of the mobile OS (Android, iOS, Windows) that could allow freedom for apps but protecting RF low level functions?
  3. What system design (hardware / software) options available to permit such capabilities?
  4. Are there cost or other impacts for such designs?
  5. Can only authorized users modify compliance related parameters and 3rd party users modify unrelated functions, and can authorization levels be reliably controlled?

SCR Subcommittee: Key Findings

- Multiple security methods exist (digital code signing, software partitioning, update blocking, etc.)
- Multiple stakeholder groups want to modify code for both RF-sensitive and non-RF-sensitive functions.
- Embedding security mechanisms to protect RF functions can block 3rd-party attempts to address security vulnerabilities.
- There is opportunity to improve guidance on documentation of devices.
- The challenge requires a much larger discussion (multi-stakeholder process) to strike a balance.
- SWG has developed a White Paper “Software Configurable Radio White Paper” – *Soliciting TAC Approval for Inclusion into Proceedings*

SCR Subcommittee: Recommendations

- **Recommendation**
  - This group recommends revising the type of guidance used for SCRs like U-NII to be more specific about disclosures manufacturers should make about the methods they employ.
- **Background**
  - Growth of software configurable radios and growth of free open source software have created an environment of rapid innovation for companies, individuals, academics, startups and more.
  - Software reconfigurations may change RF parameters under which the SCR was certified posing interference challenges.
  - Guidance on how to meet disclosure requirements for security methods allows for general responses.
  - Responses based on actual industry methods would improve visibility into potential issues at certification and actual issues in the field.

SCR Subcommittee: Recommendations

- **Additional Recommendation**
  - We further recommend that the FCC encourage formation of a multi-stakeholder forum to find a way in which manufacturers can strike the appropriate balance between embedding security mechanisms into SCRs and their ecosystem to ensure compliance with FCC service rules, while allowing innovation and the flexible addition of features, and fostering cybersecurity overall.
- **Background**
  - Contributions from the open source community made it clear that the scope of interests is much broader than this TAC subgroup.
  - This subgroup's white paper provides the background.
  - One trade association has agreed to consider hosting such a forum.
  - Some members of the 2016 subgroup are available to continue into 2017 to provide continuity and complete this effort.

2016 TAC Cybersecurity WG Recommendation Summary

- **5G:** The FCC should ensure proactive and broad industry support for 5G security by leveraging industry bodies (ATIS) and using the content and processes created and piloted by the TAC, to drive security by design principles into the 5G standardization process (3GPP).
- **Software Defined Networking:** The FCC should ensure proactive and broad industry support for security as a designed in principle for software defined networks by leveraging industry bodies (CSRIC) and using the content and processes created and piloted by the TAC to promote and drive best common practices across industry architectures and deployments.
- **Cybersecurity for Software Controlled Radios:** The FCC should revise the type of guidance used for SCRs like U-NII to be more specific about disclosures manufacturers make; and encourage the formation of a multi-stakeholder forum to address this challenge with a much wider group of inputs.

* https://transition.fcc.gov/oet/tac/tacdocs/reports/2016/TAC-5G-Cybersecurity-Subcommittee-09-12-16.pdf

Appendix

2016 TAC Cybersecurity Papers

- 5G Security

2016 FCC TAC 5G
ersec White Paper

- Securing SDN

2016 FCC TAC 5G
ersec White Paper

- Cybersecurity for Software Configurable Radios

2016 FCC TAC CS
White Paper 20161

Mobile Device Theft Prevention WG
Report to the FCC TAC

December 7, 2016

2016 MDTP WG

- The MDTP working group will continue to extend its work on device theft prevention

- Work proposed for 2016 includes developing recommendations on:
  - next generation anti-theft features,
  - assessment of the effect of previous recommendations on device theft,
  - development of recommendations for improvements in consumer outreach efforts,
  - development of mechanisms to support easier access for law enforcement to IMEI information,
  - and examination of methods for carriers to provide more useful data related to device theft and for fostering greater global effectiveness of proposed solutions.

WG Participants

- Co-Chairs:
  - Brian Daly, AT&T
  - Rob Kubik, Samsung
- FCC Liaisons:
  - Walter Johnston
  - Charles Mathias
  - Chad Breckinridge
  - Elizabeth Mumaw
- Dennis Roberson, FCC TAC Chair
- Document Editor: DeWayne Sennett, AT&T

- Jason Novak, Apple
- Timothy Powderly, Apple
- Ogechi Anyatonwu, Asurion
- Jay Barbour, Blackberry
- Brad Blanken, CCA
- John Marinho, CTIA
- Jamie Hastings, CTIA
- Mike Carson, ebay
- Mike Rou, eBay
- David Mersten, ecoATM
- Max Santiago, ecoATM
- Christian Schorle, FBI
- James Moran, GSMA
- Craig Boswell, Hobi
- Chris Drake, iconectiv
- Chip Stevens, iconectiv
- Kirthika Parmeswaran, iconectiv
- Sang Kim, LG
- Deepti Rohatgi, Lookout

- Gunnar Halley, Microsoft
- Joseph Hansen, Motorola
- Joe Heaps, National Institute of Justice
- Thomas Fitzgerald, New York City Police Department
- Jack Mcartney, Recipero
- Les Gray, Recipero
- David Dillard, Recipero
- Mark Harman, Recipero
- Maxwell Szabo, City and County of San Francisco
- Gary Jones, T-Mobile
- David Strumwasser, Verizon
- Samir Vaidya, Verizon Wireless
- Samuel Messinger, U.S. Secret Service

Thank You!

MDTP WG 2016 Priorities

✓

- Set up the common framework for collection of centralized data post July 2015 (e.g., through CTIA with input from OS providers, mobile operators, and law enforcement agencies) and framework for analysis of the data
  - (CTIA) Nielsen survey of consumers is in the field on the effectiveness of the theft prevention
  - (CTIA) Operator survey is currently underway to aggregate information

WORK IN PROGRESS CHECK BACK SOON!

- Continued studies to determine whether implementations post July 2015 have the desired effect on mobile device theft
  - Need to have data from CTIA and LEA from the above item before analysis can be performed.

✓

- Using the mechanisms being developed in ATIS and GSMA on enabling a mechanism for IMEI to be retrieved on disabled devices and educational outreach to law enforcement on using the mechanism
  - ATIS and GSMA best practices are in place.
  - Education outreach should be delayed until devices are available aligning with best practices.

WORK IN PROGRESS CHECK BACK SOON!

- Consider a study on how to expand blacklisting to all US carriers, working with the GSM Association/GSMA North American Regional Interest Group and CTIA
  - GSMA/GSMA-NA are attempting to work with carriers in the region to encourage them to use the IMEI database.
  - CTIA joint meeting with GSMA discussed development of a plan to outreach to these other US carriers.

Review of MDTP 2014 & 2015 Recommendations

- Developed Cross Reference of Industry MDTP Activity to MDTP Recommendations
  - Goal – make sure action is underway for all recommendations
- Identified Gaps to address:
  - Solutions providers and the ecosystem involved in reverse logistics (carriers, device recyclers, device resellers, etc.) - ensure that the solution providers have enacted a mechanism for reverse logistics providers
  - Perform ongoing study of potential new, measurable risks to public safety that requires future assessment and consideration by industry
  - Perform ongoing study and monitoring of the dynamic and changing threat environment
  - Investigation into whether the increased availability of anti-theft functionality on new have any effect including increasing consumer use of these features
  - Examine if anti-theft solution providers may be able to provide consumers a feature to determine enrollment status in their solution in such a way that the consumer does not have to be in physical possession of the device
  - ATIS, working with other key stakeholders such as the GSM Association, identify key technological areas where the FCC should seek further information from industry, including:
    1. IMEI
    2. Requirements and use of databases
    3. Future theft prevention opportunities

Cross Reference of Industry MDTP Activity to MDTP Recommendations

Recommendation	Associated Industry Activities
Recommendation (2014) 1.4 Recommendation (2014) 1.5	ATIS Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP) GSMA IMEI Retrieval on Disabled/Locked Devices
Recommendation (2014) 1.6	CTIA Stolen Phones Working Group
Recommendation (2014) 1.7	GSMA Information Reporting
Recommendation (2014) 1.15	CTIA Stolen Phones Working Group GSMA Carrier Recruitment
Recommendation (2014) 2.1	GSMA IMEI Database (GSMA Liaison with CTIA)
Recommendation (2014) 2.2	CTIA Stolen Phones Working Group
Recommendation (2014) 3.1	CTIA Mobile Device Information Portal (MDIP) CTIA Stolen Phones Working Group CTIA Annual Survey of Consumers

Recommendation	Associated Industry Activities
Recommendation (2014) 3.3	CTIA Stolen Phones Working Group
Recommendation (2014) 3.4	CTIA Mobile Device Information Portal (MDIP) GSMA IMEI Database
Recommendation (2014) 3.5	CTIA Mobile Device Information Portal (MDIP) CTIA Stolen Phones Working Group
Recommendation (2014) 3.6	CTIA Mobile Device Information Portal (MDIP) CTIA Stolen Phones Working Group
Recommendation (2014) 3.7	This effort is underway with continuous updates being provided to the FCC by CTIA.
Recommendation (2014) 3.8	CTIA Survey of Carriers GSMA Information Reporting
Recommendation (2014) 3.9	GSMA Device Blocking and Data Sharing Recommended Practice

Cross Reference of Industry MDTP Activity to MDTP Recommendations

Recommendation	Associated Industry Activities
Recommendation (2014) 4.3	GSMA IMEI Integrity Initiatives GSMA Anti-Theft Device Feature Requirements
Recommendation (2014) 4.4	CTIA Annual Survey of Consumers CTIA Survey of Carriers
Recommendation (2015) 1.1	CTIA Mobile Device Information Portal (MDIP) GSMA IMEI Database
Recommendation (2015) 1.2	CTIA Annual Survey of Consumers
Recommendation (2015) 1.3	CTIA Mobile Device Information Portal (MDIP) CTIA Stolen Phones Working Group
Recommendation (2015) 1.4	CTIA Stolen Phones Working Group CTIA Annual Survey of Consumers
Recommendation (2015) 1.5	CTIA Annual Survey of Consumers CTIA Survey of Carriers
Recommendation (2015) 1.7	CTIA Stolen Phones Working Group (Voluntary Commitment)
Recommendation (2015) 1.8	GSMA Device Blocking and Data Sharing Recommended Practice
Recommendation (2015) 1.9	GSMA IMEI Integrity Initiatives
Recommendation (2015) 1.10	CTIA Survey of Carriers
Recommendation (2015) 1.11	GSMA IMEI Integrity Initiatives
Recommendation (2015) 2.1	CTIA Mobile Device Information Portal (MDIP) CTIA Stolen Phones Working Group
Recommendation (2015) 2.2	CTIA Stolen Phones Working Group GSMA Carrier Recruitment
Recommendation (2015) 2.4	CTIA Annual Survey of Consumers CTIA Survey of Carriers

Industry MDTP Related Activities

- ATIS Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)
- CTIA Mobile Device Information Portal (MDIP)
  - MDIP is envisioned to be available by the end of 2016 for the Phase 1 set of requirements
  - Phase two requirements are envisioned for implementation in 2017
- CTIA Stolen Phones Working Group
  - Anti-Theft Voluntary Commitment
  - Implementation of the MDIP
  - Point for coordination with GSMA and GSMA-NA regarding industry best practices and outreach to law enforcement and other relevant industry stakeholders
- CTIA Annual Survey of Consumers
  - Solicit information regarding the adoption of anti-theft security tools on smartphones
- CTIA Survey of Carriers
  - Anonymized survey of carriers across the US to solicit feedback concerning the number of smartphones reported lost or stolen, as well as the number of potentially duplicate IMEI or MEID identifiers that may be present (4Q2016)

Industry MDTP Related Activities - continued

- GSMA MDTP Related Activities
  - IMEI Retrieval on Disabled/Locked Devices
    - Device Security Group (DSG) recognized the need to resolve the problem of extracting IMEIs from devices that have a kill switch enabled and triggered
    - ATIS presented its proposals to DSG, which fully endorsed and supported the mechanisms described in ATIS' "Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention"
  - GSMA Information Reporting
    - Quarterly reports that lists the mobile carriers and countries that are connected to GSMA's IMEI Database and the degree to which IMEI data relating to devices reported lost or stolen is shared between the connected carriers
  - GSMA Carrier Recruitment
    - Extensive campaign to recruit more carriers to participate in the device blocking and data sharing initiatives in the USA
    - Compiling feedback from those unable to commit to block devices and/or share data as to the reasons why, in order that impediments can be identified with a view to resolving them
  - GSMA IMEI Database
    - Continues to provide IMEI lookup services directly to device traders, law enforcement agencies and regulators and to consumers, through local database applications in a number of countries
    - Policy changes were introduced to ensure the widest possible access to IMEI checking services by extending the right of access to countries not already connected to the IMEI Database

Industry MDTP Related Activities - continued

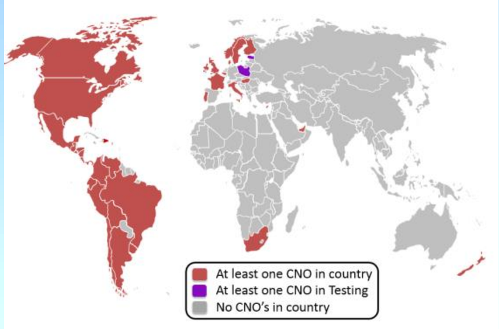
- GSMA MDTP Related Activities
  - GSMA Device Blocking and Data Sharing Recommended Practice
    - Recommended practices to be observed by US carriers pertaining to the blocking of lost and stolen mobile devices on their networks and to the sharing of data relating to those devices via the GSMA's IMEI Database
    - Recommendations are designed to address inconsistencies that may exist between the individual policy, technical and process approaches adopted by the US carriers that block devices and share information via the IMEI Database
  - GSMA IMEI Integrity Initiatives
    - Reviewed documentation pertaining to two of its initiatives designed to strengthen the security and integrity of IMEI implementations in devices to maintain trust and value in device blocking at a network level
    - Committed to working with device manufacturers to ensure IMEI security remains an important enabler to combat device theft
    - Device Security Group (DSG) undertook a review of the IMEI Security Technical Design Principles, which were defined to help device manufacturers develop a comprehensive security architecture that facilitates the deployment of a range of solutions to protect the platform on which the IMEI mechanism is stored and the IMEI implementation itself
    - DSG also undertook a review and update of the IMEI Security Weakness Reporting and Correction process, which established a formal process to centralize the reporting of newly identified IMEI security weaknesses to the affected device manufacturers and to have those issues resolved to improve device security levels during the remaining manufacturing life cycle of the product

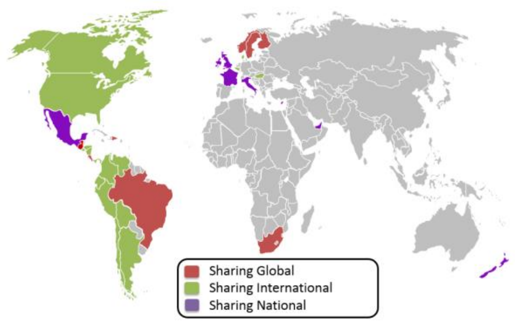
Industry MDTP Related Activities - continued

- GSMA MDTP Related Activities
  - GSMA Anti-Theft Device Feature Requirements
    - Defines a set of requirements that can be used by device manufacturers, mobile network operators, and third party service providers, to offer features to device owners to assist in locating lost/stolen devices and to protect the data within the device
    - Focused on securing the owner’s device and data using software features available on the device and/or within the mobile network and the requirements have the potential to set a benchmark for anti-theft features

GSMA Stolen Device Data Sharing Reports

- Describes the network operators participating in the exchange of IMEI data concerning devices reported lost or stolen
- Data is taken from the GSMA IMEI database and relates to operators with active live or test user accounts
- GSMA provides the blacklist information on a 24/7 basis to the operators that have established connections to the IMEI Database for them to download and use within their own networks for device blocking purposes





Key Take-away: There are many countries currently not participating in lost and stolen blacklisting and/or lost and stolen data sharing not taking place between operators, Especially Asia, Africa, Middle East

Mobile Device Information Portal - CTIA

- CTIA Stolen Phones Working Group RFP issued February 2016
  - Based on TAC MDTP Report and Portal requirements
- Several industry responses to RFP March 2016
- Detailed evaluation of responses concluded
- Vendor selection completed
- Contract executed for Portal Implementation October 2016
  - Vendor selected: GSMA
- Portal development and implementation underway
  - Consumers, Law Enforcement and Commercial Entities
  - Planned launch early in 2017
  - Public announcement planned coincident with Portal launch

CTIA Consumer Awareness and Adoption of Security Measures Survey Results

- The survey found that:
  - 69 percent of wireless consumers use PINs/passwords on their smartphones, up 13 percent from 2015, and up 38 percent from the first survey in 2012; and
  - 51 percent have built-in remote lock and erase software installed on their smartphones, up 42 percent from 2015, and up 31 percent from 2012.
- When asked about their general security practices for their smartphones, respondents said:
  - 73 percent run software updates every or almost every time on their personal smartphones;
  - 51 percent of users have an anti-virus program installed on their smartphones, up 28 percent from 2015, and up 65 percent from 2012; and
  - 86 percent say they are familiar with cybersecurity, defining it with protection, safety and prevention of unauthorized access.

CTIA Consumer Awareness and Adoption of Security Measures Survey Results

- 11 percent who reported losing a smartphone, less than half – 4.7 percent – reported it was stolen, with the rest reporting it was misplaced.
- 51% of smartphone owners say they have built-in capability for remote lock / locate / erase, though only one-third of all smartphone owners have enabled the capability.
  - One-third are not aware of such a capability being on their phone.
  - Half of users with the capability enabled it within the last year.
- Nearly half of those not enabling the lock / locate/ erase capability cite worry that they might accidentally lock or erase their data as a top reason for not enabling it.
- One-third cite too many passwords to keep track of, with lack of need and lack of time as other top reasons cited by 21 and 29 percent of those not enabling the capability.
- More information and an easier walk-through to set-up the capability are cited as encouragements to set-up by 39 and 34 percent respectively of smartphone owners who have not enabled the capability.
- Most users who have lost phones report recovering misplaced phones, with stolen phones being replaced
- Anonymized survey of carriers across the US is needed to solicit feedback on a range of matters including the number of potentially duplicate IMEI or MEID identifiers that may be present”

Challenges Tracking Where Stolen Devices Go

- Cellular operator relationships via Service Subscriptions and not via Device Ids
  - Bring Your Own Device (BYOD) model
  - Can have multiple subscriptions per mobile device

- Stolen devices can be used as Wi-Fi only devices
  - OTT applications can provide text, voice, and data services.
  - No involvement with or awareness by cellular operator networks.

- Cellular operator has limited visibility to mobile devices
  - Can only be aware of devices connecting to cellular operator’s network
  - Not aware if additional subscriptions on mobile device
  - Not aware if mobile device moved to a new subscription
  - No mechanism to determine where a specific mobile device is being used.

- Other ecosystem players such as OS vendors, mobile phone manufacturers and operators of app stores may be able to identify and flag changes of ownership and location of stolen mobile phones. Additional study is required.

Measures are working, Criminals are getting smart

- Man stole box load of cell phones, resold some, police say
  - http://www.ksat.com/news/man-arrested-after-selling-stolen-cell-phones-affidavit-says, November 17, 2016
  - "She told investigators that she bought two cell phones … and **within hours of having them activated, saw her phone service shut down due to the phones being stolen**."
- Chicago - Robbers demanding victims reset their phones in South Loop
  - Posted: Sep 12 2016 12:54PM CDT
  - http://www.fox32chicago.com/news/crime/204739103-story
- Dalton PD: Cellphone theft caught on surveillance video
  - Submitted by the Dalton Police Department, Nov 29, 2016 daltondailycitizen.com, Dalton, GA
  - "The Dalton Police Department is asking for the public's help with identifying a woman who took a cellphone left behind by accident at a local store."
  - **"The victim's cellphone was turned off right after it was taken from the store."**
  - Device was simply powered off rather than blocked. That has been a common approach for thieves for many years to make it more difficult to identify that they are in possession of the device.

An Emerging Threat – Cellphone Number & Privacy

- A 10-Digit Key Code to Your Private Life: Your Cellphone Number
  - http://www.nytimes.com/2016/11/13/business/cellphone-number-social-security-number-10-digit-key-code-to-private-life.html?_r=0
  - “The cellphone number is more than just a bunch of digits. It is increasingly used as a link to private information maintained by all sorts of companies, including money lenders and social networks. It can be used to monitor and predict what you buy, look for online or even watch on television.”
  - “investigators find that a cellphone number is often even more useful than a Social Security number because it is tied to so many databases and is connected to a device you almost always have with you”
  - “It’s not foolproof, but if a cellphone is lost or stolen, **it is typically locked**. It can be hacked into, but that takes a separate set of skills.”
    - Stresses the importance of the MDTP measures being put in place

Recommendations

- Increase Global Awareness and Participation in Smartphone Antitheft Measures Recommendation for 2016
  - The FCC TAC recommends that the FCC work with the U.S. State Department and other Executive Branch agencies of the government to lobby internationally for greater engagement on device theft issues.
  - This lobbying effort should include the goal of increasing the number of carriers participating in the blacklisting of stolen devices in the global IMEI database, as well as using data from the database to block blacklisted mobile devices on their networks.

Recommendations

- State, Local, Federal, and Tribal Law Enforcement Theft Information Recommendation for 2016
  - The FCC TAC recommends that the FCC work with State, Local, Federal, and Tribal Law Enforcement to assess the effectiveness of the mobile theft prevention measures implemented by the wireless industry.
  - The CTIA Consumer Survey measures the effectiveness of having consumers activate anti-theft mechanisms on their mobile devices. However, what remains unknown is the effectiveness of these mechanisms on the prevention of mobile device theft. Consequently, information is required from state, local, federal and tribal law enforcement regarding the patterns and trends in mobile device theft in order to assess the effectiveness of the mechanisms that have been implemented by the wireless industry.
  - Included in this assessment is the evaluation of a method to capture and share lost/stolen device attempt-to-trade activity data as a means to capture cross carrier, international, and other off-network activity that does not directly involve operator activation activities.

Additional Recommendations

- National Smartphone Antitheft Measures Framework Recommendation for 2016
  - The FCC TAC recommends that the FCC develop a smartphone antitheft measures national framework, including a consumer education kit, a voluntary code of conduct for device resellers, work with a range of law enforcement associations on consumer outreach, work with Congress on the introduction of legislation to criminalize the reprogramming of IMEIs.
- Reverse Logistics Recommendation for 2016
  - The FCC TAC recommends that the FCC work with the solutions providers and the ecosystem involved in reverse logistics (carriers, device recyclers, device resellers, etc.) ensure that the solution providers have enacted a mechanism for reverse logistics providers for devices that are covered by the industry commitments.
  - The approaches to such mechanisms vary by solution provider, but as long as there are manual or automated means to successfully achieve disabling protection, industry stakeholders should have flexibility in determining the right approach.
  - A prescriptive recommendation on the technical approach to reverse logistics limits innovation, including the ability to maintain security of reverse logistics solutions, by solution providers in a competitive market.
  - Since this recommendation was initially proposed in the 2014 MDTP report, there has been some reverse logistics methodologies implemented but these implementations do not provide reverse logistics mechanisms for all makes and models of mobile devices.

Additional Observations

- Carriers
  - Much has already been done by the major US carriers and the remaining obvious required action is for the carriers not already blocking devices and/or connected to the IMEI Database to do so.
  - Potentially, an additional action could be taken by the operators connected to the IMEI Database to comply with the recently approved recommended GSMA best practices.

- OEMs
  - The 2015 FCC MDTP report contained a number of recommendations related to IMEI security but the prioritization exercise that was conducted at the start of the work this year resulted in these being de-prioritized and ultimately eliminated. For its part, GSMA did take the opportunity to review the technical design principles and the IMEI weakness reporting and correction process.
  - A recommendation is for OEMs to commit to this issue may be required if further progress is to be made.
  - Recommendation 1.11 specifically asked that the previously outsourced IMEI security weakness monitoring and reporting service be reinstated by GSMA.

- OS Vendors
  - Recommendations 3.5 from the 2014 report and 2.3 from the 2015 report asked anti-theft solution providers to provide a facility for consumers to check the activation status of their solutions as a potential warning to consumers purchasing used devices that a device may be stolen and disabled.
  - Tracking of lost/stolen devices is another issue on which the OS vendors are uniquely placed to assist as they alone have visibility of which networks their devices are attached to, cellular or non-cellular. MDTP WG strongly believes this is something that should be discussed as it is this community, rather than the operators, that can help the FCC achieve its goal to generate some intelligence on where stolen devices are ending up.
  - The topic of device tracking involves some important considerations. For example, device tracking without the direction and consent of the authorized user is likely to conflict with privacy laws in the U.S., the European Union, and elsewhere. In addition, devices operate in an international realm. There are potential human rights issues involved with tracking devices without user consent for the purpose of turning that information over to law enforcement or other government authorities, particularly outside the U.S.
  - **MDTP WG strongly believes continued discussion is needed to help the FCC achieve its goal to generate some intelligence on where stolen devices are ending up.**

Further Work Needed

- Analyze future threats and consequences of mobile phone theft solutions
- Additional Studies Addressing Challenges of Tracking Where Stolen Devices Go
- Impact of Mobile Device Information Portal launch
- Discussions with Federal/State/Local/Tribal Law Enforcement
  - Providing the Police Chiefs with a briefing on the MDTP Information Portal (MDIP) currently being developed.
  - Soliciting feedback from the Police Chiefs on the MDIP Portal.
  - Request the Police Chiefs to advertise the MDIP Portal with their La Enforcement colleagues.
  - Request updated smartphone theft statistics in order to evaluate the effectiveness of the theft prevention measures implemented to date.

FCC Technological Advisory Council Working Group:

Implications for Mass Deployment of Aeronautical/Space Transmitters

December 7, 2016

Working Group

Steve Lanning (ViaSat) co-chair

Michael Tseytlin (Facebook) co-chair

Jeffrey Foerster (Intel)

Dale Hatfield (U Colorado)

Adam Drobot (OpenTechWorks)

Russ Gyurek (Cisco)

Lynn Merrill (NTCA, MRL&Co)

Brian Daly (AT&T)

Pierre de Vries (U Colorado)

Brian Fontes (NENA)

Brian Swenson (Microsoft)

Lisa Guess (Juniper)

Geoffrey Mendenhall (GatesAir)

McNamara, Mike (TW Telecom)

Amit Ganjoo (ANRA Technologies)

Maqbool Aliani (Ligado)

Paul Misener (Amazon)

Mark Bayliss (Visual Link)

Michael Ha (FCC liason)

Brian Butler (FCC liason)

Aeronautic Contributors

Joe Cramer (Boeing)

Tom Fagan (Raytheon)

Mike Lindsay (OneWeb)

Andrew Thurling (Aerovironment)

Shaun Coghlan (Aeryon)

Craig Ranta (Aeryon)

Michael Marcus (Marcus Spectrum)

Cortney Robinson (AIA Aerospace)

Scott Kotler (Lockheed Martin)

Alexander Gerdenitsch

Jennifer Richter (Akin Gump/CTIA)

Alex Epshteyn (Boeing)

Mike Lindsey (OneWeb)

Sean Cassidy (Amazon)

Richard Heinrich (Rockwell Collins)

Patricia Cooper (SpaceX)

Don Jansky (Jansky-Barmat Telecommunications)

Ramesh Lakshmi-Ratan (Bell and Howell)

Steve Chacko (ViaSat)

Sergio Bovelli (Airbus)

Daniella Genta (Airbus)

Amit Ganjoo (Anra Technologies)

Charlie Zhang (Samsung)

Mike Senkowski (DLA Piper)

Anna Gomez (Wiley Rein)

Sean Murphy (T-Mobile)

Overview of 4Q Activities

- Non-Geostationary (NGSO) Satellite-based Broadband Services
- High Altitude Platform Stations (HAPS)
- End to End Review of delivery platform
- Detect and Avoid
- UTM Update
- UAS Discussions
- Refine recommendations

Base Definitions

Small Unmanned Aircraft – an unmanned aircraft weighing less than 55 pounds, including everything that is on board, or is otherwise attached to the aircraft. "Unmanned "means that it is operated without the possibility of direct human intervention from within or on the aircraft. Small unmanned aircraft can be used for either recreational or commercial purposes.

Small UAS – Small Unmanned Aircraft System ("UAS") means a small unmanned aircraft and its associated elements (including communication links and the components that control the small unmanned aircraft) that are required for the safe and efficient operation of the small unmanned aircraft in the national airspace system.

Recreational Use – the "hobby" or "recreational" market for small UAS, intended solely for fun. To fly a small UAS for fun, there are two options: (1) Fly in accordance with the Special Rule for Model Aircraft (Public Law 112-95 Section 336), which includes following a community-based set of safety guidelines (AMA is the only recognized organization) Or, (2) Fly in accordance with the FAA's Small UAS Rule (Part 107).

Base Definitions

Part 107 Commercial Use – the commercial market for small UAS, which includes any operation in furtherance of a business, whether or not money is transferred, such as photography, agriculture, pipeline inspection, delivery, etc.   Part 107 users must give way to manned aircraft, operate within the VLOS, fly during daylight or in twilight with minimum weather visibility of 3 miles from the control station, fly at or below 400 feet AGL, refrain from flying over anyone not directly participating in the operation, etc. The operator must have a remote pilot airman certificate, be at least 16 years old, and may only operate one unmanned vehicle at a time.

Part 107 Waivers – the FAA has procedures for authorizing *deviations* from Part 107 for the following regulations, among others: (1) operation from a moving vehicle or aircraft; (2) daylight operation; (3) VLOS operation; (4) operation of multiple small UAS; (5) operation over people, etc.

Non-Part 107 Commercial Use – Any UAS not covered by Part 107.

NGSO Systems

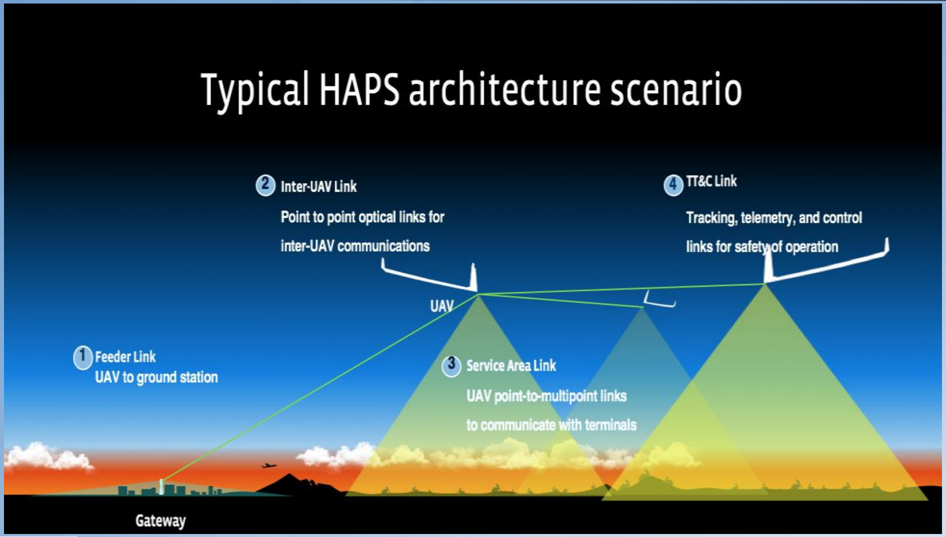
- NGSO satellite systems intended to provide fixed and mobile-satellite service (MSS) to earth stations are subject to a processing round
  - After a "leading NGSO application" is accepted for filing a cut-off date is established for the submission of competing applications using overlapping frequency bands
  - Now on circulation: NGSO FSS NPRM for Parts 2 & 25
- Ku-/Ka-band: Processing Round for NGSO systems closed November 15
  - Triggered by OneWeb Petition for Declaratory Ruling for market access for 720 satellite system in the 10.7-12.7 GHz, 14.0-14.5 GHz, 17.8-18.6 GHz, 18.8-19.3 GHz, 27.5-28.35 GHz, 28.35-29.1 GHz, and 29.5-30.0 GHz bands
  - 11 Additional NGSO applications filed
- V-band: Processing Round for NGSO systems open until March 1, 2017
  - Triggered by Boeing application to operate an NGSO system consisting of 2956 satellites in the 37.5-40GHz, 40-42GHz, 47.2-50.2GHz and 50.4-51.4GHz bands

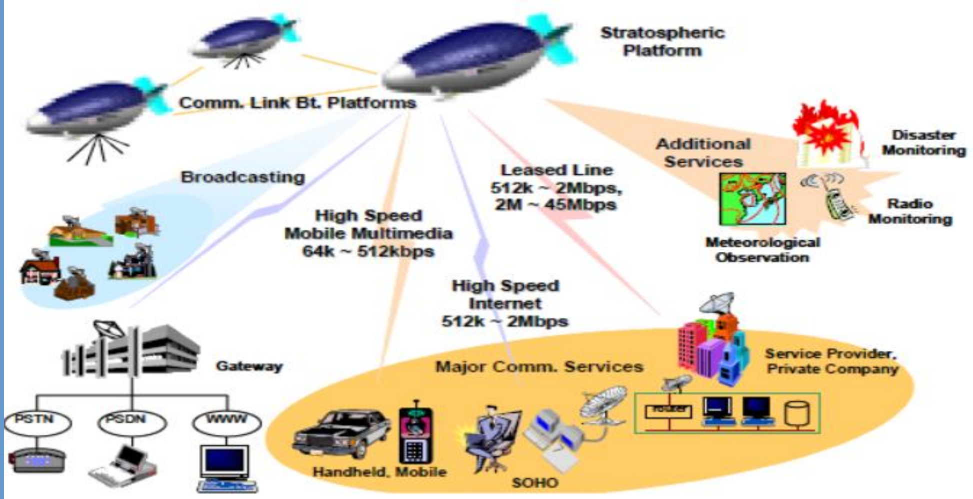
NGSO Systems - Applications filed in the Ku-Ka-band Processing Round

Satellite System Key Investors	# of Satellites	Frequency Bands
OneWeb	720	• Ku/Ka-bands
O3b/SES	20 + 40 add.	• Ka-band
SpaceX	4425	• Ku/Ka-bands
Boeing	60	• Ka-band
Telesat Canada	117	• Ka-band
LeoSat MA, Inc.	78	• Ka-band
Audacy Corporation	3	• Ka/ V-bands
Theia Holdings A Inc.	112 + 8 spares	• Ku/Ka-band, EESS, L-band radar
Kepler Communications Inc.	140	• Ku-band
ViaSat, Inc.	24 + 4 spares	• Ka/V-bands
Karousel LLC	12	• Ku/Ka-bands
Space Norway AS	2	• Ku/Ka-bands

High Altitude Platform Stations (HAPS)

The ITU definition - "a station located on an object at an altitude of 20 to 50 km and at a specified, nominal, fixed point relative to the Earth."
Two types of platforms:
Heavier than Air and Lighter than Air


Typical HAPS architecture scenario
2 Inter-UAV Link
Point to point optical links for inter-UAV communications
4 TT&C Link
Tracking, telemetry, and control links for safety of operation
UAV
1 Feeder Link
UAV to ground station
3 Service Area Link
UAV point-to-multipoint links to communicate with terminals
Gateway



Today, there is only one global allocation for HAPS, consisting of 600 MHz in the V Band (47/48 GHz). Because of the problem with rain fade, particularly in tropical rain zones, about two dozen countries in Southeast Asia agreed to an additional 600 MHz in the Ka Band (28/31 GHz) in 2000. At a subsequent WRC, four African countries and Australia (an early proponent of HAPS) agreed to 160 MHz at C Band (6 GHz) for gateway links.

Spectrum for use by HAPS was accepted as Agenda Item 1.14 at WRC-19

- Study additional spectrum needs for gateway and fixed terminal links for HAPS to provide broadband connectivity in the fixed service

- To study the suitability of using the existing identifications on a global or regional level (including 47.2-47.5 GHz and 49.9-48.2 GHz globally, and 27.9-28.2 GHz HAPS-to-ground and 31-31.3 GHz ground-to-HAPS outside Region 2)

- To study appropriate modifications of existing footnotes and associated resolutions

- To study the following frequency bands already allocated to the fixed service on a primary basis

  - On a global level, 38-39.5 GHz, and

  - On a regional level, in Region 2, 21.4-22 GHz and 24.25-27.5 GHz

- These studies include sharing and compatibility studies to ensure protection of existing services allocated in the frequency ranges identified

High Altitude Platform Stations (HAPS)

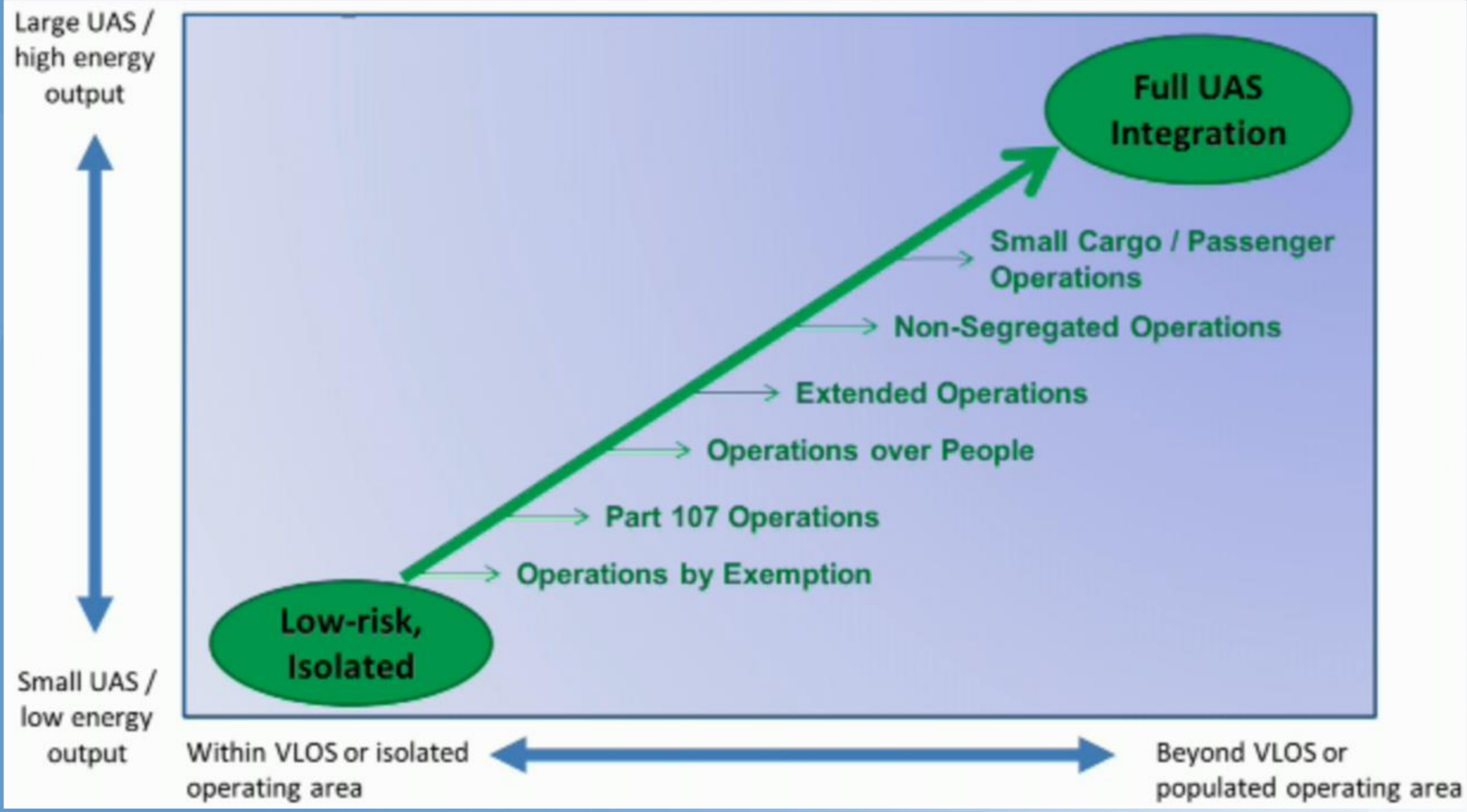
- Several companies worldwide are engaged in development
  - Facebook demonstrated first Aquila flight
  - Google flew Titan last year
  - Airbus ongoing project on Zephyr in UK
  - Thales develops Stratobus
- As HAPS are still in the experimental stage, the TAC WG recommends individual companies continue their efforts and inform FCC on their progress, as appropriate.
- No further action is required by FCC at this moment

Stratobus
ThalesAlenia Space
NEWS
An autonomous stratospheric platform, midway between a satellite and a drone
To be built by Thales Alenia Space and its partners

Large UAS (HALE/MALE/HAPS) Recommendations

- TAC recommends the Commission begin and quickly conclude proceedings on service rules for Command and Control (C2) for large UAS, including HALE/MALE/HAPS, using ITU recommended frequency bands, including; portions of the “L-band” and “C-band”, and utilizing Satellite Services.
- The TAC also recommends the FCC gather information on the Payload Services for large UAS, particularly HAPS, targeted applications and sharing techniques with incumbent users.

FAA Strategic Priorities



Large UAS / high energy output

Small UAS / low energy output

Within VLOS or isolated operating area

Beyond VLOS or populated operating area

Low-risk, Isolated

Operations by Exemption

Part 107 Operations

Operations over People

Extended Operations

Non-Segregated Operations

Small Cargo / Passenger Operations

Full UAS Integration

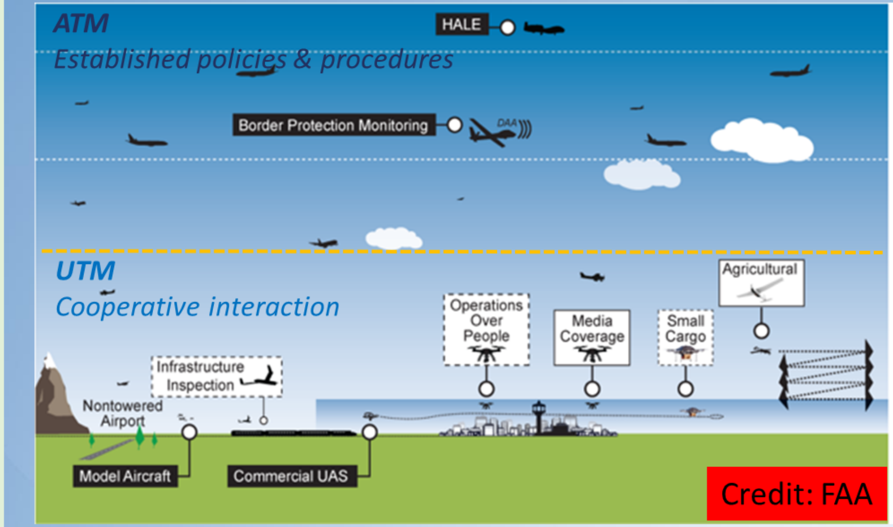
- UTM Principles: Services for Safe Integration
  - Users operate in airspace volumes as specified in FAA authorizations, which are issued based on type of operation and operator/vehicle performance
  - UAS stay clear of each other
  - UAS and manned aircraft stay clear of each other
  - UAS operator has complete awareness of airspace and other constraints
  - Public safety UAS have priority over other UAS
- Key UAS-related services
  - Authentication
  - Airspace configuration and static and dynamic geo-fence definitions
  - Weather and wind prediction and sensing
  - Conflict avoidance (e.g., airspace notification)
  - Demand/capacity management
  - Large-scale contingency management (e.g., GPS or cell outage)

Source: NASA

NASA UTM Project Scope (and RTT focus) – In close coordination with FAA

Scope focuses on uncontrolled airspace and uncontrolled operations inside controlled airspace

- Predominantly small UAS (< 55lbs)
- Beyond visual line of sight (BVLOS) of the operator
- Low altitudes (at or below 400 feet AGL)
- All airspace classes (B, C, D, E, & G) except Class A
- Airspace where the FAA does not interact directly (e.g., no controller clearances to each vehicle)



Credit: FAA

UTM construct is scalable to other uncontrolled airspace and vehicle classes:
ODM, high altitude (60,000 ft.), and space traffic (100K ft.): anywhere FAA does not provide services

Source: NASA

Current UAS Uses and Applicable FCC Rule Parts

	FAA Part 107 (Recreational)	**FAA Part 107 (Commercial)**
Applications	Recreational Non-revenue	Commercial uses in furtherance of business, whether or not money is exchanged, including : real estate, news services, photography, package delivery agricultural, utilities surveys, fleet service
User Base	Individuals	Individuals, public safety, industry, utilities, newsgathering, drone service providers, package delivery
Command & Control (C2) Links	FCC Parts 15/95/97	FCC Parts 15/22/24/27/90 Terrestrial cellular or satellite with appropriate reliability
Payload Links	FCC Parts 15/24/95/97	FCC Parts 15/22/24/25/27/90 Terrestrial cellular or satellite

Recommendations on Part 107 Commercial and Recreational UAS

- The Commission should promote use of existing communications infrastructure whenever possible to support small, low-altitude UAS communications functions avoiding unnecessary costs and regulatory delays.
- Commercial wireless networks, which enjoy flexible licensing, and commercial satellite networks, present solutions for control, tracking and payload communications for small, low altitude UAS. There is no need for a new regulatory regime.
- Although the working group does not anticipate the need, the Commission should act now to study if any rule changes or additions are required in order to allow for airborne use of commercial wireless bands
- Most, if not all, UAS communications needs are foreseeable, and the Commission's work can be done in parallel to the FAA's, not serially and there is no need to delay action

Recommendations on Small UAS - cont

- The Commission should harmonize the 800 MHz band with other commercial mobile wireless bands, allowing its use to support airborne communications for small, low-altitude UAS.
- As the Commission considers autonomous cars and other similar applications that provide for collision avoidance technologies (DAA, SAA in 5.9 GHz, 24 GHz, 32 GHz, 76-81 GHz and other bands), the Commission also should consider collision avoidance spectrum opportunities for small UAS at low-altitudes and whether the same technologies and bands should be available for both use cases.
- The Commission should support use of commercially available licensed and unlicensed bands wherever possible for small, low-altitude UAS.
- The Commission should support use of ADS-B technology for small UAS to coordinate operations among manned and unmanned aircraft, allowing small UAS to listen for ADS-B messages from manned aircraft, and transmitting identity and location information for small UAS using either ultra-low-power ADS-B or alternate implementations of ADS-B-like technologies.

Recommendations on Small UAS - cont

- The FCC should support innovation and technology leadership by the United States, similar to other countries that already have embraced UAS technology.
- The Commission should initiate a rulemaking process for command and control links using the C-band and the L-band. The Commission’s allocations and service rules for these bands should be flexible enough to accommodate future uses of these bands by low-altitude small UAS.
- The Commission should recognize, however, the C-band and L-band allocations for UAS from the World Radio Conferences in 2007 and 2012 are not near-term solutions for control links for small, low-altitude UAS. The use of commercial wireless bands, to support small, low-altitude UAS should not be delayed as a result this proceeding.

Thank you

Future Game Changing Technologies Working Group

Chairs: Kevin Sparks and Adam Drobot
FCC Liaison: Walter Johnston

7-Dec.-2016 Washington, DC

FGCT Working Group Charter for 2016

The work group will continue its focus on seminal technical areas for 2016:

i) Concentrate on identifying the technical challenges in developing 5G and what can to be done to ensure rapid deployment in the U.S;

ii) Examine potential new business models and service regimes that could be enabled by future programmable networks. The work group will also address the adoption of dynamic, virtualized networks and the implications for current FCC rules and policies;

iii) Address how the FCC can better anticipate rapid changes in technology and an approach to rules and policies that have the best outcome for rural and urban settings.

iv) Finally, the work group will continue its efforts to identify key new and emerging technologies

Working Group Members

- WG Chairs: Kevin Sparks, Nokia
  Adam Drobot, OpenTechWorks
- SWG Chairs: Nomi Bergman, Advance/Newhouse
  Brian Daly, AT&T
  Charla Rath, Verizon
- FCC Liaison: Walter Johnston, Padma Krishnaswamy
- Members:
  - Kumar Balachandran, Ericsson
  - John Barnhill, Genband
  - Mark Bayliss, Visualink
  - Michael Browne, Verizon
  - Lynn Claudy, NAB
  - Marty Cooper, Dyna LLC
  - Jeffrey Foerster, Intel
  - Dick Green, Liberty Global
  - Lisa Guess, Juniper Networks
  - Russ Gyurek, Cisco

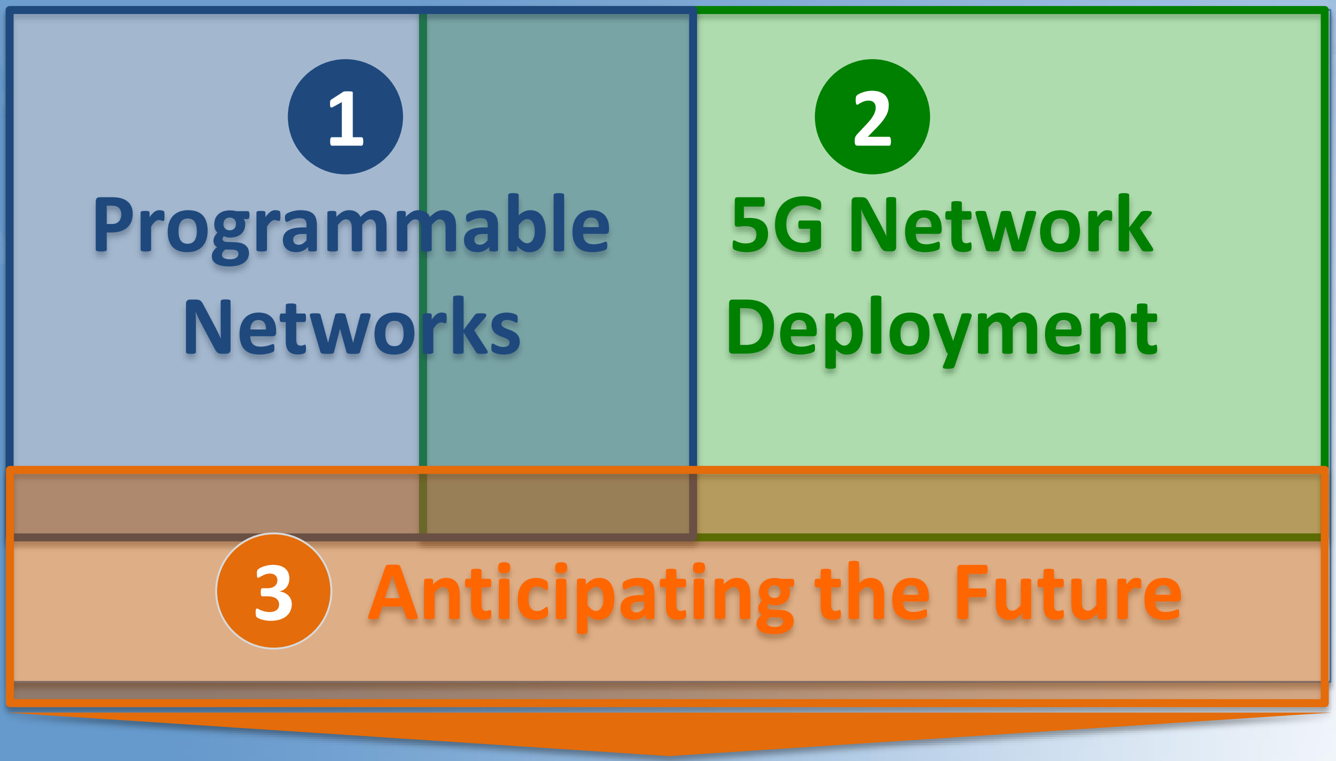
Working Group Members Cont'd

- Steve Lanning, Viasat
- Brian Markwalter, CEA
- Lynn Merrill, NTCA
- Paul Misener, Amazon
- Jack Nasielski, Qualcomm
- Ramani Panduragan, XO Communications
- Charlie Jianzhong Zhang, Samsung
- Chenghao Liu, Samsung
- Mark Richer, ATSC
- Hans-Juergen Schmidke, Facebook
- Dewayne Sennett, AT&T
- Marvin Sirbu, SGE
- Paul Steinberg, Motorola Solutions
- Michael Tseytlin, Facebook
- Dale Hatfield, SGE

SME Presentations and Discussions

April 28th “Network Latency in LTE” Ericsson
May 20th “3GPP Low Latency Requirements” Intel – Nageen Hymayat
May 20th FCC Wire-line and Wireless Bureaus Discussion
May 27th “5G” Nokia – Volker Ziegler
May 27th “Programmable Networks” VmWare - Dharma Rajan
June 3rd “5G Cutting the last Cord” Phazr – Farooq Khan
June 3rd “Futurescapes” Institute for the Future – Mike Liebhold
July 29th “Holographic Beamforming” Pivotal Communications – Eric Black
August 5th “Advanced antennas” Kymeta – Nathan Kundtz
August 12th “The 4P Project” Stanford U. – Prof. Nick McKeown
August 25th “Wireless Access Products” Tarana Wireless - Steve Sifferman
August 26th “Terragraph Briefing” Facebook – Neeraj Choubey
August 26th “Spectrum Collaboration Challenge” DARPA – Paul Tilghmane
Sept. 1st “Expected Tech Changes in Media Distribution” Akamai – Will Law (joint w/NGI)
Oct. 28th “5G” Verizon - 5G: Adam Koeppe, VP - Network Technology Planning

2016 FGCT WG Focus Topics

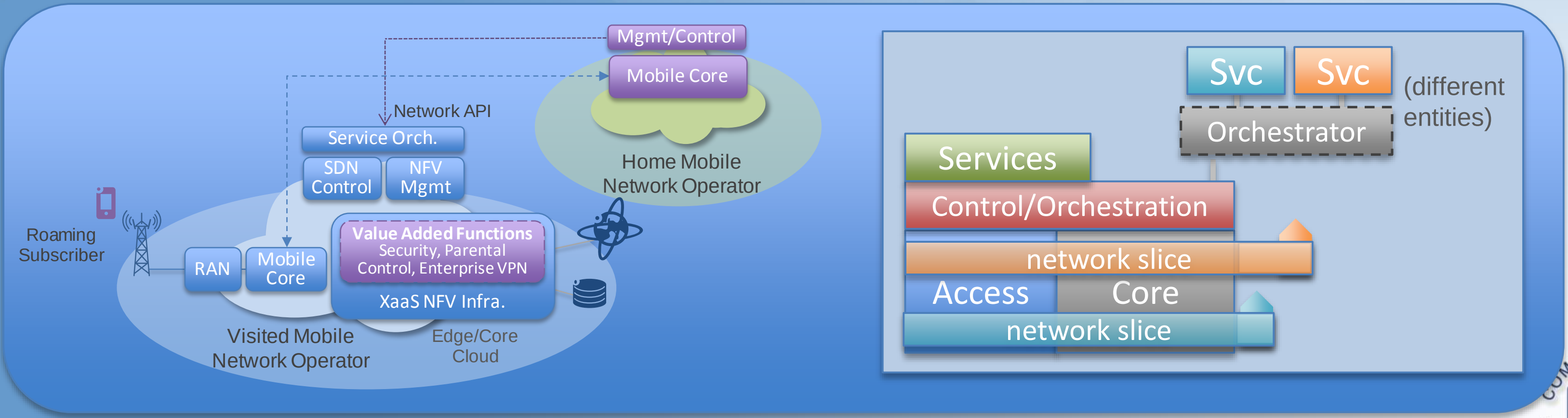


1 Programmable Networks

2 5G Network Deployment

3 Anticipating the Future

Programmable Networks



Programmable Networks

Dimensions of Change

1) **Convergence** – blurring of wireline & wireless networks; services offered independently of access type
2) **Disaggregation** – service functions virtualized & modularized; service chain can be split across entities
3) **Virtualized Sharing** – multi-tenant compute, functional and networking capacity that entities lease & control
4) **Dynamic Consumption** – network resources consumed on-demand, for short durations, with variable capacity

Example Use Cases

❖ **Localized mobile operator roaming** (home functions in visited network)

❖ **IoT video Application Provider** (local processing for BW-intensive appl.)

❖ **Low latency services/Tactile Internet** (AR/VR, industrial automation, robotic control)

❖ **Network slicing for providing QoS** (appl.-specific slice of network)

❖ **Converged wireless/wireline carrier** (access independent services)

Prog. Networks - Implications for FCC (1/2)

Regulatory Structure – As wireline and wireless networks blur, the structure of regulations and staff will need to move away from access technology defined silos to a more inter-connected model reflecting the variety of new service delivery architectures.

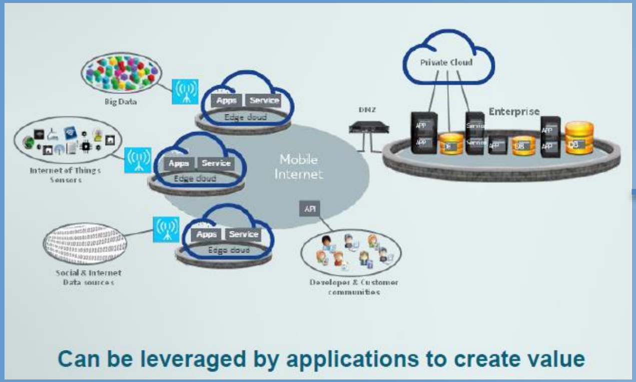
Entity Classifications - Definitions of communications service entities regulated by the FCC and corresponding rights and obligations (e.g. 911/PSAP access, number assignment, SS7 access, legal intercept) may need to be flexibly assigned according to functional roles in disaggregated service delivery chains.

Process Dynamics - Processes for establishing services and for incremental expansion of provider footprint (spectrum, capabilities, geographic scope) will need to be streamlined and dynamic (i.e. portal/API-driven automation).

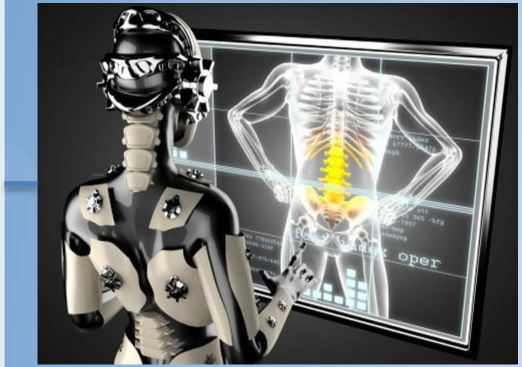
Prog. Networks - Implications for FCC (2/2)

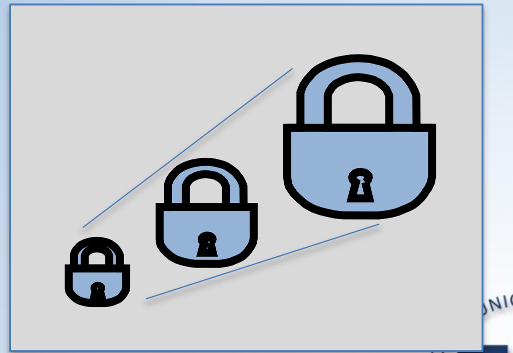
Tactile Internet QoS – Extremely low latency and mission critical services may require prioritization (even though otherwise an Internet service), or even dedicated/ preemptory access to spectrum.

Security – Programmable network slices may have greatly improved security properties from SDN automation tools. They also introduce additional security aspects to address, due to an altered attack surface and larger scope of control exposure.



Can be leveraged by applications to create value





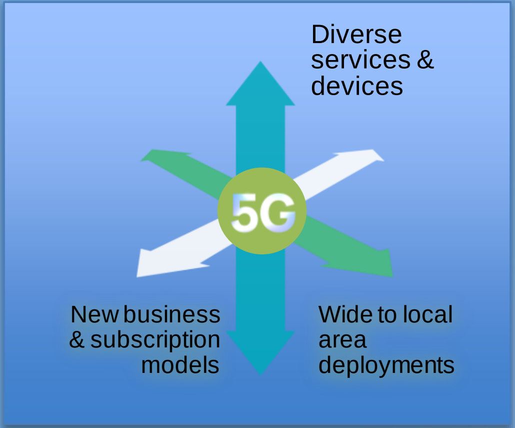
Programmable Networks - Recommendations

Transformation of regulation and policy architectures

A critical re-examination of regimes in reaction to the rapid and ongoing changes in the ICT Industry driven by advances in ‘programmable networks’:

- FCC should form a **cross-organization multi-stakeholder taskforce** focused on creating a **plan of actions** needed to align the architecture of the regulatory/policy framework with emerging developments in technology, use cases, and business model innovations.
- The assessment should be informed by the annual facilitated study exercises (recommended separately), TAC reports, and other multi-stakeholder inputs, and should be re-assessed on a regular basis in the spirit of **continuous adaptation**.

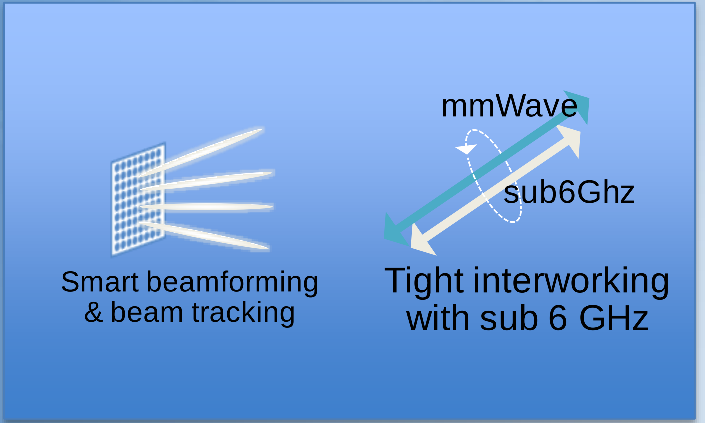
5G


Diverse services & devices

5G

New business & subscription models

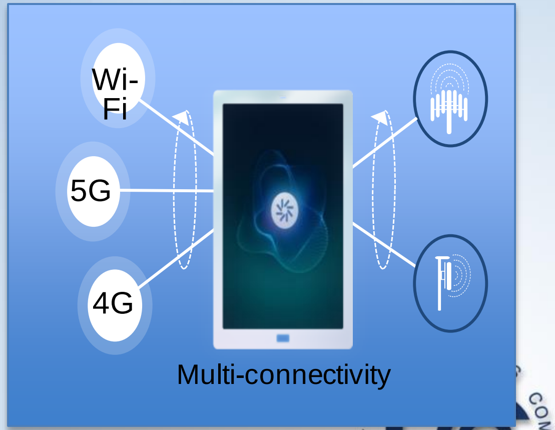
Wide to local area deployments


mmWave

sub6Ghz

Smart beamforming & beam tracking

Tight interworking with sub 6 GHz


Wi-Fi

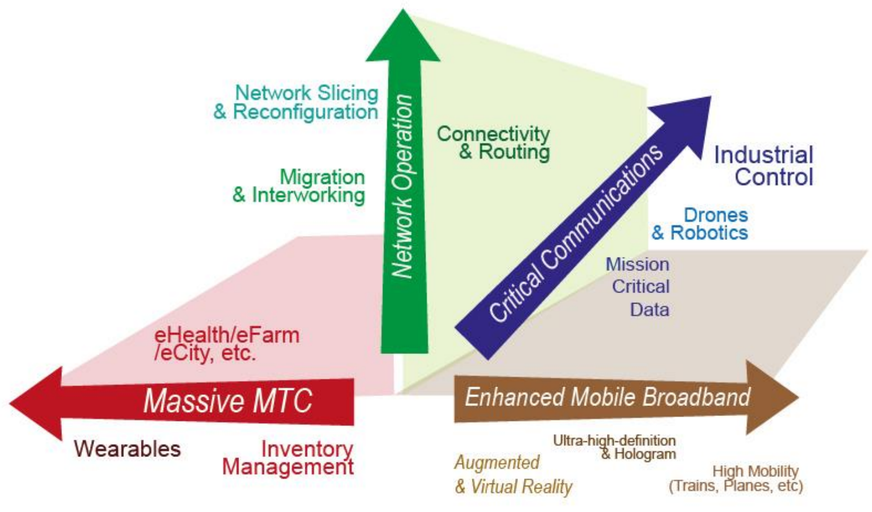
5G

4G

Multi-connectivity

5G Target Use Cases & Goals

5G: New Radio, NG Core, & new RAN architectures (Cloud RAN, Massive MIMO, ...)



Main 5G Use Case Priorities

Target Benefits:

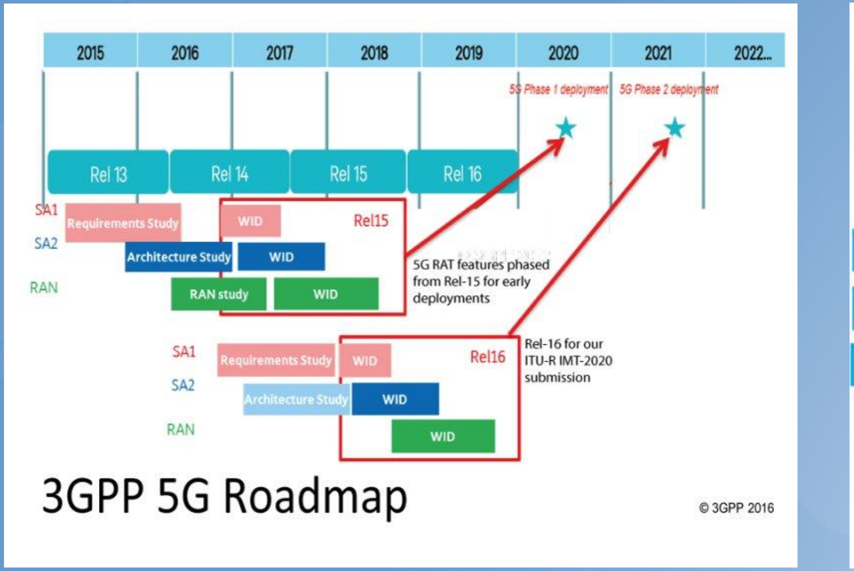
- Maximizing spectral efficiency
- Expanded spectrum (v. high/med/ low, licensed/unlicensed/shared)
- Low end-end latency (1-few ms)
- Ultra reliable & low latency comms
- Network slicing (virtual slices)
- Flexible & automated software-defined control, policy, & mgmt
- Access-agnostic virtualized core
- Optimized performance for diverse devices/applications (thruput, latency, low power/TCO)

Balanced and Best use of Spectrum

- The use of spectrum must be balanced with the consumption needs of urban, sub-urban, and rural settings and at the same time account for physical and environmental constraints.
  - Complementary use of licensed and unlicensed spectrum
  - Exploitation of low, medium, and high frequencies
  - Emphasis on efficiency [more bits/Hz, sharing of spectrum, and reuse through densification]
  - Incentives for non-operators to share infrastructure in low population density areas
  - Long term goal of achieving ubiquity of coverage through use of multiple spectrum bands

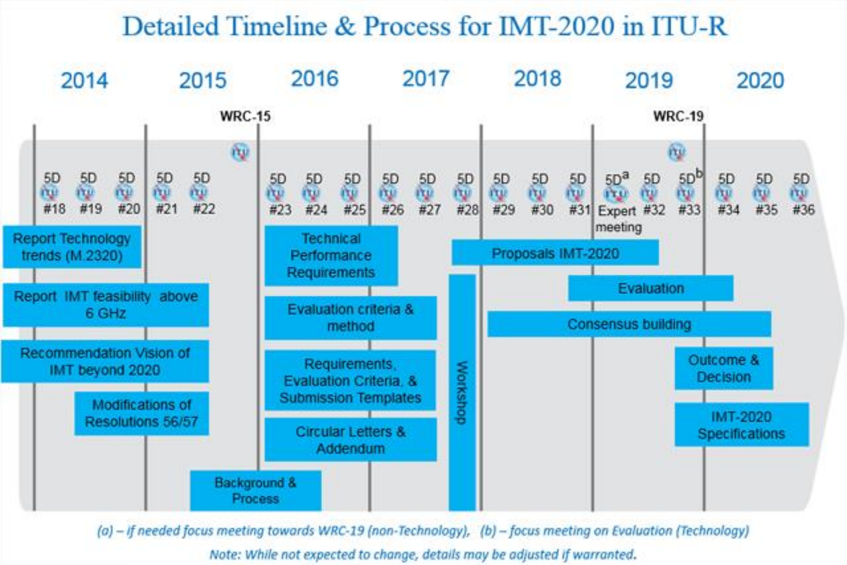
Propagation
Building
Penetration
Weather Conditions
Impact of Foliage
Health and Safety

5G Standardization & Timelines



3GPP 5G Roadmap

© 3GPP 2016


Detailed Timeline & Process for IMT-2020 in ITU-R
2014
2015
2016
2017
2018
2019
2020
WRC-15
WRC-19
5D #18
5D #19
5D #20
5D #21
5D #22
5D #23
5D #24
5D #25
5D #26
5D #27
5D #28
5D #29
5D #30
5D #31
5D[a] Expert meeting
5D #32
5D[b] #33
5D #34
5D #35
5D #36
Report Technology trends (M.2320)
Report IMT feasibility above 6 GHz
Recommendation Vision of IMT beyond 2020
Modifications of Resolutions 56/57
Background & Process
Technical Performance Requirements
Evaluation criteria & method
Requirements, Evaluation Criteria, & Submission Templates
Circular Letters & Addendum
Workshop
Proposals IMT-2020
Evaluation
Consensus building
Outcome & Decision
IMT-2020 Specifications

(a) – if needed focus meeting towards WRC-19 (non-Technology), (b) – focus meeting on Evaluation (Technology)

Note: While not expected to change, details may be adjusted if warranted.

- 3GPP R15 targets early deployments of enhanced mobile broadband by 2020
- pre-standard deployments, especially for fixed wireless broadband, can occur earlier
- 3GPP R16 & ITU-R IMT-2020 process targets more complete 5G deployments by 2021

Challenges to Early/Rapid 5G Deployment

- Magnitude/complexity of standards effort given ambitions of 5G
- Access to spectrum for coverage, penetration, & dense capacity
- Flexibility for efficient best use of multiple spectrum bands and licensing types in combination
- Siting and approvals for infrastructure densification
- Sufficient backhaul for massive capacity & high volume of sites
- Understanding the impact of various novel licensing schemes and impacts on motivating sustained technology investment. [build-out requirements, substantial use, and presumption of renewal rules]
- Flexibility to experiment & innovate to optimize utilization/value

5G - Recommendations [1/2]

Upping the game on the key ingredients for leading in the wireless revolution

Ensure a continued balanced blend in spectrum allocation for best use:

– FCC should work closely with the Administration and Congress to ensure a flow of **spectrum balanced** across high, middle, and low spectrum bands for commercial use, and promote **flexible-use** policies that support experimentation across a range of frequencies and access approaches, including exclusive flexible use licensing, light licensing, sharing, and unlicensed.*

– FCC should conduct a set of studies, with input from industry and other stakeholders, that leads to a **balanced spectrum architecture** and **roadmap** fitting the Nation’s needs into the 21st century.

* included in the ‘2016 TAC Chairman’s Recommendations’

5G - Recommendations [2/2]

Upping the game on the key ingredients for leading in the wireless revolution

Emphasize the importance of spectrum efficiency:

- In future spectrum allocations, the FCC should encourage state of the art **efficient usage for existing services** to free up spectrum, and make available large swaths of contiguous spectrum in single bands to support most efficient use going forward.

Exert leadership in international standards/open source, advocate US interests:

- FCC should establish a '**technology watch list**' (evolving 4G and emerging 5G) of priorities for the US market, and use to guide an ongoing dialogue with industry to ensure they are met in standardization and open source activities.*
- FCC should also **allocate resources** to promote that architecture as part of its **participation** in influential **standards** and **open source** bodies.

* included in the '2016 TAC Chairman's Recommendations'

Anticipating the Future

Innovation for Critical Services

- An increasing fraction of traditional and emerging critical services is exploiting public networks and the new capabilities they represent. The participation of the FCC is crucial in assuring that in the complex negotiations and decisions for Architecting future networks such services are fairly represented.
  - That the FCC develop the full capability to analyze the impacts of decision and negotiations in standards and open source bodies
  - That there is full transparency and ability for stakeholders to impact decisions
  - That the FCC use multi-stakeholder processes to arrive at requirements for such services
  - That the FCC be a strong voice for driving innovation in areas important to societal goals

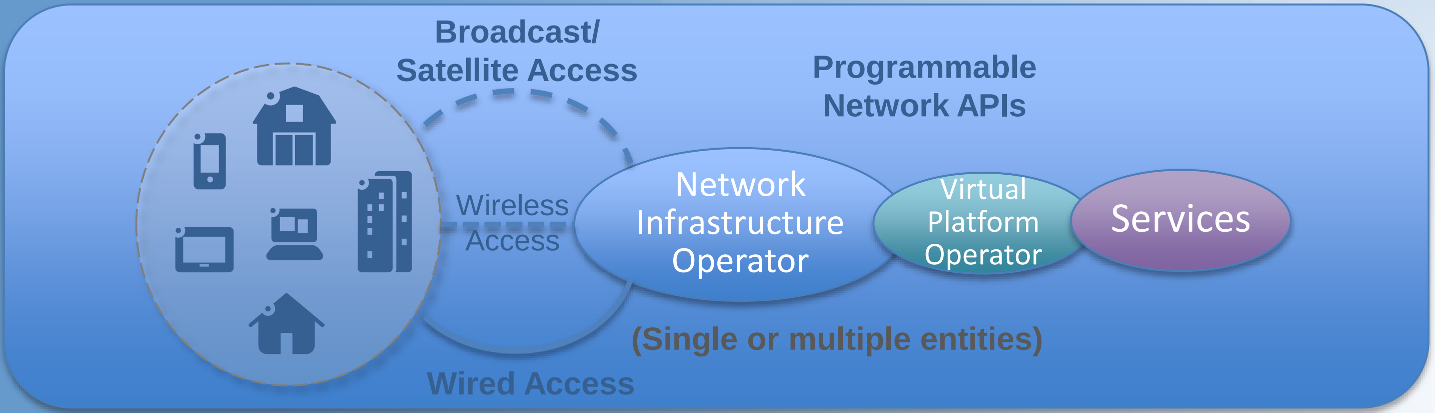
CALEA
Emergency Response
Security/Privacy
Disability Access
IPR Protection …….

Operating in an Era of Continuous Change

- In the past many of the decisions at the FCC to implement successive technologies were discrete events. Today the functionality of almost all services can be offered through multiple technologies. Furthermore the technologies are evolving at a fast and continuous pace. It is a setting in which it is increasingly harder to identify a traditional “operator”, an “equipment vendor”, or “content provider”. The FCC should:
  - Organize its approach to policy and regulation around functionality and not technologies.
  - Re-examine its view and approach to what constitutes competition
  - Conduct a critical review of policies and regulations that are prescriptively tied to specific technologies and may inhibit innovation
  - Develop a consistent approach to incentivize investment where the timescale of innovation is matched to the changes in technology and provides the US the advanced network capabilities that drive economic activity.

Necessity of End-End System Thinking

- The “Networks” being built today are increasingly built on top of common digital technologies – they rely on mash-ups of access and service types. The capabilities of the foundational building blocks are changing rapidly – in terms of technologies, adoption clusters, and approach to business models.
  - Understanding how the “Networks” function requires a unified system view – it is a capability that the FCC needs to develop across its many organizations
  - The FCC should rely on that capability, and that provided by its many constituents, to avoid surprises in impacts to critical services, responsibility for obligations, and the advantage or disadvantage of participants.



Getting Ahead of the Curve

- While the FCC has access to many sources of knowledge and mechanisms for staff development there are several steps that should be take to further strengthen its capabilities. The FCC should:
  - At least annually engage in a facilitated study exercise with outside parties
  - Include a broad range of participants representing, industry, academia, other government entities, and key stakeholders
  - Challenge base plans and beliefs by exposing them to outside experts in technologies and in other industries
  - Identify potential impacts of emerging technologies and innovation for disruptive change in the communications sector
  - Use the results as a foundation to develop plans and strategies to address the anticipated changes
  - With the aid of academia and industry develop consensus plans and roadmaps – playing a positive role in leading the dialog to give the US the most advanced communication systems.

Anticipating the Future - Recommendations

Getting ahead of the curve

Institutionalizing a process at the FCC for anticipating and keeping up with major shifts in technology, usage patterns, and business models:

– FCC should engage in an **annual facilitated study exercise** to gain essential insights on the impact of emerging technologies and innovations for disruptive change in the communications sector. FCC staff, representative of all key Bureaus and Offices, would interact in a **highly focused workshop environment** with experts representing industry, academia and other stakeholders on key forward challenges and opportunities facing the FCC.*

– The results of this exercise should be the foundation for the **development of plans and strategies** to address anticipated change, in support of a robust US digital innovation economy and the furtherance of societal goals.*

* included in the '2016 TAC Chairman's Recommendations'

Topics for 2017 TAC

- Multiplatform Technologies
- Broadband and Mobile Coverage for Rural and Sparsely Populated Areas
- Influence on Governance in SDO and Opens Source Bodies
- Privacy in 5G and Broadband
- Automating Technologies for Enforcement of Interference
- “5G for Dummies” Service Requirements for IoT Devices and Applications
- Public Safety Requirements for Wireless and Broadband Networks - Interoperation between 5G and other Public Safety Infrastructure
- Network Evolution Paths and Alternatives
- Numbering, Naming and Identification of Network and Service Components - Traceability
- The Dark side of Networks
- Local, Regional, and National Peering Regimes for Broadband
- Devices in Distress and End of Life
- Leadership in the management of Radio Spectrum with a focus on important applications such as Public Safety, Healthcare, Education, ...

Thank you!

Next Generation (NG) Internet Service Characteristics & Features Working Group

Chairs:	Russ Gyurek, Cisco John Barnhill, Genband
FCC Liaisons:	Walter Johnston, Scott Jordan, Alec MacDonell, Brian Hurley, Padma Krishnaswamy

Date: December 1, 2016

FEDERAL COMMUNICATIONS COMMISSION USA

2016 Working Group Team Members

- Mark Bayliss, Visualink
- Brian Daly, AT&T
- Adam Drobot, OpenTechWorks
- Andrew Dugan, Level3
- Lisa Guess, Juniper
- Stephen Hayes, Ericsson
- Theresa Hennesy, Comcast
- Brian Markwalter, CTA
- Milo Medin, Google
- Lynn Merrill, NTCA
- Jack Nasielski, Qualcomm
- Ramani Pandurangan, XO
- Mark Richer, ATSC
- Hans-Juergen Schmidtke, FB
- Marvin Sirbu, SGE
- Kevin Sparks, Nokia
- David Tennenhouse, VMware
- David Young, Verizon

Al Morton (AT&T), Michael Browne (Vz), and other Industry SME’s

NG Internet Service Characteristics & Features Charter

Two Areas of Focus: General Improvements and Meaningful Metrics

1. Working across ISPs, the work group will seek to **identify achievable Internet improvements** that could **increase network efficiencies**, **security** or **otherwise improve the Internet ecosystem**;
2. Building on 2015, the work group will consider proposals to **extend data collection efforts**, both in terms of **efficiency** and **scale**, as well as **identifying network points** from which data should be available.
   - The possibility of end-to-end **measurements** will be examined together with the potential impact of **differentiated E2E QOS,** leveraging **alternative sources** of data (e.g. crowd sourcing), and **examining broadband bottlenecks** and **breakpoints**.

Team Agenda 2016 – 3Q Focus Areas

- Measuring QoS- BIAS

  - *Actionable recommendation to conclude this work*

- E2E QoS

  - *Continued work from 2015: “Fork in the Road”*

- Internet improvements and efficiencies

  - *New topic for WG in 2016*

Interviews and Guest Speakers

National Science Foundation

DASH Industry Forum

at&t

5G

broadband forum

Consumer Technology Association™

hulu

ITU-T Study Group 12

verizon✓

COMCAST

Akamai

CONVIVA®

Carnegie Mellon

facebook.

Academic Researchers

Interviews and Presentations

- Findings
  - Video continues as dominant trend driving growth and investment.
  - Market-based Solutions are emerging to deliver improved experience for Video
  - Instrumented clients generate data to allow content providers to improve the QoE provided to their users
  - Changes in media formatting will lead to fewer versions of files and reduce network bandwidth demand

INTERNET IMPROVEMENTS AND EFFICIENCIES

Interviews and Guest Speakers

NATIONAL SCIENCE FOUNDATION
5G
DASH Industry Forum
hulu
facebook
at&t
COMCAST
Akamai
CONVIVA
Carnegie Mellon
verizon

Academic Researchers

Interviews and Presentations

- Findings
- Significant Work being done to define the Future of the Internet
  - Evolving core and access to keep pace with demand
  - Near term focus on access speed and content delivery efficiencies
  - Content and Coding mechanisms evolving to more efficiently support traffic
- National Science Foundation Grants
  - Multiple streams of research currently being conducted (SDN, ICN, NFV, OS, Coding techniques, etc)
  - 5G will be a key driver for the Next Gen Internet core

Issues with the Current Internet

- IP addresses used as both locators and identifiers
  - Why mobility is difficult
- No security support built into the IP network
- Hostile to ad hoc, DTN (delay tolerant networks), peer-to-peer, intermittency
- New usage models added complexity and overhead
  - Content & service networking require a level of indirection
- Many work-arounds and patches (CDN, middleboxes, etc.)
- Adding functionality in the network is difficult
  - (Multicast, intserv, diffserv, IPv6. also: explicit congestion, etc.)

Source: Darlene Fisher, National Science Foundation

Observations on NG Internet Improvements and Efficiencies

- Key evolution Concepts: All include intrinsic security
  - Designed for Mobility First
  - Named Data Networking
  - eXpressive Internet Architecture (XIA)
- Industry Bodies –work being done by : ATIS, NSF – Multiple academic institutions
- Seeking Input from collective TAC on areas to investigate and priorities
- 5G, IoT and virtualization will drive the network evolution

Mobility First: Key Components

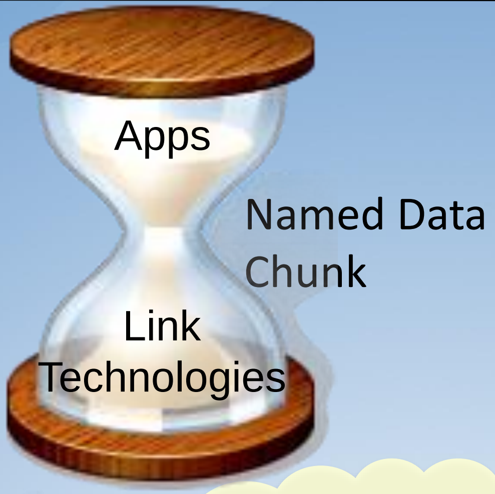
- Global name service (GNS)—logically centralized service responsible for naming, security, network functionality
  - Clean separation of identity and location of endpoints
- Globally unique identifier (GUID) identifies interfaces, content, services, human end-user device or group of devices, etc.
  - Flat identifiers are location-independent and cryptographically verifiable (an approach is a one-way hash of a public key)
- Global name service (GNS) resolves a GUID to its current network address (a self-certifying identifier for a network like an AS today).

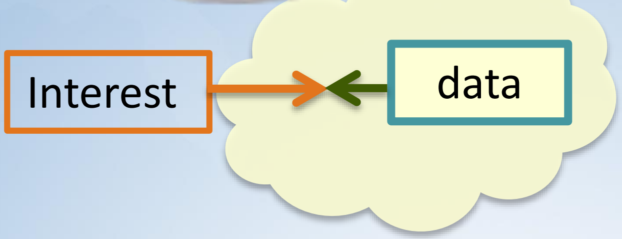
Source: Darlene Fisher, National Science Foundation

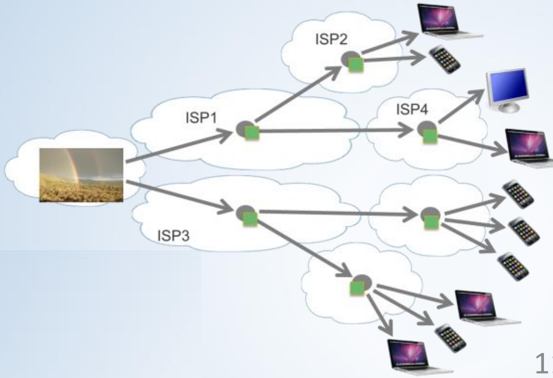
Named Data Networking: Key Features

NDN directly focuses on the outcome: retrieving data

- Names the data not the hosts with hierarchical names
- The narrow waist is named data chunks not IP
- Content producers name and advertise data
- Users issue “Interests” to ask the network for content by name. Interests are stored along path to where data is located.
- Network returns content from cached data (or if necessary from the producer) along the same return path as the interest traveled and is delivered to all users along the path who issued interests for the data







Source: Darlene Fisher, National Science Foundation

XIA: Three Simple Ideas

- Support multiple types of destinations
  - Not only hosts, but also content, services, etc.
  - Not having to force communication at a lower level (e.g., hosts) reduces complexity and overhead
- Flexible addressing gives network more options for successfully completing communication operations
  - Include both “intent” and “fallback” address support
  - Supports evolvability, network diversity, fault recovery, mobility, ..
- Intrinsic security guarantees security properties as a direct result of the design of the system
  - Do not rely on external configurations, data bases, ..

When do we expect to see change?

Next 5 Years

- Initial 5G Deployments
- SDN/NFV
- MPEG/DASH
- Network evolution:
  - compute resources moving to the edge
  - Cloud based solutions
  - Video, AR/VR
  - IoT: Expanded use cases & support
- Security evolution & improvements required

5 Years +

- XIA
  - ICN –
- Evolution to next gen 5G network – full 5G roll-outs
  - Next Gen Core
- Data driven network mngt services
  - Cognitive networks: ML/AI, etc

QUALITY OF SERVICE, QUALITY OF EXPERIENCE

Next Gen Internet – *The End-to-End QoS Fork in the Road*

Undifferentiated Internet

Current Internet, massively scaled

- Ever higher BW applications enabled
- QoE still not predictable

Differentiated Internet

Paid QoS Internet

- For subset of traffic only
- Predictable QoE for wider range of uses

Unpaid QoS Internet

- Who gets differentiation?

Best Effort

Transactional

Summary of Inputs – Interconnection Health and QoS

Commission Action
- Existing MBA

Academic Research
- Nick Feamster presentation/paper
- Clark and Claffy paper

Public Reports
- Netflix speed index
- Google Video Quality Report

Standards
- ITU-T Study Group 12 (QoS & QoE)
- CTA work on QoE
- IETF Work on QoS
- Dash - IF QoE Factors

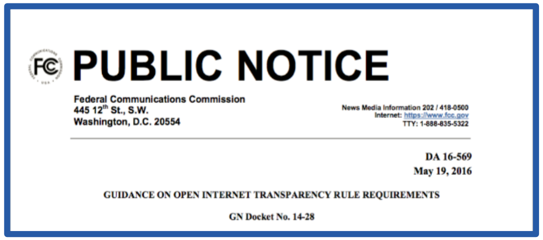
Industry
- Input from Comcast
- Input from Conviva
- Input from Hulu

- Conclusion: There isn't an easy solution to assessing interconnection health or the CDN performance
- Authority: Commission has asserted authority over interconnection (with respect to BIAS) and could benefit from more data in this area

Quality Metrics - QoS

Commission Driven Metrics

Open Internet Transparency Guidance



PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

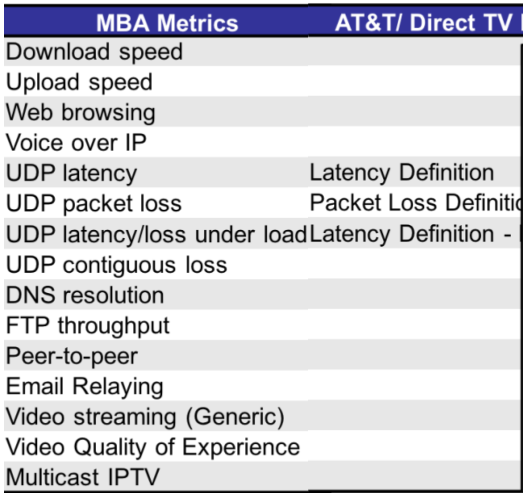
News Media Information 202 / 418-0500
Internet: https://www.fcc.gov
TTY: 1-888-835-5322

DA 16-569
May 19, 2016

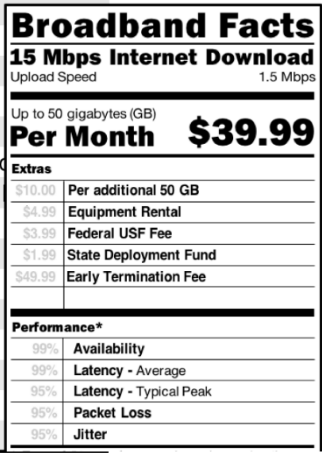
GUIDANCE ON OPEN INTERNET TRANSPARENCY RULE REQUIREMENTS

GN Docket No. 14-28

DA 16-569
May 19, 2016



MBA Metrics	AT&T/ Direct TV Merger
Download speed	
Upload speed	
Web browsing	
Voice over IP	
UDP latency	Latency Definition
UDP packet loss	Packet Loss Definiti
UDP latency/loss under load	Latency Definition -
UDP contiguous loss	
DNS resolution	
FTP throughput	
Peer-to-peer	
Email Relaying	
Video streaming (Generic)	
Video Quality of Experience	
Multicast IPTV	



Broadband Facts

15 Mbps Internet Download

Upload Speed 1.5 Mbps

Up to 50 gigabytes (GB)
Per Month $39.99

Extras	
$10.00	Per additional 50 GB
$4.99	Equipment Rental
$3.99	Federal USF Fee
$1.99	State Deployment Fund
$49.99	Early Termination Fee

Performance*	
99%	Availability
99%	Latency - Average
95%	Latency - Typical Peak
95%	Packet Loss
95%	Jitter

Standards Driven Metrics

ITU

IETF

BITAG
Broadband Internet Technical Advisory Group

atis

3GPP
A GLOBAL INITIATIVE

ETSI

ANSI

Private Initiatives

Various Parties Developing Instrumented Clients

Infrastructure focus, Human Factors Needs More Work

Recommendation: QoS/QoE

- Expand MBA program to add additional QoS and QoE measurements
  - Expand testing to include CDN performance
  - Expand testing to include Interconnection health

- QoE:
  - The commission should closely monitor work being done in standards bodies regarding Quality of Experience, particularly work done in ITU-T SG12 and IETF
  - Ultimately, QoE depends on end-user experience. The commission should seek a public/ private partnership to determine actual consumer experience.
  - Public/Private partnership to perform a QoE consumer survey (neutral)

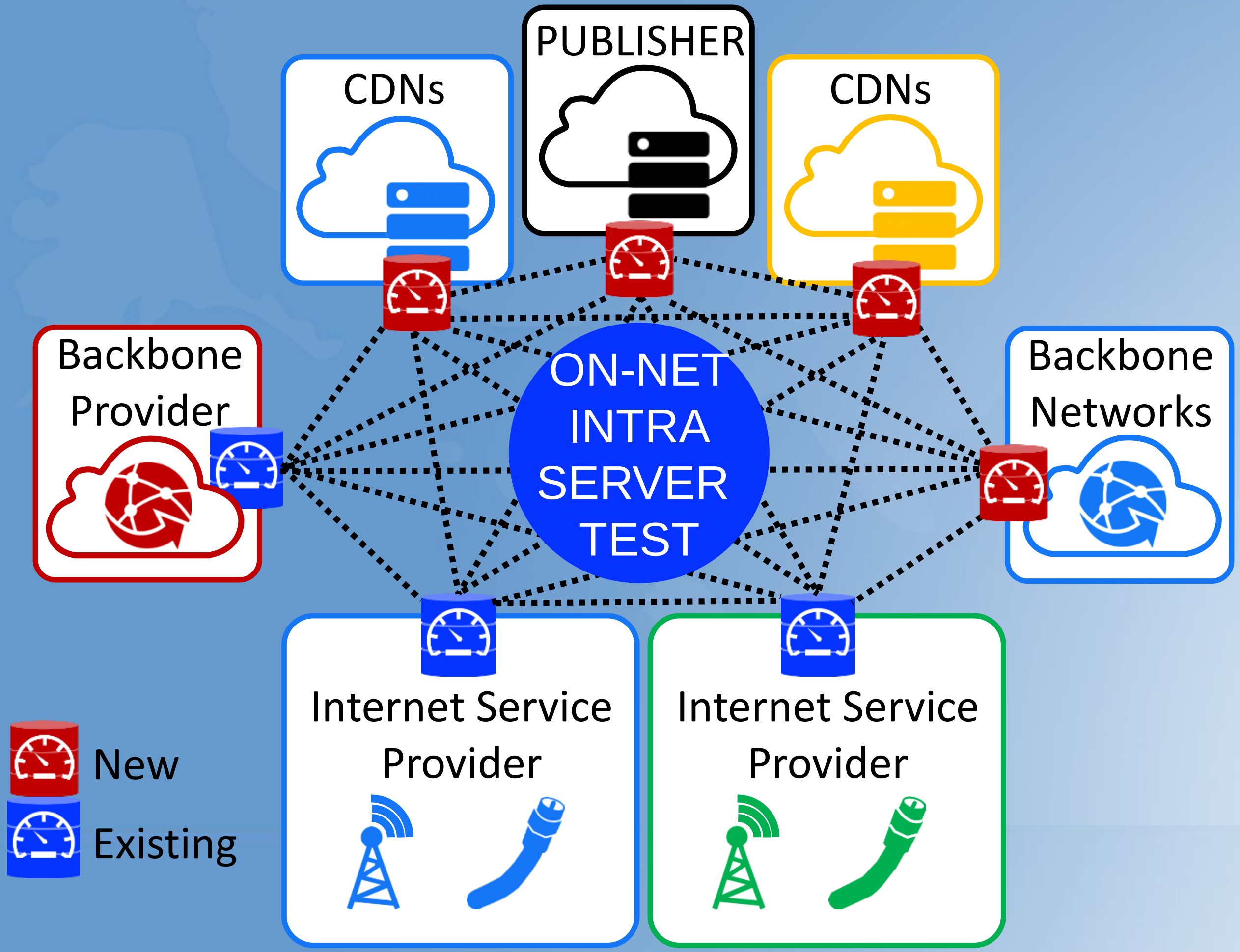
Recommendation: Additional Network testing to Understand End-to-End QoS

- As the commission seeks to understand the end-to-end performance of the network, collection of additional performance data is required to characterize end-to-end Quality of Service.
  - Example: congestion at network interconnection points has been shown to be a key factor in end-to-end Quality of Service.
- The MBA program should be expanded to inform the commission on the measurement of QoS Data across interconnection points.
  - It may be useful to enhance on-net MBA servers to support active measurements
- Third party experts should be engaged to develop a program of QoS data collection and related analytics
  - Incorporate industry data sources on CDN performance and interconnection health.

Measurement Recommendations – MBA Expansion

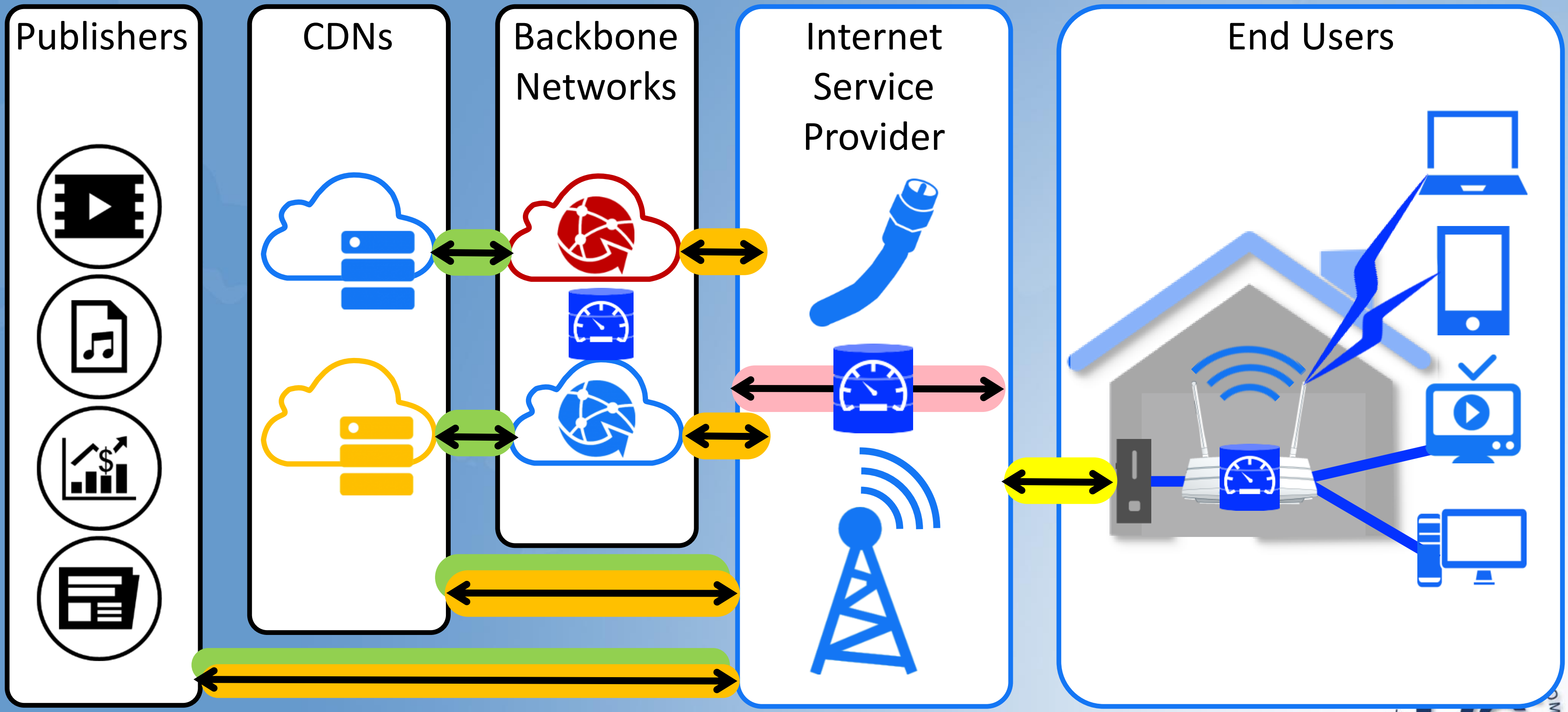
- Expand/Substitute for existing active measurement set to cover fundamentals
  - Permit light-load testing during Consumer busy-hours with concurrent user traffic
    - (because long-session duration users mean no idle time during busy hours)
  - DNS Response time and Reachability/Reliability
  - Continuous tests to support availability measurements
- Measurement Architecture Evolution: Responder at Premise Service Demarc.
  - Reduced complexity – embed measurement responder into customer gateway (CPE)
  - Tie-in with Home Network Recommendations: ability to act as a responder for Home network measurements (facing consumer/WiFi network, Client is User device).
- Measurement Architecture Evolution: Measure between MBA ISP Servers
  - Characterize other path segments (sub-e2e paths)
  - Possibly more Host Servers at strategic interconnection points
- Specific evolutionary recommendations solicited from third-party experts and publicly discussed
- Consider including data collection from non-traditional data sources

Enhance On-Net MBA Servers to Support Active Measurements



- Overcomes one-way data visibility
- Tests are guaranteed to cross an I/C point.
- Server pairs could be selected to (try to) exclude multiple I/C points in tandem on test path.
- On-net Servers geographically close to I/C points are preferred.
- Advanced traceroute measurements will help identify the tested path (Tools: *Paris-Tracert and/or fbtracert*)
- On-net servers need to be enhanced to initiate active measurements.
- Measurements should include Loss and Delay, possibly “available rate” measurements.

Expand MBA program to reflect granular QoS performance



Publishers

CDNs

Backbone Networks

Internet Service Provider

End Users

🟩 CDN Performance

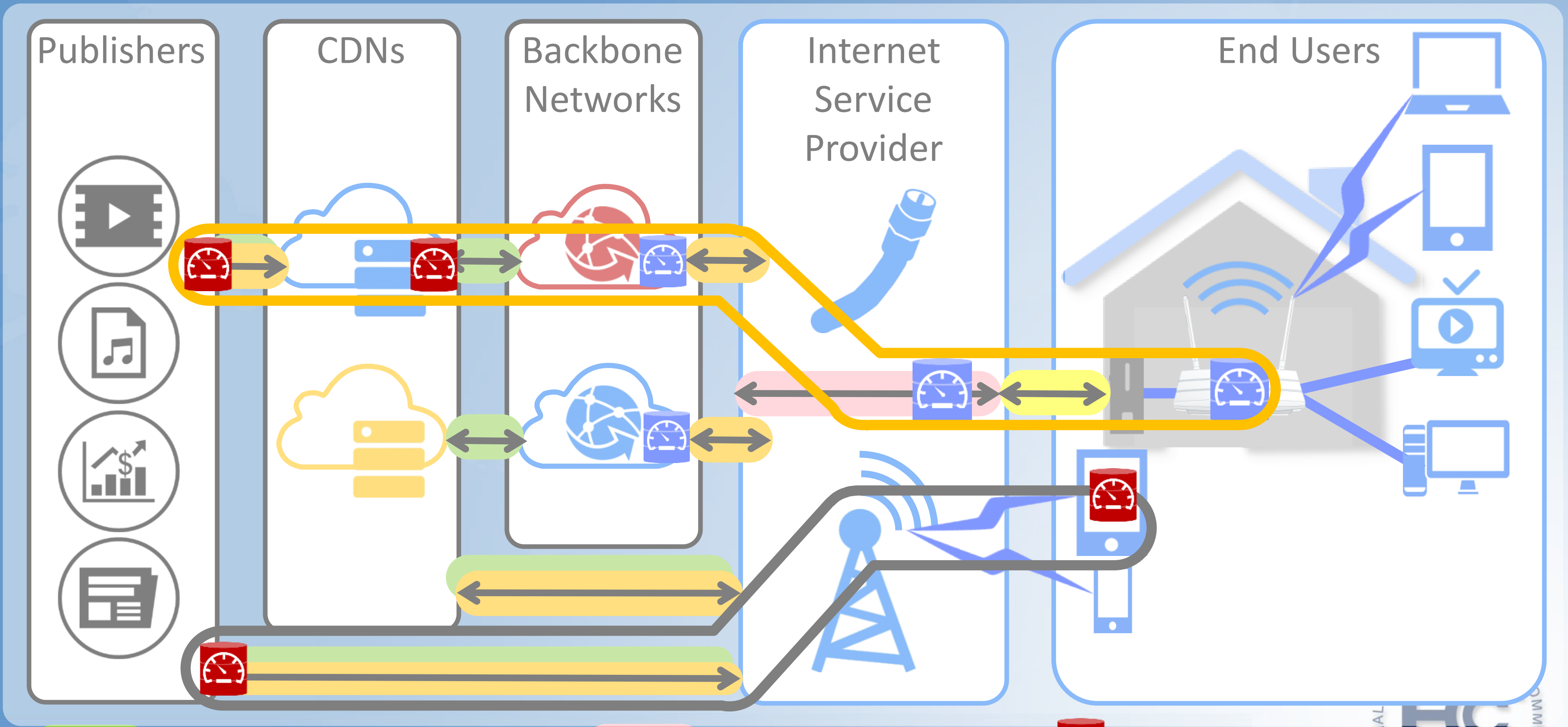
🟧 Interconnection Health

🟥 BIAS Cloud

🟨 BIAS Last Mile

Existing MBA

Expand MBA program to reflect granular QoS performance



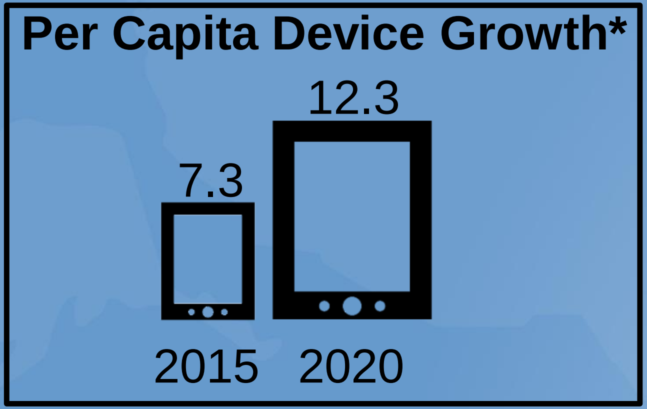
🟩 CDN Performance
🟧 Interconnection Health
🟥 BIAS Cloud
🟨 BIAS Last Mile
🟥 Expanded MBA
🟦 Existing MBA

IN-HOME NETWORKS

In-Home Sub-WG- Summer Activity

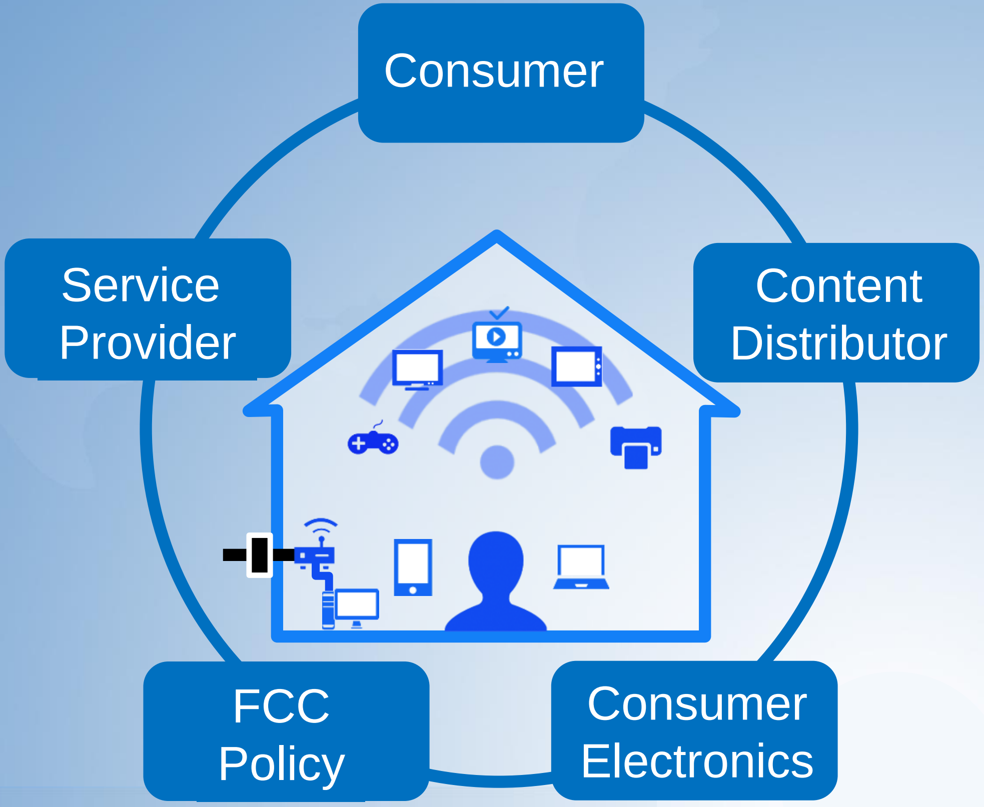
- CTA Collaboration:
  - Performance measurements are of interest to consumer device manufacturers
- 3rd Party Data Collectors: Hulu, Akamai, Conviva
  - Potential for the FCC to leverage data for in-home QoS/QoE
  - A clear interest to content providers
- BBF Collaboration:
  - Explored standards work into TR69 (including TR 304)
- Comcast, AT&T, Verizon:
  - Interest in reduced truck rolls/trouble tickets
- ATIS:
  - Growing interest and focus on in-home performance

The Impact of the In-Home Network on QoS/QoE



Importance of In-Home Networks

- Quality of User Experience
- Consumer device performance - Industry Interest
- Remote trouble-shooting
- Remote Management
- Diagnose device misconfiguration
- Bandwidth use/trends for policy decisions



Consumer

Service Provider

Content Distributor

FCC Policy

Consumer Electronics

* Source: Cisco VNI

Rational for In-Home QoS/QoE Measurements

- Why In-Home Measurements are needed
  - In Home is the only portion of the network where there are no industry standardized measurements that are made available to consumers, providers or content owners
  - Ability to Identify under-performing equipment to improve in-home experiences
  - Develop base line and establish methods to measure E2E services performance

- What is the anticipated outcome
  - Develop a standardized broadband measurement system available for the consumer, industry and FCC to understand QoS/QoE within the home
  - Provide a means for consumers to measure, test and initiate problem solving techniques by themselves or through the broadband service provider
  - Reduced trouble tickets for providers, content owners
  - Align performance objectives to network services and home environments

Recommendation: Public Notice on In-Home Network

- FCC to issue a Public Notice on in-home networks and their contribution to overall Quality of Service/ Experience

Recommendation: Public Notice – In-Home Networks

- Initiate information solicitation seeking to better characterize current capabilities and evolution of broadband home networks.
- Identify stakeholders and potential 3rd party data sources on in-home networking performance
- Seek stakeholder perspective regarding initiatives to improve knowledge of home networking environment and help establish performance goals
- Gain information on impact of home network performance on end/end services and applications
- Seek input on critical factors affecting in-home broadband performance
- Solicit suggestions for incorporation of 3rd party data sets into FCC reporting and identify potential issues derivative from using such data
- Solicit ideas/suggestions on trackable metrics that would best inform on status and changing home environment
- Solicit suggestions to improve home networking environment increasing its utility for both the consumer, (and) service providers, content owner, and equipment vendors
- Seek to identify industry collaborative relationships and synergies that would contribute to QoE home networking goals

THANK YOU!

BACK-UP MATERIAL

Links to Research, Reports, References

- KC Claffy, David Clark et al. “Policy challenges in mapping Internet interdomain congestion.” https://www.caida.org/publications/papers/2016/policy_challenges_mapping_internet/policy_challenges_mapping_internet.pdf
- DASH-IF position Paper: Proposed QoE Media Metrics standardization for segmented media playback. http://dashif.org/wp-content/uploads/2016/10/ProposedMediaMetricsforSegmentedMediaDelivery-r12.pdf
- Google Video Quality Report, 2016. https://www.google.com/get/videoqualityreport/
- Nick Feamster. “Revealing Utilization at Internet Interconnection Points.” http://interconnection.citp.princeton.edu/wp-content/uploads/2016/04/1603.03656v1_IMP-Working-Paper.pdf
- ITU-T Study Group 12: Performance, QoS and QoE. http://www.itu.int/en/ITU-T/studygroups/2013-2016/12/Pages/default.aspx
- Measuring Broadband America. Federal Communications Commission. https://www.fcc.gov/general/measuring-broadband-america
- Measurement Lab. http://ww.wmeasurementlab.net
- Netflix ISP Speed Index. https://ispspeedindex.netflix.com/country/us/
- TR-069 CPE WAN Management Protocol https://www.broadband-forum.org/standards-and-software/technical-specifications/technical-reports
- TR-304 Broadband Access Service Attributes and Performance Metrics https://www.broadband-forum.org/technical/download/TR-304.pdf

Technological Advisory Council

Spectrum and Receiver Performance

Working Group

December 7, 2016

Spectrum and Receiver Performance Working Group

- **Chairs:**
  - Lynn Claudy, NAB
  - Greg Lapin, ARRL
- **FCC Liaisons:**
  - Julius Knapp
  - Robert Pavlak
  - Matthew Hussey
  - Ziad Sleem

- **Participants / Contributors:**
  - Pierre de Vries, Silicon Flatirons
  - Dale Hatfield, University of Colorado
  - Brian Markwalter, CTA
  - Geoff Mendenhall, GatesAir
  - Dennis Roberson, IIT
  - Robert Dalgleish, Ericsson
  - David Gurney, Motorola Solutions
  - Bruce Judson, Qualcomm

Meeting Presentation Topics

- – Actionable Recommendations
  - Noise Floor
  - Interference Resolution and Spectrum Management
  - Enforcement
- – Report on Noise Floor Technical Inquiry

Actionable Recommendations

– Three topics for actionable recommendations are based on our evolving work over the past three years:

- Noise Floor recommendations are based on the replies to our Technical Inquiry, ET Docket 16-191.
- Interference Resolution and Spectrum Planning recommendations are based on the evolution of Harm Claim Thresholds, Risk Informed Assessment and Basic Principles for Compatibility of Spectrum Allocation
- Enforcement using the Next Generation Architecture for Interference Resolution and a database of radio-related enforcement activities with the inclusion of interference hunters.

Noise Floor Action Recommendations

Take actions on noise sources, based on responses submitted to the TAC Technical Inquiry, ET Docket 16-191, as well as interviews with professional interference hunters and related sources. The Technical Inquiry received 108 filings with opinions from nearly all segments of the communications industry. Additionally, we discussed the experience of locating noise sources with professional noise hunters. While there was variation in the responses to many of the topics, there were certain issues that were agreed upon with near unanimity. For those items, we recommend that the FCC take the following actions:

Noise Floor Action Recommendations (cont)

- Direct the OET Lab to make measurements of advanced lighting and switching power supplies currently on the market to ascertain if they meet regulatory radiated and conducted emissions limits, and initiate enforcement actions if required.
- Issue NOI / NPRMs to gain more information about the advisability of rule changes to cope with 1) advanced lighting and switching power supply-type devices, 2) noise generation below 30 MHz, 3) devices that are excluded from mandatory emission testing, 4) the aggregation of noise from groups of compliant devices, 5) the current applicability of Class A vs. Class B emissions limits, 6) differences between Part 15 and Part 18 emissions limitations, and 7) requiring an FCC label on every device that has been tested and confirmed to meet emission limits.

Spectrum Management Recommendations

- Initiate a Policy Statement, voted on by the Commission, setting forth spectrum management guidance based on TAC recommendations made to the FCC.
  - Implement receiver recommendations and spectrum allocation principles as described in the December 2015 TAC paper and formalize them into allocation policies; set clear expectations about the affected system's capabilities regarding interference, such as harm claim thresholds.
  - Pursue adoption of risk-informed interference assessment and adopt statistical service rules more widely in order to support risk analysis.

Spectrum Management References

(all papers can be found at https://transition.fcc.gov/bureaus/oet/tac/tacdocs)

- See March 2014 TAC paper, “Interference Limits Policy and Harm Claim Thresholds: An Introduction”, TACInterferenceLimitsIntrov1.0.pdf; see especially *Section 5, Developing harm claim threshold values*.
- April 2015 TAC paper, “A Quick Introduction to Risk-Informed Interference Assessment”, Intro-to-RIA-v100.pdf; see especially *Section 5, Recommended FCC Action*
- Dec 2015 TAC paper, “A Case Study of Risk-Informed Interference Assessment: MetSat/LTE Co-existence in 1695–1710 MHz”, MetSat-LTE-v100-TAC-risk-assessment.pdf; see especially *Section 8, Conclusions and recommendations*, and the *Executive Summary*.
- December 2015 paper “Basic Principles for Assessing Compatibility of New Spectrum Allocations”, Principles-White-Paper-Release-1.1.pdf

Enforcement Recommendations

- Commission a study to develop the next generation systems architecture for radio spectrum enforcement and interference resolution
- Create a comprehensive and unified publicly available database of past radio-related enforcement activities
- Incorporate the use of interference hunters in the interference enforcement process.

Enforcement References

- March 2016 paper, “A Study to Develop the Next Generation Systems Architecture for Radio Spectrum Interference Resolution”, https://transition.fcc.gov/oet/tac/tacdocs/reports/2016/A-Study-to-Develop-a-Next-Generation-System-Architecture-V1.0.pdf
- June 2014 paper, “Introduction to Interference Resolution, Enforcement and Radio Noise”, https://transition.fcc.gov/bureaus/oet/tac /tacdocs/meeting61014/ InterferenceResolution-Enforcement-Radio-Noise-White-Paper.pdf; see especially *Section V, Potential New Strategies or Approaches for Addressing Enforcement Challenges*

Emerging Enforcement Concerns

- Software Defined Radio and Software Controlled Radio
  - Many types of publicly available radio communications equipment can be “opened up” to non-authorized users by simple software or hardware changes to spectrum segments used by public safety, air traffic control, and other life support communications
  - False radio messages can be generated to appear as if they were coming from legitimate sources, a technique known as spoofing
  - The FCC needs to develop a strategy to protect these services from spoofing

FEDERAL COMMUNICATIONS COMMISSION
FCC
USA

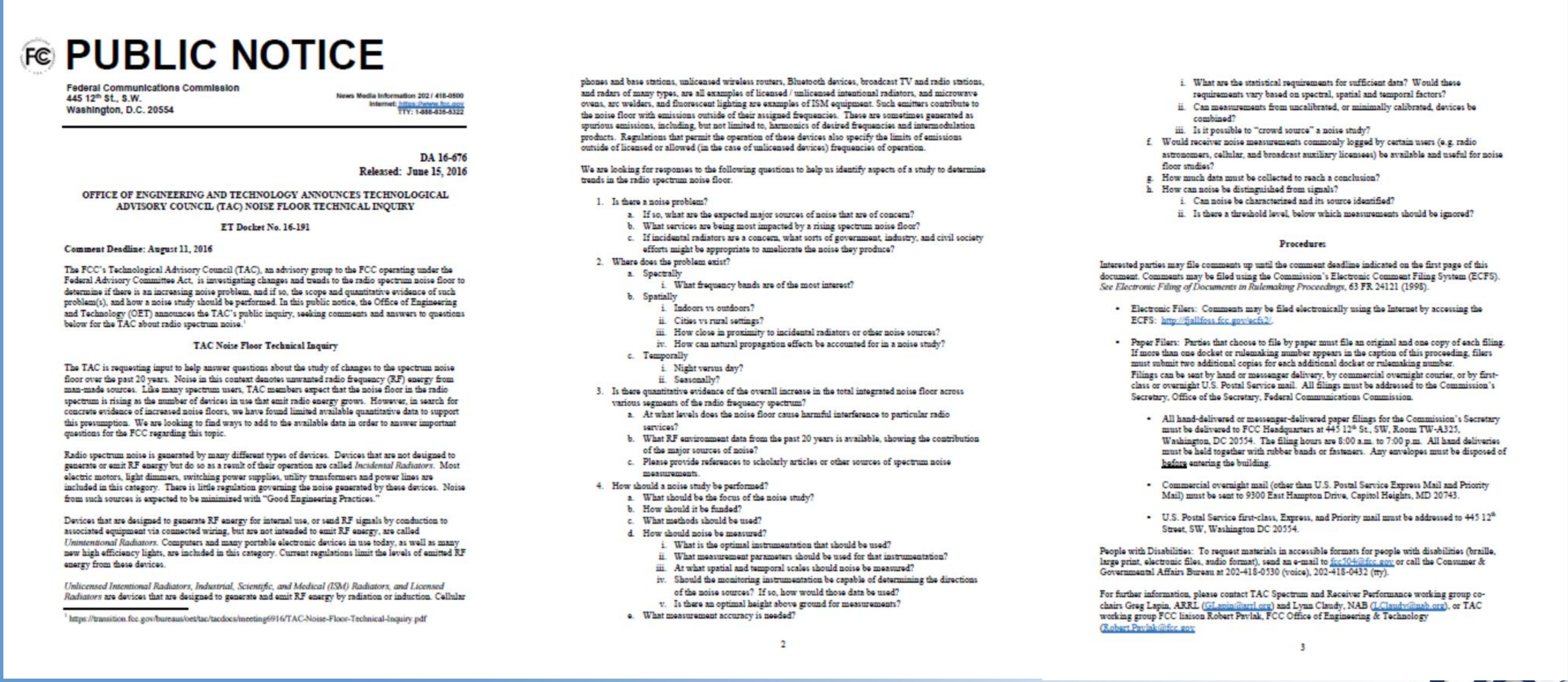
Emerging Enforcement Concerns (cont)

- GPS
  - GPS has become more vulnerable as new technology makes “Jamming” and “Spoofing” more accessible to criminal activities
  - GPS signals can be jammed; obliterated by stronger signals.
  - GPS signals can be spoofed without warning to make the position appear to be different than the actual position
  - The FCC enforcement bureau needs to develop a strategy to protect GPS services

Emerging Enforcement Concerns (cont)

- Noise
  - There is evidence that devices may be marked as “FCC compliant” which were never tested or were cost reduced after they were tested making them “non-compliant”
  - The FCC enforcement bureau needs to develop a strategy to stop the manufacture and importation of non-compliant switching power supply “Wall Warts” , LED lights, and CFL lights that do not meet current regulations
  - Enforcement of current FCC limits is urgently needed to curtail the rapid increase in the noise floor across all spectral segments before it becomes completely unmanageable

Technical Inquiry ET16-191



PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

News Media Information 202 / 418-0500
Internet: https://www.fcc.gov
TTY: 1-888-835-5322

DA 16-676
Released: June 15, 2016

OFFICE OF ENGINEERING AND TECHNOLOGY ANNOUNCES TECHNOLOGICAL ADVISORY COUNCIL (TAC) NOISE FLOOR TECHNICAL INQUIRY

ET Docket No. 16-191

Comment Deadline: August 11, 2016

The FCC's Technological Advisory Council (TAC), an advisory group to the FCC operating under the Federal Advisory Committee Act, is investigating changes and trends to the radio spectrum noise floor to determine if there is an increasing noise problem, and if so, the scope and quantitative evidence of such problem(s), and how a noise study should be performed. In this public notice, the Office of Engineering and Technology (OET) announces the TAC's public inquiry, seeking comments and answers to questions below for the TAC about radio spectrum noise.[1]

TAC Noise Floor Technical Inquiry

The TAC is requesting input to help answer questions about the study of changes to the spectrum noise floor over the past 20 years. Noise in this context denotes unwanted radio frequency (RF) energy from man-made sources. Like many spectrum users, TAC members expect that the noise floor in the radio spectrum is rising as the number of devices in use that emit radio energy grows. However, in search for concrete evidence of increased noise floors, we have found limited available quantitative data to support this presumption. We are looking to find ways to add to the available data in order to answer important questions for the FCC regarding this topic.

Radio spectrum noise is generated by many different types of devices. Devices that are not designed to generate or emit RF energy but do so as a result of their operation are called *Incidental Radiators*. Most electric motors, light dimmers, switching power supplies, utility transformers and power lines are included in this category. There is little regulation governing the noise generated by these devices. Noise from such sources is expected to be minimized with "Good Engineering Practices."

Devices that are designed to generate RF energy for internal use, or send RF signals by conduction to associated equipment via connected wiring, but are not intended to emit RF energy, are called *Unintentional Radiators*. Computers and many portable electronic devices in use today, as well as many new high efficiency lights, are included in this category. Current regulations limit the levels of emitted RF energy from these devices.

Unlicensed Intentional Radiators, Industrial, Scientific, and Medical (ISM) Radiators, and Licensed Radiators are devices that are designed to generate and emit RF energy by radiation or induction. Cellular phones and base stations, unlicensed wireless routers, Bluetooth devices, broadcast TV and radio stations, and radars of many types, are all examples of licensed / unlicensed intentional radiators, and microwave ovens, arc welders, and fluorescent lighting are examples of ISM equipment. Such emitters contribute to the noise floor with emissions outside of their assigned frequencies. These are sometimes generated as spurious emissions, including, but not limited to, harmonics of desired frequencies and intermodulation products. Regulations that permit the operation of these devices also specify the limits of emissions outside of licensed or allowed (in the case of unlicensed devices) frequencies of operation.

[1] https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting6916/TAC-Noise-Floor-Technical-Inquiry.pdf

We are looking for responses to the following questions to help us identify aspects of a study to determine trends in the radio spectrum noise floor.

1. Is there a noise problem?
   a. If so, what are the expected major sources of noise that are of concern?
   b. What services are being most impacted by a rising spectrum noise floor?
   c. If incidental radiators are a concern, what sorts of government, industry, and civil society efforts might be appropriate to ameliorate the noise they produce?
2. Where does the problem exist?
   a. Spectrally
      i. What frequency bands are of the most interest?
   b. Spatially
      i. Indoors vs outdoors?
      ii. Cities vs rural settings?
      iii. How close in proximity to incidental radiators or other noise sources?
      iv. How can natural propagation effects be accounted for in a noise study?
   c. Temporally
      i. Night versus day?
      ii. Seasonally?
3. Is there quantitative evidence of the overall increase in the total integrated noise floor across various segments of the radio frequency spectrum?
   a. At what levels does the noise floor cause harmful interference to particular radio services?
   b. What RF environment data from the past 20 years is available, showing the contribution of the major sources of noise?
   c. Please provide references to scholarly articles or other sources of spectrum noise measurements.
4. How should a noise study be performed?
   a. What should be the focus of the noise study?
   b. How should it be funded?
   c. What methods should be used?
   d. How should noise be measured?
      i. What is the optimal instrumentation that should be used?
      ii. What measurement parameters should be used for that instrumentation?
      iii. At what spatial and temporal scales should noise be measured?
      iv. Should the monitoring instrumentation be capable of determining the directions of the noise sources? If so, how would those data be used?
      v. Is there an optimal height above ground for measurements?
   e. What measurement accuracy is needed?
      i. What are the statistical requirements for sufficient data? Would these requirements vary based on spectral, spatial and temporal factors?
      ii. Can measurements from uncalibrated, or minimally calibrated, devices be combined?
      iii. Is it possible to "crowd source" a noise study?
   f. Would receiver noise measurements commonly logged by certain users (e.g. radio astronomers, cellular, and broadcast auxiliary licensees) be available and useful for noise floor studies?
   g. How much data must be collected to reach a conclusion?
   h. How can noise be distinguished from signals?
      i. Can noise be characterized and its source identified?
      ii. Is there a threshold level, below which measurements should be ignored?

Procedures

Interested parties may file comments up until the comment deadline indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: http://fjallfoss.fcc.gov/ecfs2/.

- Paper Filers: Parties that choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.
  Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

  - All hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes must be disposed of before entering the building.

  - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

  - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington DC 20554.

People with Disabilities: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

For further information, please contact TAC Spectrum and Receiver Performance working group co-chairs Greg Lapin, ARRL (GLapin@arrl.org) and Lynn Claudy, NAB (LClaudy@nab.org), or TAC working group FCC liaison Robert Pavlak, FCC Office of Engineering & Technology (Robert.Pavlak@fcc.gov

Technical Inquiry Responses

- Responses were received from 83 different people/entities.
  - 100 submissions to ECFS, including some duplicates
  - 8 direct submissions to the committee by email are not in ECFS
- The breakdown on responders (with some overlap between groups):
  - 24 Companies/Industry Organizations.
  - 39 RF Professionals.
  - 31 Licensed Radio Amateurs.
  - 2 University Researchers
  - *9 Responders did not reply to the questions asked.*

Responding Entities

- NAB (Broadcast)
- SBE (Broadcast)
- DTS Inc (Broadcast)
- Wisconsin Public Radio (Broadcast)
- V-Soft (Broadcast)
- Cohen, Dippell & Everest (Broadcast)
- LHW Consulting (Broadcast)
- Kintronic Labs (Broadcast)
- NPSTC (Public Safety)
- Calif Office Emerg Serv (Public Safety)
- Society of Amateur Radio Astronomers
- Radio Jove Spectrograph (Astronomy)
- ARRL (Amateur Radio)
- GPSIA (GPS)
- Deere and Company (GPS)
- Exacter, Inc (Power Lines)
- Shure Inc (Wireless Microphones)
- Pericle Comm (Noise Hunter)
- CTIA (Cellular)
- AT&T Services (Cellular)
- Verizon (Cellular)
- American Lighting Assoc (Lighting)
- Philips Lighting (Lighting)
- NEMA (Lighting)

Cited Noise Sources

- Power Lines (cited by 28 respondents)
  - Incidental Noise Source
    - Power Line Arcing
  - Unintentional Noise Source
    - Power line radiation of conducted noise
  - Intentional Noise Source
    - Broadband over Power Lines (BPL)
    - Power Line Communications (PLC)

Cited Noise Sources

- Advanced Lighting (cited by 32 respondents)
  - CFL
  - LED
  - Unintentional Radiators
- Rebuttals
  - Industry representatives claim that properly designed lights meet regulatory standards
  - Some respondents reported some brands of lights caused excessive noise while others did not.

Cited Noise Sources

- Arrays of Lights (5 respondents)
  - Individual lights were reported to be compliant
  - The array made with those compliant lights was heard to be noisy
- Reported Noise vs. Compliance
  - Many respondents reported lighting devices that were “noisy”
  - No respondent made calibrated measurements to confirm that the “noise” they reported exceeded regulatory limits.

Cited Noise Sources

- Switching Power Supplies (32 respondents)
  - Unintentional Radiators
  - Consumer Electronic Power Supplies and Wall Chargers
  - Found almost everywhere
  - “Noisy” vs “Quiet” Wall-Warts were reported
  - No respondent made calibrated measurements to confirm that the “noise” they reported exceeded regulatory limits.
- Pulse Width Modulated Speed Motors (14 respondents)
- Cable TV Leakage (2 respondents)

Cited Services That Are Affected

- MF (34 respondents)
  - AM Broadcast Radio
- HF (31 respondents)
  - Amateur Radio
  - Shortwave Broadcast
- VHF (28 respondents)
  - FM Broadcast Radio
  - Low band DTV
  - Public Safety

Cited Services That Are Affected

- UHF (16 respondents)
  - High Band DTV
  - Public Safety
  - Cellular Telephone
  - WiFi and Bluetooth
- GPS/GNSS (7 respondents)
- General principle is that noise affects low frequencies the most and decreases with increasing frequency
- Trend appears to be that noise at higher frequencies is increasing

Regulations

- Conducted vs Radiated Emissions
  - Conducted noise can aggregate on power lines and then radiate
- Class A vs Class B Limits
  - Devices tested to higher limits (Class A, Industrial) but often used in residences (Class B), with more stringent limits
- Part 15 vs Part 18 Limits
  - Misinterpretation of rules causes some lighting devices to be tested to higher limits that appropriate

Regulations (cont)

- Frequency Ranges Tested
  - Radiated limits not tested below 30 MHz
- Good Engineering Practice
  - Interpreted differently by various manufacturers
- Enforcement
  - 19 respondents say more enforcement is needed
  - 1 respondent submitted examples of enforcement actions that have been taken against noncompliant devices

Other Concerns

- Propagation (5 respondents)
  - Evidence of directionality of HF noise from Asia in Guam
  - Evidence of decreased noise floor during power grid failure hundreds of miles distant.
- Noise in Cellular Bands
  - 2 respondents stated that license holders in cellular bands often solve their noise problems expeditiously and privately
  - 3 respondents related noise situations that have degraded operation of cellular systems and were not caused by other cellular carriers. Solving such noise problems case-by-case was “the slowest, most expensive, and most inefficient method and would be more efficiently dealt with by regulatory avoidance of noise.

Performing a Noise Study

- Virtually unanimous agreement that a noise study is needed
  - 1 respondent thinks problems are obvious, no study needed
- 20 respondents had suggestions for studying the noise floor
  - Most thought uncalibrated data could be used to show trends
  - Several respondents mentioned existing data taken over years that is available for analysis
  - 2 respondents believe only calibrated data can be used

What’s Next?

- NOI / NPRM should be issued to resolve unanswered questions and take corrective action, if necessary.
  - Is observed noise due to noncompliant devices on the market?
  - Should radiated emissions testing be made below 30 MHz?
  - How should aggregation of emissions from arrays of individually compliant devices be regulated?
  - Should the distinction between Class A & Class B devices remain?
  - Should differences between Part 15 & Part 18 emissions limits remain?
  - Are current regulatory emissions limits sufficiently low?
  - Should some classes of devices continue to be excluded from mandatory emissions testing?
  - Should an FCC label confirming emissions testing be required on every device?

THANK YOU