FCC Technological Advisory Council

September 20, 2016

Agenda

12:30pm	Introduction
12:40pm	Mobile Device Theft Prevention Working Group
01:20pm	Cybersecurity Working Group
02:00pm	Implications for Mass Deployment of Aeronautical/Space Transmitters
02:40pm	Future Game Changing Technologies Working Group
03:20pm	NG Internet Services Working Group
03:35pm	Spectrum and Receiver Performance Working Group
03:50pm	Wrap Up

Mobile Device Theft Prevention WG
Report to the FCC TAC

September 20, 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

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
- 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.
- 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.

Status Review of MDTP 2014 & 2015 Recommendations

- Develop 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	Associated Industry Activities
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

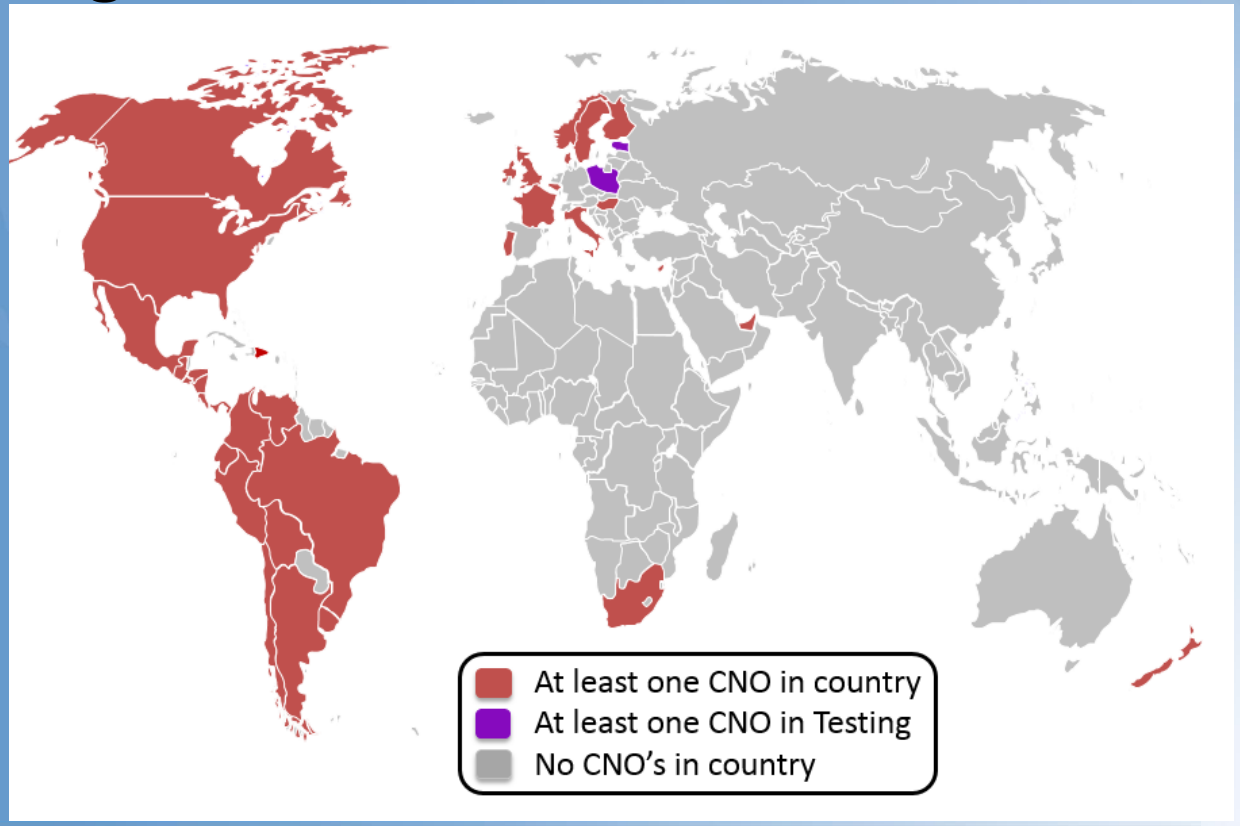
Industry MDTP Related Activities - continued

- 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

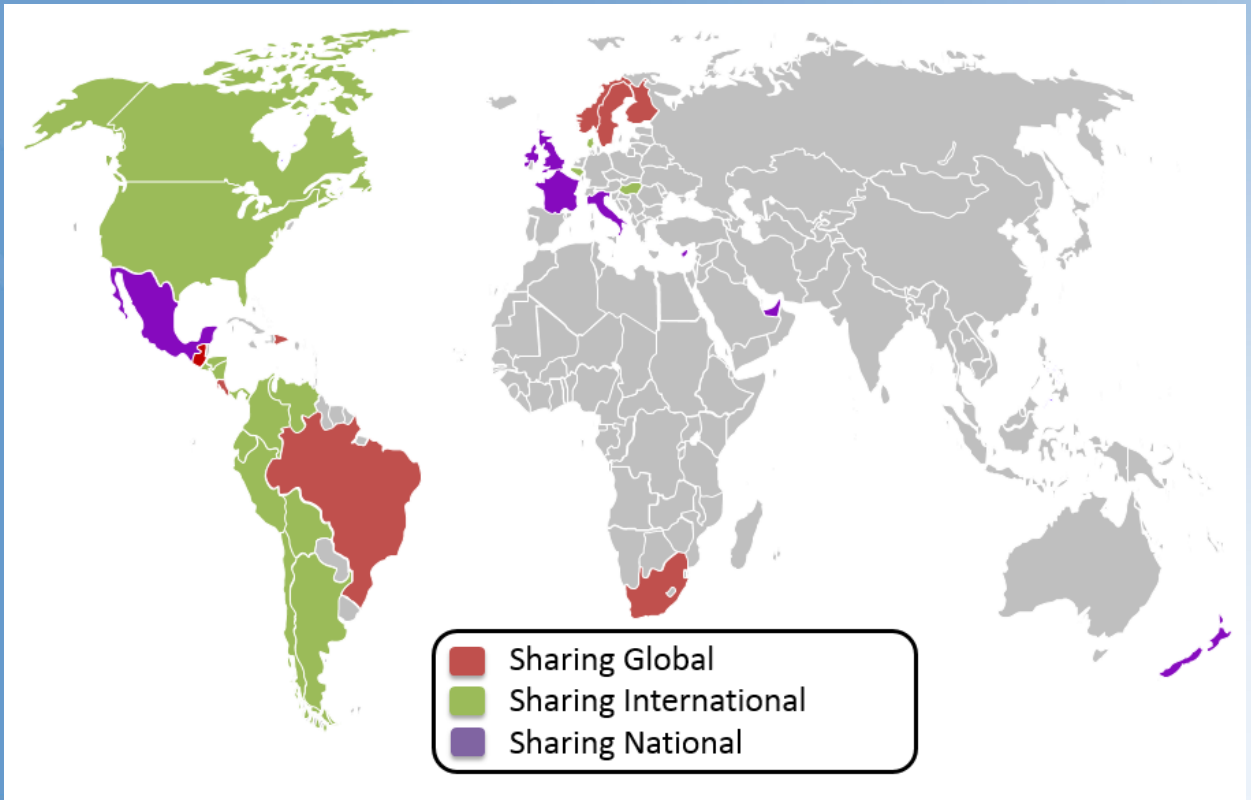
GSMA Stolen Device Data Sharing Report July 2016

- 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 IMEI Database maintains a global blacklist collated from the data provided by the contributing operators
- 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

Operators currently participating in lost and stolen blacklisting are active in the shaded countries



Rough overview of lost and stolen data sharing taking place between operators



Key Take-away & Draft Recommendation

- 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
  - Australia uses national solution
- Draft recommendation
  - The FCC TAC recommends that the FCC work with the U.S. State Department to encourage further global participation in lost and stolen blacklisting and lost and stolen data sharing

Lost/Stolen Device Trafficking Patterns Project

- Industry does not have good information on where lost or stolen devices are appearing on networks and whether any trafficking patterns can be detected

- GSMA indicated that there is an opportunity to gather new information to address this, ie
  - What levels of lost or stolen devices are being blocked on networks by taking blocking logs from carrier blocking solutions?
  - What levels of lost or stolen devices are appearing on networks not implement blocking by taking dumps of the IMEIs on such networks and comparing them to the blacklist?

- GSMA called for volunteers to participate in gathering this information to determine what we can learn, i.e.,
  - Can we establish how many stolen devices stay in-country vs leave?
  - Do stolen devices migrate to non-blocking networks and to what degree?
  - When stolen devices are presented to a network, which networks do they come from?

- Such information could be useful to both carriers and the FCC

- Requires effort on the part of participating carrier's in gathering data
  - The data is sensitive and GSMA will respect any confidentiality requirements

Breaking News – Further MDTP Analysis Needed

- 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
  - CHICAGO (Sun-Times Media Wire) - Chicago Police are warning of robbers who have stolen cellphones, then demanded victims reset the phones in the South Loop over the last two weeks
  - The suspects confront victims on the sidewalk, pull out a semi-automatic handgun and demand cellphones, wallets and purses, police said.
  - They threaten violence and demand that victims **unlock their phones and reset the settings to factory status**, police said. They also demand the PIN numbers of victims' bank cards.

- London - post "kill switch" anecdotal reports that while there was a downward pressure on volume of phone crime the nature of the remnants were becoming more serious as the thiefs got wise to the necessity to disable solutions such as find my iphone

Next Steps

- **Proposed scope/direction**
  - Provide recommendations from the 2014 and the 2015 MDTP reports to close any remaining gaps toward completing the actions specified
  - Analyze consequences of mobile phone theft solutions (“Breaking News”)
  - Initiate GSMA Lost/Stolen Device Trafficking Patterns Project
  - Discussions with Police Chiefs:
    - 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 Law Enforcement colleagues.
    - Request updated smartphone theft statistics in order to evaluate the effectiveness of the theft prevention measures implemented to date.

- **Key deliverables**
  - **December 2016:**Provide final recommendations and industry updates for 2016 work items; propose 2017 work items

Cybersecurity Working Group

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

20-Sept-2016

Topics

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

5G Security Subcommittee

- Amit Ganjoo – ANRA Technologies (co-chair)
- Tom McGarry – Neustar (co-chair)
- George Popovich – Motorola Solutions
- 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
- Brian Russell – Cloud Security Alliance
- Christoph Schuba – Ericsson
- Paul Steinberg – Motorola Solutions
- John Yeoh – Cloud Security Alliance
- Padma Krishnaswamy – FCC
- Ahmed Lahjouji – FCC

2016 TAC 5G Security – Scope/Deliverables

- **Proposed 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

2016 TAC 5G Security – Work Plan

- **Security Recommendations**
  - Create a TAC paper of draft security recommendations by Sept TAC meeting – Complete
    - DoS
    - Key Management
    - Identity Management
    - Isolation Mechanisms
  - Obtain TAC paper approval at Sept TAC meeting
  - Obtain TAC approval to work draft recommendations/paper with ATIS PTSC at Sept TAC meeting
  - Create TAC paper of final security recommendations pursuant to ATIS interactions
  - Obtain revised TAC paper approval at Dec TAC meeting
  - Obtain TAC and FCC approval of final TAC security recommendation
    - FCC recommendation to encourage 3GPP members to support TAC paper at 3GPP
    - Potentially encourage support at other SDOs – TBD
- **5G SDOs**
  - Identify key SDOs working on 5G standards
  - Informational only, no specific recommendation
  - Recent focus has been on recommendations
    - Subcommittee will finalize SDO work in 4Q

FCC TAC 5G Security Appendix: Recommendations

2016 TAC 5G Security – Recommendations

- **Denial of Service**
  - It is recommended that 5G standards be defined in such a way as to enable resource isolation techniques such as network slicing to confine the effects of DoS attacks
  - It is recommended that 5G networks be able to deauthorize an individual device (or multiple devices) in such a way as the device does not continue to utilize the control plane or media plane resources
  - It is recommended that base stations have the ability to schedule the radio resource for each device in an unpredictable way
  - It is recommended that 5G network elements embed DoS detection and mitigation functions into the RAN functions via key security indicators with related dynamic resolution

2016 TAC 5G Security – Recommendations

- **Key Management**
  - It is recommended that industry standard encryption techniques be used to protect data during transport
  - It is recommended that 5G networks provide options for using asymmetric key material to support diverse IoT Use Cases
  - It is recommended that 5G networks enable privacy protections to guard against using key and certificates to identify and track consumers
  - It is recommended that 5G standards development consider alternative trust models that enable flexibility in establishing trust models across heterogeneous devices, access technologies, network domains and communication modes
  - It is recommended that 5G networks support new secure enrollment processes that allow entities other than carriers to provision enrollment certificates to devices
  - It is recommended that 5G networks support robust methods for identifying and responding to misbehavior
  - It is recommended that 5G networks support multiple devices that operate at multiple levels of sensitivity/assurance

2016 TAC 5G Security – Recommendations

- **Identity Management**
  - It is recommended that the 5G network that provides access to a device be able to uniquely identify, authenticate and authorize each individual device that accesses the network either directly or indirectly (e.g., via a gateway, virtual network)
  - It is recommended that an equipment or subscriber identity that is transported across networks and presented to a terminating device be authenticated and authorized
  - It is recommended that UE be able to authenticate the network before attaching
  - It is recommended that Soft SIMs deploy rigorous cybersecurity measures that can protect against attacks aimed at software applications
- **Isolation Mechanisms**
  - It is recommended that 5G standards be defined in such a way as to enable resource isolation techniques such as network slicing to enable different levels of security among different resources
  - It is recommended that there be access to the control plane and media plane at the base station to enable security monitoring of traffic

Topics

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

Cyber Security - SCR Sub-Working Group

Mike Bergman – CTA (leader)
Ahmed Lahjouji- FCC
Alex Salvarani – Nokia
Amit Ganjoo – ANRA Technologies
Brian K. Daly – AT&T
Bruce Oberlies – Motorola Solutions
Christoffer Jerkeby – Ericsson
Dan Torbet – Arris
David Kay – Netgear
Edna Prado – FCC
George Popovich – Motorola Solutions
Martin C. Dolly – AT&T
Mike Geller – Cisco
Paul Steinberg – Motorola Solutions
Rashmi Doshi – FCC
Richard Green – Liberty Global
Russ Gyurek – Cisco

FCC Direction: Cyber Security of Software Configurable Radios

- 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?

Additional Background to the Problem Space

- FCC feedback:
  - Current SDR rules and checklist approach is problematic
  - Ref. KDB 594280 D02, U-NII Device Security
  - Manufacturers rarely use this “SDR” option
  - Checklist submissions reuse same info
  - Still have SDR interference problems in the field
- Possible to improve the filing process, or identify a “technical fix”, to improve these results?

SCR Group Plan

- Develop Background Information
  - Identify target parameters and controls
  - Identify common methods of protection
  - Identify key issues
- Review existing SDR approach (checklist)
  - What works?
  - What does industry do in this context?
  - What can we recommend ("technical fix")?
    - A technical challenge – how does the device know where it is?

Protect: Target RF Parameters

- Operating frequencies (band and bandwidth)
- Output power
- Modulation and media access types
- Smart antenna programming
- Spectrum sharing algorithms and decision-making processes

Protect: Configuration controls

- Master vs. client controls (15.202)
- Regional controls (USA RF-related behavior vs. ROW)
- Module controls
- Operational mode
  - Ad-hoc/p2p/mesh (e.g. 802.11);
  - Bridge/mesh; master/client; and p2p/p2mp (access points)
- Antenna configuration

Status

- Meeting weekly since 6/16/2016
- Developing background information based on manufacturer input (white paper format)
- Reviewing SDR checklist
- Considering “technical fix” challenges
  - AuthN/AuthZ, geolocation, impact on business processes…?

Topics

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

Securing SDN Sub-Working Group

Mike Geller – Cisco (co-leader)
Ken Countway – Comcast (co-leader)
Martin Dolly – AT&T
Brian Daly – AT&T
Ramani Pandurangan – XO Communications
David Tennenhouse – VMWare
Dennis Moreau – VMWware

Christoph Schuba - Ericsson
Shanthi Thomas – Motorola Solutions
Kathrina Hardy – Verizon
Padma Krishnaswamy – FCC
Ahmed Lahjouji- FCC
Kevin Rossi - Genband

FCC Direction: Securing SDN

- **FCC's Goal for the WG**

  "SDN is sometimes considered to carry significantly more cyber risk than traditional network architectures. Therefore, the need to manage cyber risk in the SDN centralized network's control plane and distributed dataplane seems essential. It would be worthwhile to build security in up-front as opposed to retrofitting it, and seeking to apply lessons learned from the long running efforts to secure existing control plane protocols such as BGP and DNS. To that end, we suggest the following approach: Leverage what has been learned during the first phase of this work to develop Best Common Practices (BCP) to mitigate cyber risk associated with SDN/NFV."

- **FCC's Questions**

  1. Identify existing BCPs that focus on securing programmable networks, particularly those that are based on SDN/NFC 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

- **Proposed 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 NVF 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 (on track)
  - **December 2016:** a) BCPs Finalized for Prioritized Use Cases, b) Promotion Activity

Progress From Last Update

- Several companies/speakers have been hosted for presentations and discussion
  - Versa Networks
  - Dispersive Technologies
  - Red Hat (OPNFV Security Group Founder)
  - VMWare
- BCP work has now started

Draft BCP's In-Progress

1. Service Provider SD WAN

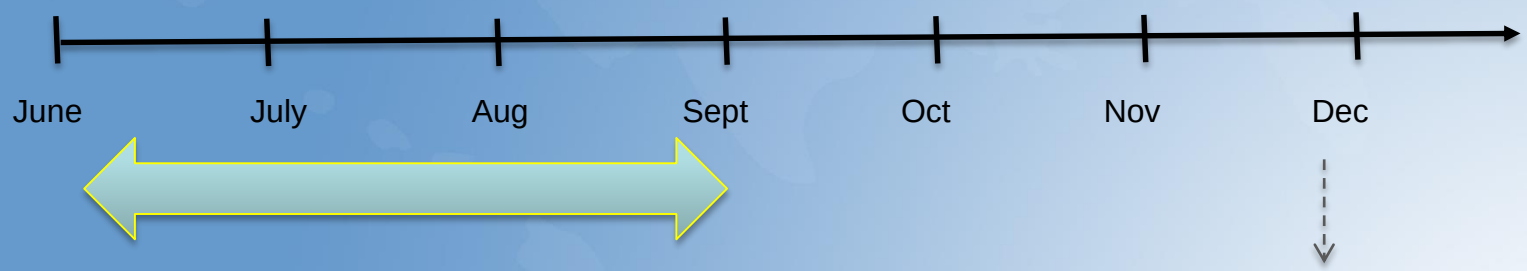
- Secure SD WAN Endpoint Enrollment
- Key Management
- Identity Management
- Ongoing Endpoint Trust

2. Using SDN to Mitigate DDOS Attacks

Work Plan Status – *On Track*

- *Team finalized and engaged*
- *Use cases finalized*
- *High level project plan developed*
- *Industry expert interviews begin*

- *Begin writing BCP's*
- *Assign and distribute work across the team*
- *Bring in expert knowledge as needed*



- *Further refine Work Plan*
- *Key areas of focus under use cases begin to form/refine*
- *Adjust industry engagement as needed*
- *Build BCP structure and outline #1,2*
- *Draft BCP life cycle recommendations #3,4,5*

Final Draft BCP's, White Paper and Life Cycle Recommendations to FCC

FCC Technological Advisory Council Working Group:

Implications for Mass Deployment of Aeronautical/Space Transmitters

September 20, 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)

Sean Cassidy (Amazon)

Richard Heinrich (Rockwell Collins)

Patricia Cooper (SpaceX)

Don Jansky (Jansky-Barmat Telecommunications)

Overview of 3Q Activities

- High Altitude Platform Stations (HAPS)
  - Facebook and Google are conducting experiments and Facebook demonstrated first HAPS flight
  - As the HAPS are still in an experimental stage, the TAC WG recommends individual companies to continue their efforts and inform FCC on their progress as appropriate.
  - No further action is required by FCC at this moment
- LEO Satellite-based Broadband Service
  - TAC WG was briefed by OneWeb and Boeing on their plan to deploy hundreds/thousands LEO satellites. TAC will be briefed by Space-X on their NGSO satellite broadband constellation plans.
  - WG may continue further discussions in 4Q on NGSO spectrum needs and spectrum sharing with NGSO and UAS
- UAS Discussions
  - During the 3Q, most of the WG resources were spent on UAS classifications, relevant issues and formulating recommendations

Goals of UAS WG Discussion

- Collect and classify industry spectrum needs for Unmanned Aircraft Systems ("UAS"), for:
  - (1) small UAS recreational
  - (2) small UAS commercial
  - (3) Other UAS commercial operations

- Help identify issues for FCC and FAA resolution to clear the way for use of spectrum for UAS.

UAS Discussions In a Nutshell

Federal Communications Commission

Federal Aviation Administration

National Aeronautics and Space Administration

Spectrum Management

Safety of Life

UAS Traffic Management

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), and observing many of the same operating restrictions that apply under Part 107 (VLOS, below 400 feet AGL, give way to manned aircraft, etc.) 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.

Classes of Operations

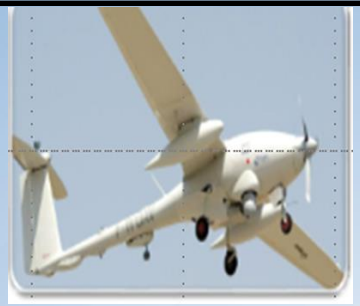
FAA Part 107 (Recreational)

- No direct safety requirement
- Registration
- Limitations:
  - Visual Line of Sight
  - <400 feet
  - restricted from airport and sensitive areas

FAA Part 107 (Commercial)

- Same as Recreational
- Wireless and satellite networks are considered for BVLOS
- Additional safety and reliability requirements may apply for Part 107 waivers

FAA Non-Part 107 (Commercial)



- Risk Based Certification , for example kinetic energy or other criteria
  - Scalable design assurance levels based on use

Spectrum Considerations

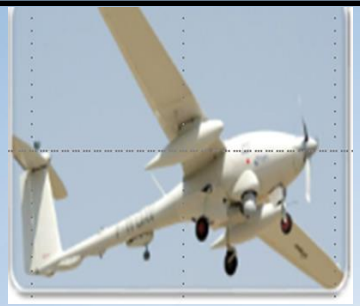
FAA Part 107 (Recreational)

C2 + Payload
(May Be Integrated Spectrum)

FCC Parts 15, 90, 95, 97
22, 24 (PCS), 25 (limited to Commercial),
27 (700 MHz, WCS, EBS, BRS,
AWS, L-band MSS)
There also is interest in using 800 MHz.

FAA Part 107 (Commercial)

FAA Non-Part 107 (Commercial)



C2

AM(R)S (terrestrial),
AMS(R)S & FSS
(satellite), L-band MSS

Payload

FCC Parts 15/24/
25/27/95

Certain waivers may require safety based spectrum

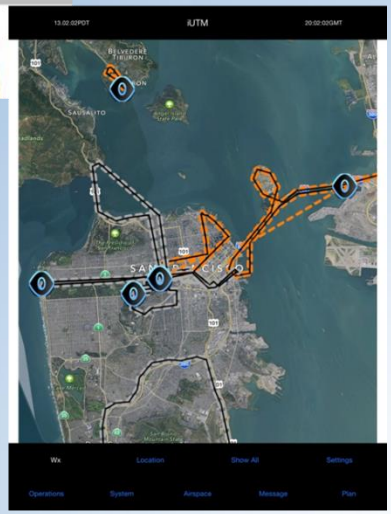
Unmanned Aerial Systems Traffic Management (UTM)
UAS Operator/UTM Functions

UTM: AIRSPACE MANAGEMENT

- Notifications accessible to UAS operators and public
- Static (like TFR) and dynamic (like security or public health scenario)

UAS OPERATOR

- Broadcast identity (and possibly intent)
- Operations accessible by all
- No anonymous flying



(source: NASA UTM presentation to TAC)

Unmanned Aerial Systems Traffic Management (UTM) Functions (source: NASA UTM presentation to TAC)

Route Structure

- Only where needed for safety or efficiency of flight
- Procedural rules-of-road (corridors, altitudes, etc).

Flow Control

- Only where needed for safety or efficiency of flight
- Manage access into areas of operation, not particular operation

Air Traffic Control

- Integrated with manned air traffic control, where positive UAS control is required for safety or efficiency of flight
- Static or dynamic application (e.g., ability to respond in crisis situation where sustained mixed operations are required)

Mantra 1:
Flexibility where possible and structure where needed

Mantra 2:
Risk based- Geographical needs, application, and performance-based airspace operations

(source: NASA UTM presentation to TAC)

UTM Research Technical Capability Level Timeline

Each capability is targeted to type of application, geographical area and uses risk-based approach

Capability 1 (August 2015)

- Reservation of airspace volume
- Over unpopulated land or water
- Minimal general aviation traffic in area
- Contingencies handled by UAS pilot
- Enable agriculture, firefighting, infrastructure monitoring

Capability 3 (January 2018)

- Beyond visual line of sight
- Over moderately populated land
- Some interaction with manned aircraft
- Tracking, V2V, V2UTM and internet connected
- Public safety, limited package delivery

Capability 2 (October 2016)

- Beyond visual line-of-sight
- Tracking and low density operations
- Sparsely populated areas
- Procedures and “rules-of-the road”
- Longer range applications

Capability 4 (March 2019)

- Beyond visual line of sight
- Urban environments, higher density
- Autonomous V2V, internet connected
- Large-scale contingencies mitigation
- News gathering, deliveries, personal use

(source: NASA UTM presentation to TAC)

Recent Headlines

Google's Alphabet Wing drones will deliver burritos to students at Virginia Tech University

Patent Gives a Peek at Amazon's (AMZN) Ambitious Drone Delivery Project

Facebook's Aquila drone completes first test flight

Jessica Guynn, USA TODAY 9:08 p.m. EDT July 21, 2016

AT&T tests drones on its LTE network to prepare for deliveries

And it's all powered by Qualcomm's Snapdragon Flight platform.

Qualcomm and AT&T Are Joining Forces on a New Drone Project

Comparison Matrix

	Part 107 (Recreational)	Part 107 (Commercial)	Non-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	>55 pounds • Will also include platforms <55 pounds that exceed Part 107 limitations Commercial Services: • Unmanned commercial aircraft • Communications • Public safety • Federal Use
User Base	Individuals	• Individuals • Leased service suppliers • Package delivery	• Commercial service providers • Individuals
Market Size (by volume)	Very Large	Large	Medium to Small

Comparison Matrix (cont)

	FAA Part 107 (Recreational)	FAA Part 107 (Commercial)	FAA Non-Part 107 (Commercial)
C2 Links	FCC Parts 15/95/97	FCC Parts 22/24/27/90 Terrestrial cellular or satellite with appropriate reliability	FCC Part 87, AM(R)S, FCC Part 25, AMS(R)S, FSS and L-band MSS* Requires C2
Payload Links	FCC Parts 15/24/95/97	FCC Parts 15/22/24/25/27/90 Terrestrial cellular or satellite	FCC Parts 15/22/24/25/27/90 HAPS allocation
C2 Safety Spectrum	Excluded (non-safety command, control, and payload communications capability)	Excluded (non-safety command, control, and payload communications capability) Part 107 Waivers: Depends	Required
UTM	UTM (still under WG discussion)	UTM (still under WG discussion)	IFR / Core Air Traffic Control environment

*subject to RTCA SC-228 C2 satellite MOPS

Future FCC Actions for Part 107 Recreational UAS

Requirements	Recommendations
C2/Payload	Part 15/95/97 are used in today's products and expect to be used in future FCC to study the interference risk from wide use of airborne transmitters to terrestrial and other airborne systems that are based on Part 15 rules
Safety/Certification	FCC should invite study of harmful interference in bands adjacent to those used by UAS FCC should notify services adjacent to UAS frequency bands of the possibility of harmful interference.
Air Traffic Control/UTM	May not be required for VLOS, seeking clarification from FAA or WG experts

Future FCC Actions for Part 107 Commercial UAS

Requirements	Recommendations
C2/Payload Spectrum	FCC to consider how to support VLOS and eventual BVLOS UAS flights with terrestrial network and whether all data and safety needs can be met via one system that may include MSS satellite spectrum TAC WG discussion will be focused on recommendations during the 4Q quarter FCC should invite study of harmful interference in bands adjacent to those used by UAS. Study outcome may indicate FCC should notify services adjacent to UAS frequency bands of the possibility of harmful interference.
Safety/Certification	For Part 107 waivers: • FAA to manage in consultation with relevant stakeholders, including UAS community and wireless carriers • Certain safety features may require unique implementation depending on specific frequency bands and their associated FCC regulations. • FCC to continue collaboration with FAA on such instances

Future FCC Actions for Non-Part 107 Commercial UAS

Requirements	Recommendations
C2	FCC to initiate the rulemaking process to establish the service rules for C2 per WRC 12 and WRC 15 (Res. 155)
Payload Spectrum	Further WG discussion in Q4. Expect Satellite or other commercial links will be utilized (application specific)
Safety/Certification	FAA to manage with consultation with relevant stakeholders, including RTCA and ICAO Certain safety features may require specific use of frequency bands or subject to FCC regulations. FCC to continue collaboration with FAA on such instances.
Air Traffic Control/UTM	FAA to manage with consultation with NASA and relevant stakeholders

Future FCC Actions for Non-Part 107 Commercial UAS

Requirements	Recommendations
Air Traffic Control/UTM	FAA to manage in consultation with NASA and relevant stakeholders
C2	FCC to initiate the rulemaking process to establish the service rules for C2 per WRC 12 and WRC 15 (Res. 155)
Payload Spectrum	Payload Spectrum is not safety critical but may be critical for commerce. Many payload applications, such as video transmission, may require significantly more bandwidth than C2. Satellite or other commercial links may be a solution in some cases but investigations may be required to determine how airborne usage affects existing users sharing or using adjacent spectrum. There may be other UAS operations with needs that cannot be served by satellite or commercial wireless networks that may require new allocations of dedicated or shared spectrum.

Future Actions for Non-Part 107 Commercial UAS

Requirements	Recommendations
Safety/ Certification	FAA to manage with consultation with relevant stakeholders, including RTCA and ICAO Certain safety features may require specific use of frequency bands or subject to FCC regulations. FCC to continue collaboration with FAA on such instances.

Work Plan Q4

- Better understand industry perspectives
  - Capacity Estimates available from industry
  - Study types needed to understand capacity requirements
  - Detect and Avoid Spectrum Issues
  - Payload spectrum discussions
  - BVLOS satellite discussions
- HAPS – outstanding issues for WG
- Recreational – collect input that has not been represented
- Commercial – further organization and refinement of recommendations

Thank you

Glossary

ACAS-Xu – Airborne Collision Avoidance System – Xu (UAS) – this is the next generation collision avoidance infrastructure that enables lateral avoidance maneuvers. It utilizes ADS-B information exchanges. (See TCAS)

ADS-B Out – Automatic Dependent Surveillance – Broadcast Out – a periodic message broadcast using 1090 MHz and 978 MHz (Universal Access Transceiver – UAT) to provide the address, position, velocity, time, and position performance information to air traffic management and aircraft equipped with suitable receivers to improve situational awareness

ADS-B In – this is the ability to receive and display ADS-B Out messages from adjacent platforms. This could include conflict detection algorithms for processing the reports to take specific separation management actions

ADS-B Out-like – The same as ADS-B in terms of information exchange but uses other spectrum. (e.g. Cellular/LTE) This technology can be used for airframe to airframe conflict management.

Autonomy / Automated / Automation – The automation in certain small unmanned aircraft flying below 400 feet may suggest that less continuous spectrum access is needed for C2, compared to aircraft that are not as automated.

BLOS – Beyond Line of Sight – this is the generic term. See BRLOS and BVLOS

Glossary

BRLOS – Beyond Radio Line of Sight – in the context of communications (C2 and Payload) this is a description of the operational coverage "range". This characteristic will be different for single channel, point-to-point structures versus networked communications systems

BVLOS – Beyond Visual Line of Sight – this is the sight distance between the operator and the flying platform. The BVLOS characteristic requires visual observation of the platform either from the controlling pilot or a designated observer.

C2 – Command and Control – this is the "telemetry" exchange between the ground control station and the flying platform. Trajectory management, state information, etc. are exchanged

CNPC – Control, Non-Payload Communications – safety designated spectrum has been specifically segregated for command and control and does not include payload information exchanges. CNPC spectrum is reserved for non-FAA Part 107 operations. (Payload would be handled over another communications link and may not have the same link performance parameters.)

DAA – Detect and Avoid – this is the capability to provide separation management and collision avoidance between platforms. It consists of three elements: cooperative separation management (**e.g.** ADS-B), Collision Avoidance (**e.g.** ACAS-Xu), and a non-cooperative sensor (e.g. optical sensor, radar, etc.)

Leased Service Providers – Fleet operators that aggregate services. Sell services on a per hour or per task basis. Eliminates the need for individual users to meet the operational criteria

Payload –Everything that a UAV carries that is not required for flight. This includes the information captured by and sent from the flying platform (e.g. optical, sensor data, live video communications, etc.)**. It also includes spectrum for end user communications for HAPS networks and other UAS uses for communications relay and distribution. If UAS are to be used as infrastructure for currently assigned wireless network spectrum then additional rule making may be required to ensure that UAS usage stays within acceptable interference footprints as today's towers.**

Recreational – part of the category description for Model Aircraft and FAA Part 107 platforms. This is meant to include hobby, radio control enthusiast, amateur, and non-revenue operations. The only policy requirement is to register the platform, and the operating restrictions are similar to commercial Part 107 users. This class of platform comes with a public use, non-safety command, control, and payload communications capability which also applies to commercial Part 107 users.

RA – Resolution Advisory – Part of TCAS – this is the coordinated evasive maneuver to avoid a collision between two flying platforms

TA – Traffic Advisory – Part of TCAS – this is the coordinated identification of traffic that is in-range and a potential collision candidate. Interrogations and Replies are exchanged between the platform pair

TCAS Type 1 – Traffic Collision Avoidance System – a cooperative collision avoidance system. Type 1 recognizes that one of the platforms passive and is not capable of taking an evasive maneuver and relies on one of the paired aircraft taking the action. Evasive maneuvers are vertical, not lateral

TCAS Type 2 – Traffic Collision Avoidance System – a cooperative collision avoidance system. Type 2 recognizes that both of the platforms negotiate an evasive maneuver using the TA/RA logic. Evasive maneuvers are vertical, not lateral

UTM – UAS Traffic Management – This is focused on supporting FAA Part 107 operations below 400 feet. At present the FAA's view is for this to be a traffic monitoring capability for operations below 400 feet to provide situational awareness, allow data exchange among operators and regulators, provide authentication, airspace configuration, weather and wind prediction and sensing, conflict avoidance, airspace notification, demand/capacity management, large scale contingency management (GPS outage, cell outage).

Future Game Changing Technologies Working Group

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

20-Sept.-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
- FCC Liaison: Walter Johnston, Padma Krishnaswamy
- Members:
  - Kumar Balachandran, Ericsson
  - John Barnhill, Genband
  - Mark Bayliss, Visualink
  - Lynn Claudy, NAB
  - Brian Daly, AT&T
  - Hans-Juergen Schmidke, Facebook
  - Jeffrey Foerster, Intel
  - Dick Green, Liberty Global
  - Ramani Panduragan, XO Communications
  - Jack Nasielski, Qualcomm

Working Group Members Cont'd

- Russ Gyurek, Cisco
- Brian Markwalter, CEA
- Paul Misener, Amazon
- Lynn Merrill, NTCA
- Mark Richer, ATSC
- Marvin Sirbu, SGE
- Paul Steinberg, Motorola Solutions
- Lisa Guess, Juniper Networks
- Nomi Bergman, Brighthouse Networks
- Michael Browne, Verizon
- Steve Lanning, Viasat
- Marty Cooper, Dyna LLC
- Charla Rath, Verizon
- Dewayne Sennett, AT&T
- Michael Tseytlin, Facebook

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

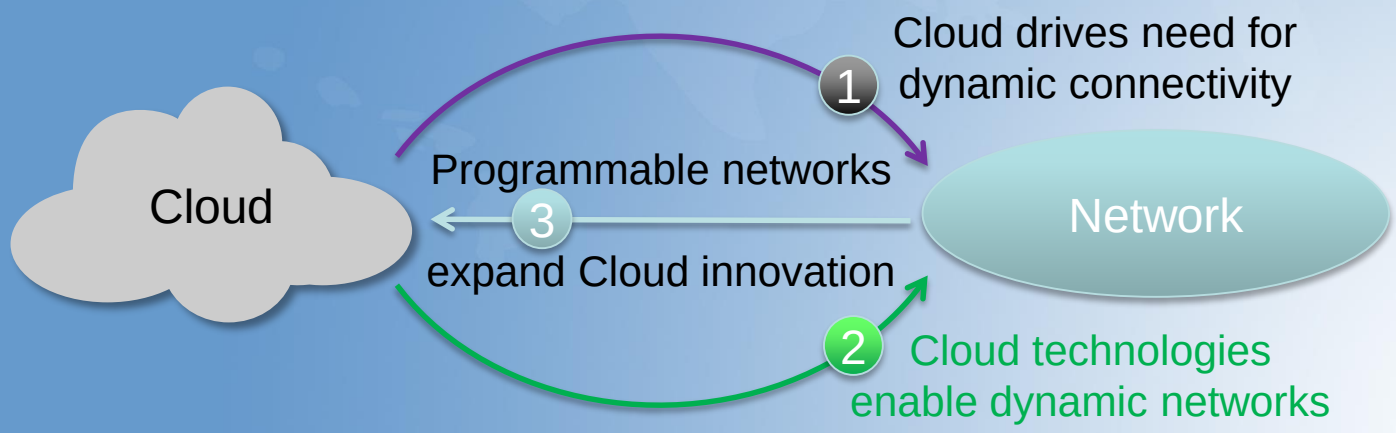
July 29th "Holographic Beamforming" Pivotal Communications – Eric Black
August 5th "Advanced antennas" Kymeta – Nathan Kundtz
August 12th "The 4P Project" Stanford U. – Prof. Nick McKeown
August 25th "Wireless Access Products" Tarana Wireless - Steve Sifferman
August 26th "Terragraph Briefing" Facebook – Neeraj Choubey
August 26th "Spectrum Collaboration Challenge" DARPA – Paul Tilghmane
Sept. 1st "Expected Tech Changes in Media Distribution" Akamai – Will Law (joint w/NGI)

Mindset for the Future

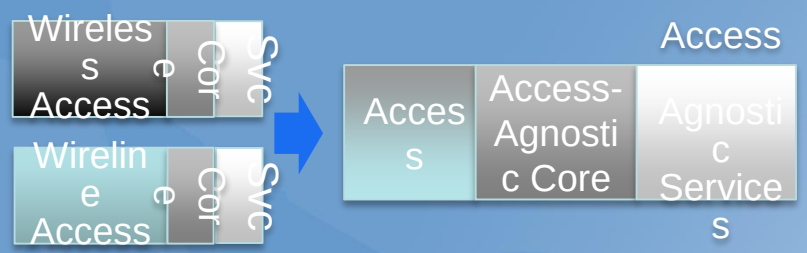
- Key thoughts
  - Oversight, investments in, and operations of communication infrastructure and services are facing a world in which:
    - The change in technologies, operations, and business models is continuous and rapid
    - Similar functions for voice, data, and video can be delivered in multiple ways often using very different technologies
    - The applications of communications are increasingly parts of complex systems and there is significant overlap between the tradition roles of operators, equipment suppliers, and the creators of content and applications
    - Access to broadband wireless Internet is becoming an essential ingredient for education, health care, and other societal needs; the FCC will need to consider actions that facilitate ubiquitous and affordable broadband wireless access for all
    - End users have a strong "app mindset" with increased expectations for service availability & reliability, performance, rapid availability of new and improved apps and services

Programmable Networks

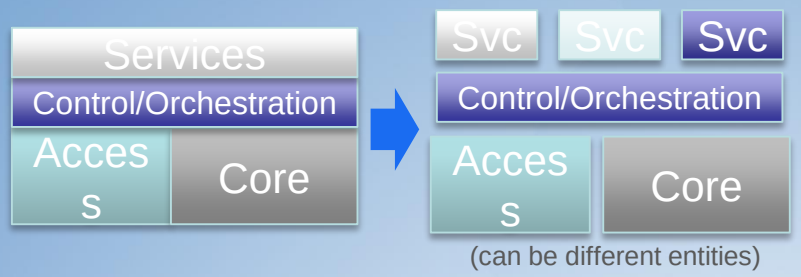
- Key thoughts
  - Network programmability is inextricably intertwined with Cloud, and will likewise be an area of rapid change for the next decade
  - Opens new (efficiently shared) uses of the network, much like cloud did for compute & storage
  - Virtualized distributed Edge Cloud/Fog/Mist architectures enable new performance sensitive applications, and new business models
  - Open source software will be an important component of this virtualized network function ecosystem
  - Networks will benefit from reduced cost, improved security, agility, and new products and services



4 Dimensions of Change Enabled by Programmable Networks

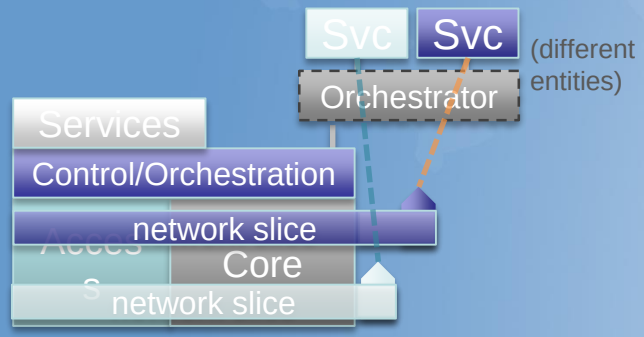


Convergence

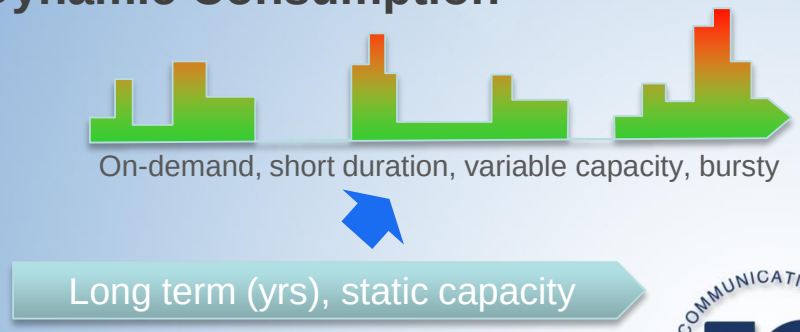


Disaggregation

Virtualized Sharing



Dynamic Consumption



4 Dimensions: Convergence

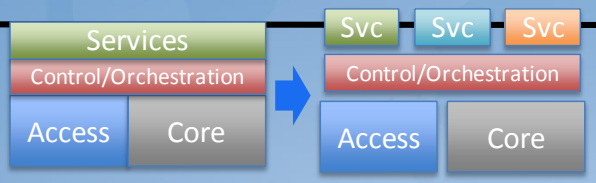
Drivers & Importance

- Access technology blurring
  - Fixed wireless 'last 100m' access
- Tighter RAN/backhaul coupling
  - Wireless network densification
  - mmWave spectrum usage, licensed/unlicensed/shared
  - Centralized cloud RAN
- Converged edge clouds
  - critical mass for wireless edge & low latency services distribution
- Essential for orders-of-magnitude wireless capacity scaling

Industry & FCC Consequences

- Wireless networks will benefit from access to wireline (Telco, Cable) assets
  - also hybrid satellite networks
- SDN/NFV transformation is *the* prime opportunity to converge networks and service offerings
- Conflicts with FCC and regulatory 'architecture', structured along wireless-wireline lines

4 Dimensions: Disaggregation



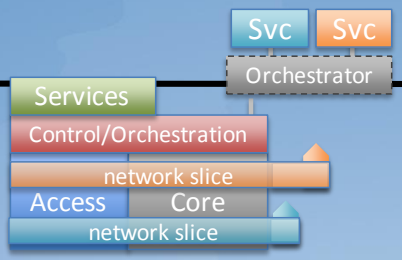
Drivers & Importance

- Network programmability enables modularization of value chain
  - mirrors disaggregation (and programming) within a network
- Mix & match agility to create new services
  - can include functions embedded in other entities' networks
- Flexibility to exploit new business models can spur economic activity

Industry & FCC Consequences

- Service delivery may become more segmented (involve more entities)
- Regulatory responsibilities may need to shift per segmentation of roles and relative feasibility
  - 911/PSAP access, LI, number assignment, SS7 access, …
- Black & white Common Carrier vs. non-CC distinction may be too rigid, impeding innovative

4 Dimensions: Virtualized Sharing



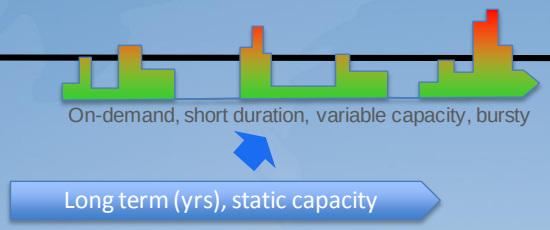
Drivers & Importance

- 5G use cases demand very diverse and extreme requirements
- Network programmability enables virtualized network slices
  - virtual functions, connectivity, or other resources dedicated to an entity, application, or service
- Opens opportunities for resource sharing both within and between operators
  - e.g. radio resources, edge compute
- Better utilization of scarce resources
- Enabler for 5G low latency applications

Industry & FCC Consequences

- Further segmentation & blurring of roles in service delivery chain
- Regulatory responsibilities may need to follow owner and location of key (often virtual) functions
- Black & white Common Carrier vs. non-CC distinction may be too rigid, impeding innovative

4 Dimensions: Dynamic Consumption



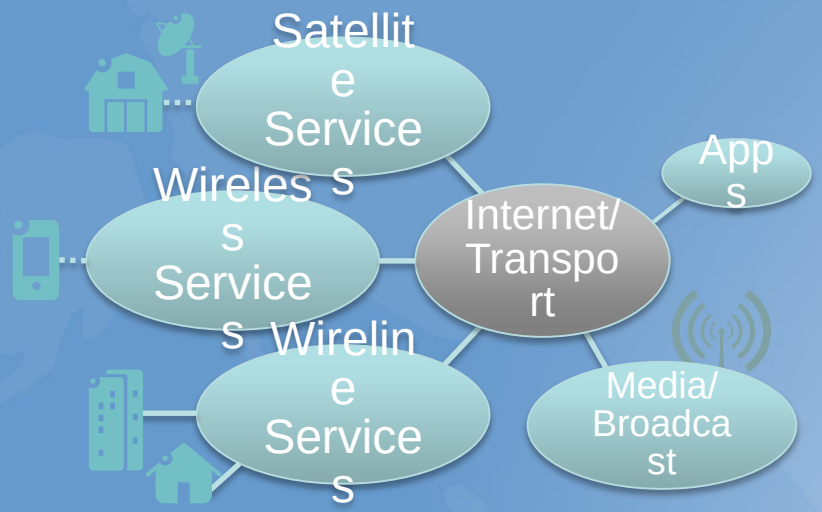
Drivers & Importance

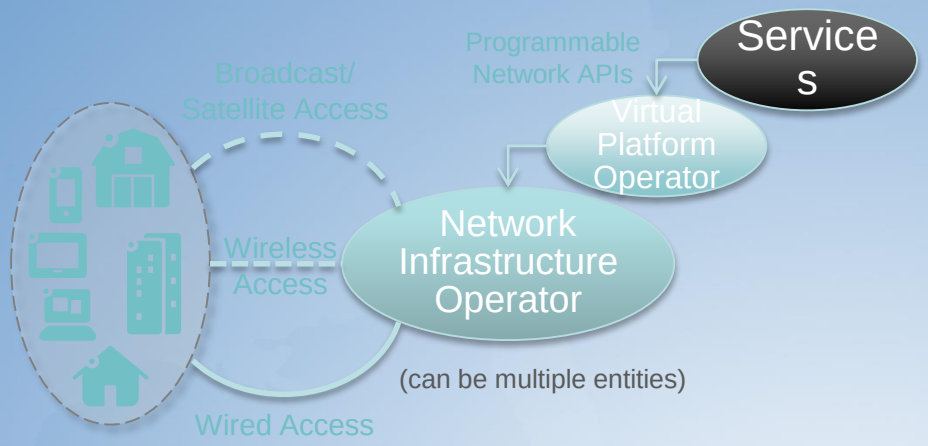
- Allows efficient 'pay-as-you-need' consumption of network resources
  - low startup linear cost structures
  - analogous with cloud services
  - driven by the dynamic needs of cloud
- Extends economical sharing opportunities end-end
- De-risks and encourages service & biz model experimentation
- 'Greases' service innovation, creating economic value

Industry & FCC Consequences

- Network services delivery must be fully automated, and API-driven
- Service offerings and entities will come & go on short timecycles
- Regulatory environment needs to operate on similarly short cycles
  - e.g. 3.5 GHz CBRS one-time upfront approval process

Need for Shift to Systems Thinking





Traditional Service-Technology Silos

- Specialized technologies/networks
- Largely static standard services
- Well defined entity relationships

Dynamically Interrelated Future

- Common Digital/IT technologies
- Mash-ups of access & services
- Rapidly changing

5G Networks

- Key thoughts
  - Involves a basket of technologies that will continue to drive performance and new functionality
  - Each of the technologies has its own evolution path
    - new air interface, mm-Wave, re-architecture of the mobile core, new applications, etc.
  - 5G technologies represents an evolution of existing capabilities but also the introduction of a significant new capabilities that will lead to value through completely new applications
  - Key use cases for 5G include:
    - Enhanced Mobile Broadband – enabling 4K video, VR, AR, Tactile Internet
    - Massive IoT – “billions” of connected devices, connected “everything”, Smart Cities
    - Wireless fixed access -
    - UHRLLC – highly reliable low latency enabling autonomous vehicles, Industrial control, Remote manipulation, Mission-critical applications e.g. eHealth, hazardous environments, rescue missions, etc.

5G: A Focus on Understanding Applications

- Key thoughts
  - A driver for 5G is the anticipation of **new and diverse requirements for IoT and new applications**. This includes greater automation, higher speed, lower latency and jitter, and co-existence of critical and non-critical functions. Lowering the economic barrier for introduction and sustainment of new applications is key.
  - An intrinsic assumption is that general purpose, software enabled and virtualized **5G** networks and infrastructure will **enable almost any application**. This will relieve the need for networks dedicated to a single purpose or to a specific industry.
  - Many applications that fall in the **IoT** space require ubiquity – anytime, anyplace. Examples include agriculture, energy production and transmission, natural resource extraction and processing. The verticals that operate in sparsely populated areas require a new approach for **economically viable 5G Network business models**.
  - A **systems view** puts a premium on establishing the business cases for major applications, whether private or public, that can justify the commitment to investments in 5G Networks. This include areas such as Health care, Education, Law Enforcement, Transportation and Logistics, Mining, Manufacturing, Energy, and Management of Natural Resources.

5G: Significant Improvement in Spectrum Utilization

- Key thoughts
  - New spectrum in the **mm wave** bands is a significant element in the technical discourse about 5G network. It will likely have an impact well beyond just cellular mobile networks. The mm wave early prototypes have crossed the speed threshold to be a viable access technology, accelerating the convergence of fixed and wireless networks.
  - 5G air interfaces are being designed with significant emphasis on **advanced beamforming** capabilities, primarily to support millimeter wave bands, but just as relevant in providing coverage using low centimeter wave bands. **Massive MIMO**, **advanced signal processing** and **adaptive antenna systems** will play a key role in serving fixed and mobile broadband use cases.
  - The availability of spectrum at the foundational lower frequencies is at a premium because of superior propagation and interaction with obstacles. With the limited spectrum available there are several paths to better utilization: (1) through frequency sharing or **densification**; and (2) through greater efficiency in exploiting the spectrum that is available through **spatial diversity**, **multi-path effects**, or **innovative signal processing and antenna technology**.
  - The introduction of **SDN** and **NFV** further provides 5G Networks with the agility and underlying technologies to master **spectrum sharing** and **mobility on demand** at a much more granular level than we have contemplated so far.

Awareness, Transparency and Openness

- Key thoughts
  - We don't know exactly what 5G will look like; given the 'softwarization' of the network, it will likely be rapidly-evolving and continuously changing
  - There is no overall architect of tomorrow's networks
  - Anticipation of consequences for critical services and common societal goals is hard to do
  - Goods and services delivered in our domestic marketplace are significantly and increasingly affected by the scale of the global market place
    - This includes the processes and practices that emerge from international standards bodies and from major actors in the supply chain
  - It is important for the FCC to have insight into the architectures that emerge
    - Sufficient capability to understand the impact and consequences so that our national goals are met, and to ensure that the voice of our stakeholders can influence outcomes

Societal Needs Examples

Legislatively Mandated or Widely Agreed Upon Public Policy Goals

- Next Generation 9-1-1 Services
- Disability Access
- Next Generation Enforcement*
- Lawful Intercept
- Network Security
- Public Safety/Mission Critical
- Outage/Performance Reporting
- Intellectual Property Protection (DRM)
- Privacy
- Transparency & Openness

Many of these may be impacted by programmable network and 4G+/5G internationally established architectures, standards and specifications

- both positive and negative impacts

* interference, spoofing, jamming, etc.

Other Relevant Societal Needs Examples

Application areas in which both 5G and programmable networks will play an important role

- Healthcare
- Education
- Environmental
- Transportation
- Smart Cities (and Villages)

Recommendations (for inclusion in Chairman's letter)

Understand - FCC establishes an 'excellence' program around future end-end networks & systems, combining targeting staff training and (SME) augmentation with regular structured workshops to harvest the latest industry and other agencies insights and expertise (academia, NGOs, appropriate stakeholders, …)

Re-assess - FCC undertakes an updated assessment of fundamental US societal needs, priorities for economic growth and organizational structure, informed by in-depth insight into industry impact of systemic SDN/NFV/Cloud technology-driven changes

Influence - FCC establish and maintain a living '5G watch list' of priorities and essential needs for the US market, and use that to guide a robust ongoing dialogue with industry to ensure that these needs are met in 5G-related standardization and specifications activities

Recommendation Specifics (1/3) [draft]

Understand - FCC establishes an 'excellence' program around future end-end networks & systems, combining key staff training and (SME) augmentation with regular structured workshops to harvest the latest industry and other agency insights and expertise

- Build up in-depth insights and understanding of SDN/NFV, 5G (NR and NG Core), and other technologies with significant network transformational impacts
- Leverage many sources for staff education, including industry groups (CTIA, 5GAmericas, ATIS, etc.) and TAC FGCT & NGI WG outputs and recorded sessions
- Expand technical staff with expertise in emerging cloud-driven networks and technologies
- Improvements to FCC staff training
  - Continual development of strategic curriculum by Bureaus/Offices emphasizing future end-end networks/ systems
  - Mandatory training requirements for general staff
- Prototype a methodology that could provide the Commission with an evergreen approach to reviewing market signals and earmarking select impactful evolving technologies
  - Begin with an experimental workshop, to be completed this Fall, partnering with the Institute For The Future

Recommendation Specifics (2/3) [draft]

Re-assess - FCC undertakes an updated assessment of fundamental US societal needs, priorities for economic growth and organizational structure, informed by in-depth insight into industry impact of systemic SDN/NFV/Cloud technology-driven changes

- Assess which societal needs remain a priority for the FCC to continue to defend
- Identify changes to the set of essential services and capabilities
- Assess what forms of new network innovation that the FCC wants to encourage to stimulate/maximize resulting economic growth in the US
- Consider FCC organizational structure changes that reinforces systems thinking, reflects emerging industry changes, and moves away from access technology silos

Recommendation Specifics (3/3) [draft]

Influence - FCC establish and maintain a living '5G watch list' of priorities and essential needs for the US market, and use that to guide a robust ongoing dialogue with industry to ensure that these needs are met in 5G-related standardization and open source activities

- Informed by above educational and assessment activities
- Leverage industry for two way learning and influence of 5G (and 4G evolution) standards directions
- Frequent enough regular interaction for timely response to changing standards situations but lightweight enough to be sustainable (3 times/year?)

FGCT WG Next Steps

- SME talks and use case analysis continuing throughout the year
- 5G/Satellite services for rural
- Emerging societal needs
- Plan and execute IFTF Workshop
- Assess and summarize additional scanned new technology areas
- Schedule for Key deliverables
  - December 2015
    - Results of initial trial of structured workshop approach
    - Final 5G and Programmable Networks whitepapers, briefings, and presentations
    - Refinement of Actionable Recommendations

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: September 20, 2016

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

broadband forum

verizon

5G

at&t

ITU-T Study Group 12

hulu

Consumer Technology Association™

COMCAST

Akamai

CONVIVA®

facebook.

Academic Researchers

Q3 Interviews

- Akamai, Comcast, Verizon, Conviva Facebook, BBF, & AT&T
- 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

WG In-Home Network QoS/QoE Findings

- Modern service delivery dependent on quality of in-home networks
  - In-home ”managed” by consumer, often with no experience or tools
- No public data is available on current measurements within the Home
- Few industry resources available for in-home measurement or self testing
- FCC does not have access to measurements beyond residential gateway
- Measurements within the home would help FCC, Service Providers, equipment makers, content providers and consumers understand constraints and areas for improvement
  - Unlicensed spectrum requirements (FCC)
  - Wi-Fi interference (Consumer, SP, FCC)
  - Impact due to number of devices or legacy equipment (Consumer, SP, FCC)
  - Evolution of services for future policy needs (FCC & Standards Bodies)
  - Reduce trouble tickets (Consumer, SP)

Observations on CDNs from presentations

- Two extremes of content delivery
  - The Superbowl live: everyone watching the same segments, but they can't be pre-positioned
  - A rainy Saturday: everyone wants to watch a different movie/TV show.
- Content/ Rights Owners building standalone CDN's
- Video stored as video segments (at multiple encoding rates) plus a manifest file
  - Different rates for different devices; adaptive change to lower rate segments under congestion
  - Different container standards for encoded segments multiplies segments that must be cached
  - Implementation of Common Media Application Format (CMAF) for segment containers has the potential to reduce caching burden
- Wireless Carriers transparently cache/transcode data to reduce bandwidth but increasing use of encryption precludes this
  - As caches move closer to consumer, less need for transparent caching
  - Proposals being worked to share keys/ deal with encryption
- Smaller communities less likely to see local caching.
  - Another form of digital divide?

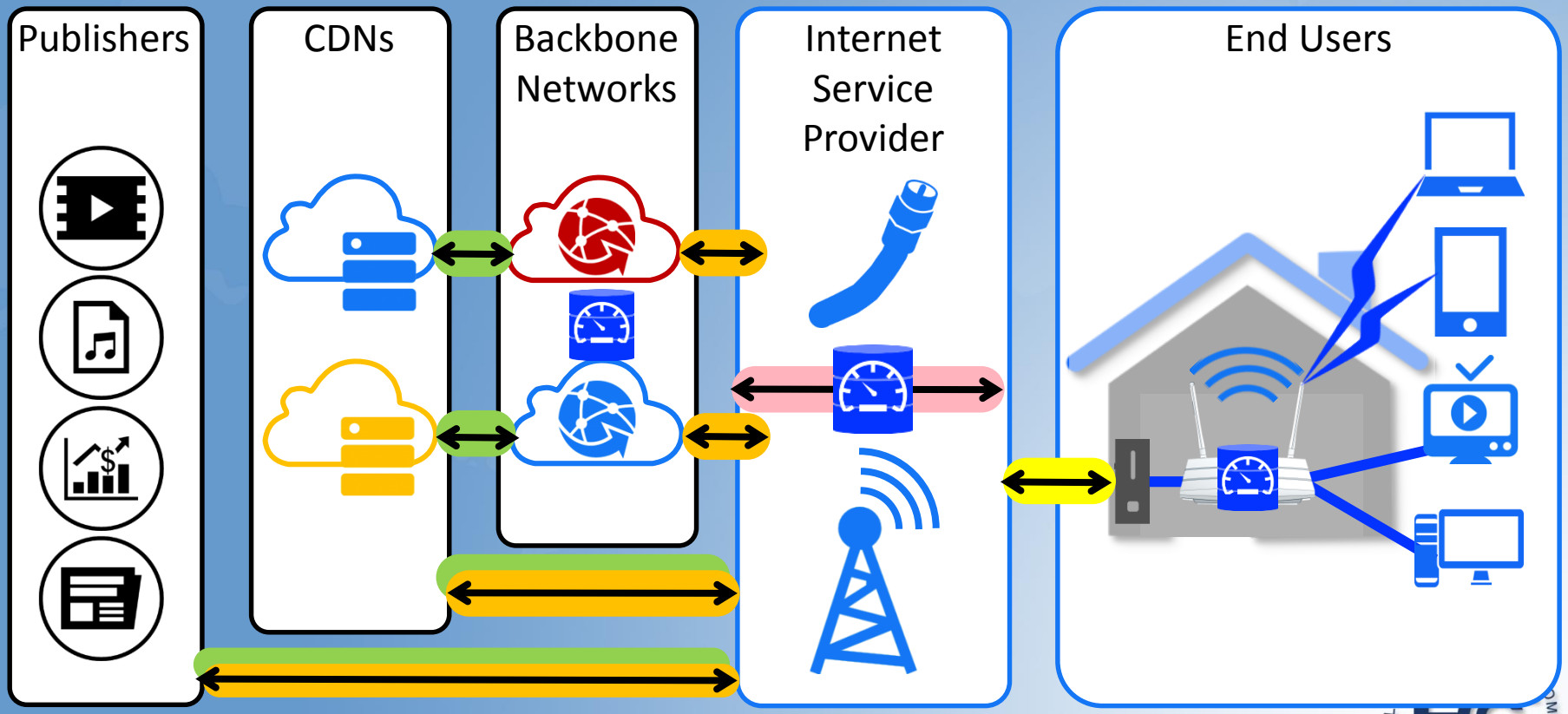
Observations on NG Internet Improvements and Efficiencies

- Significant Work being done to define the Future of the Internet
  - 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
- Key Concepts
  - Information-centric networking (ICN) is an approach to evolve the Internet infrastructure away from a host-centric paradigm based on perpetual connectivity and the end-to-end principle, to a network architecture in which the focal point is “named information” (or content or data).
  - Business models for ICN are not defined
- Industry Bodies –work being done by : ATIS, NSF
- Content and Coding mechanisms evolving to move efficiently support traffic
- Research on future NG-I architectures is focused on mobility, self-certifying identifiers, ICN and enhanced security
- Policy related issues: Consider the NN ruling as background
- Input fro[illegible]es

WG team focus in Q4 of TAC

QUALITY OF SERVICE, QUALITY OF EXPERIENCE

Expand MBA program to reflect granular QoS performance



CDN Performance
Interconnection Health
BIAS Cloud
BIAS Last Mile
Existing MBA

Guiding Principles for QoS Data Collection

- **Goal**:
  - Ability to observe the QoS performance of the Internet. By assessing the various complex network components and identifying where QoS issues exist and can be addressed
- **Target data collection objectives**:
  - 3rd party data contribution
  - Report directly from infrastructure, Autonomous
  - Fair, balanced and neutral
  - Voluntary participation
- **Areas for consideration**:
  - There is minimal E2E measurement being done today
  - Measuring segments provides better isolation of issues

What MBA does *not* Measure

- Enterprise Services
- ***Interconnect Health***
- Smaller Providers
- Rural/Smaller ISPs
- Anchor Institutions
- Network Reliability
- Network Resilience
- Network Availability
- Network Features
- ***QoS and QoE***
- Consumer Adoption
- Content Decisions
- ***CDN Performance***

Recommended QoS Measurement

Metric	Target Measurement Scope
Latency at Interconnect	Latency between border router of interconnect company and border router of ISP
Packet Loss, Packets Dropped	Measurement of packet loss (as percent of total traffic) between border router of interconnect company and border router of ISP (loss pattern)
Traffic Utilization	The traffic utilization (as a percent of capacity) between border router of interconnect company and border router of ISP
BIAS Latency	Measurement of packet latency between border router of ISP at interconnect point and CPE demark point
BIAS Packet Loss	Measurement of packet loss (between border router of ISP at interconnect point and CPE demark point)
BIAS Jitter	Measurement of jitter on packets (between border router of ISP at interconnect point and CPE demark point)
DNS Response Time	Time from user initiated query to the time of an authoritative response

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

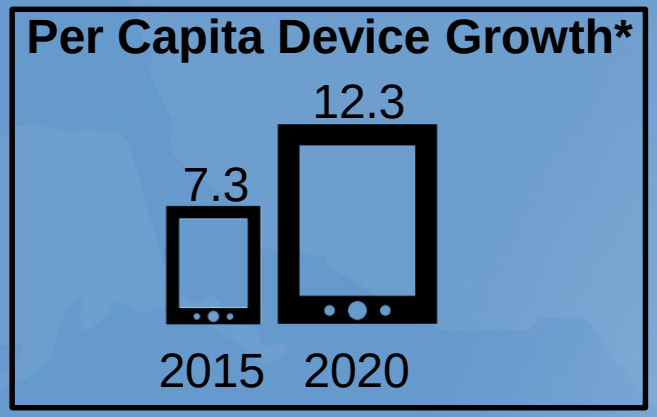
- QoE:
  - The commission should closely monitor work being done in standards bodies regarding Quality of Experience, particularly work done in ITU-T SG12 and IETF
  - Ultimately, QoE depends on end-user experience. The commission should seek a public/ private partnership to determine actual consumer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

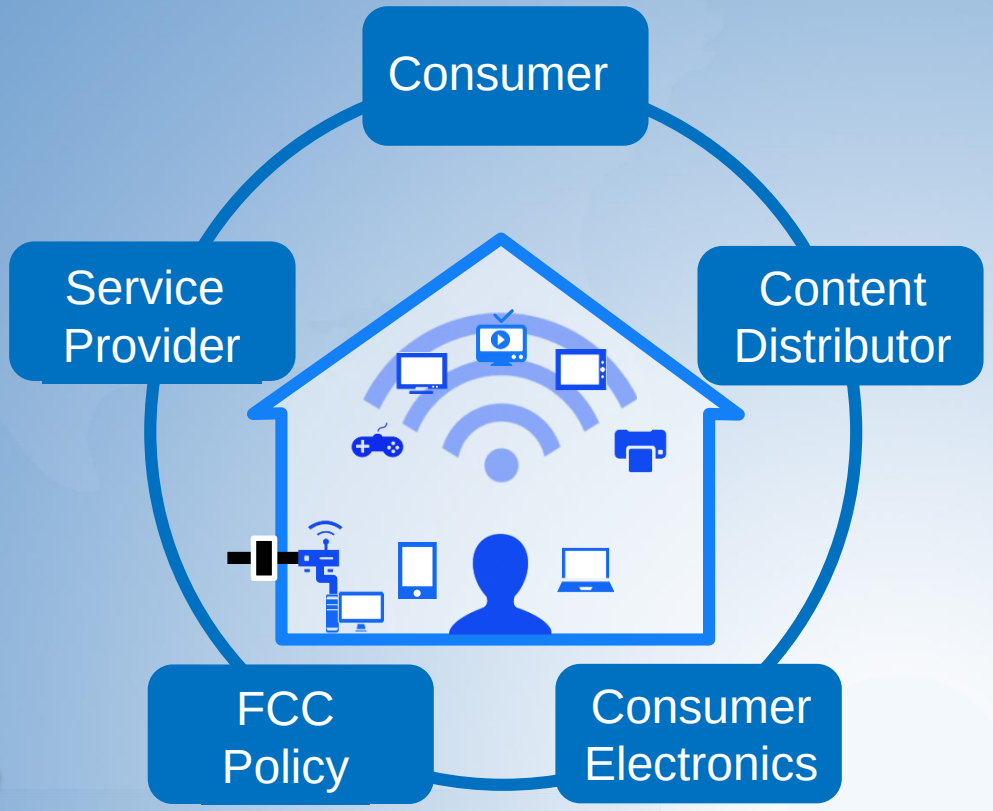
IN-HOME NETWORKS

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

- **Consumer device performance & troubleshooting tools**
- **SP: Remote management, trouble-shooting**
- **Content owners app performance**
- **Consumer electronics performance**
- **Policy: Trend data, usage data, etc**

* Source: Cisco VNI

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

Q4 Focus

- Deep dive on Internet Improvements and Efficiencies
- Work with FCC to further refine metrics recommendation

THANK YOU!

Availability- *Work in Progress*

- Availability includes multiple factors
  - Connectivity– IP Layer
  - Service activation/accessibility – DHCP/DNS response time
  - Busy Hour Performance
  - IoT will increase the availability requirement as devices are constantly producing data to monitor
- Availability metrics in a future broadband environment will be important
  - Standards bodies are pursuing and we recommend the FCC leverage that work
- Proposed Exclusions:
  - Power loss – From TAC perspective, availability should be measured when power is available. Excludes batter back-up issues and overlapping responsibilities between power/communication entities
  - Mobile networks: standards foundation emerging

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**

Technological Advisory Council

Spectrum and Receiver Performance

Working Group

September 20, 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
  - David Gurney, Motorola Solutions
  - Bruce Judson, Qualcomm

Topics

- Enforcement
  - Develop database of Enforcement activities for researchers
  - Jamming and Spoofing Protection
    - GPS
    - RF Signals in other services
- RF Noise Assessment
  - Noise Floor
  - Professional Interference Hunters

Enforcement

- In our ongoing examination of enforcement issues related to interference and noise:
  - We believe that a public record of past FCC enforcement activities would aid researchers in their development of more secure and efficient RF environments
- **Recommendation:**

  The Commission should create a comprehensive and unified publicly available <u>database</u> of past enforcement activities
- We have started to study another interference threat:
  - There are potentially disastrous effects from intentional RF interference that disables or spoofs GPS signals

RF Noise Assessment

- Research literature and measurements on RF noise floor changes
- Research FCC rules on RF emission limits
- Compare available measurement data from devices relative to current emission limits
- Research required noise floor for various radio service bands and assess RF environment contributions to noise floor(s)

Interference Hunters

- Interviewed three professional interference hunters:
  - Pericle Communications
  - Signal Finders
  - Ray Vincent
- Learned about typical interference complaints
  - How they are located
  - How they are resolved
- Discussed the lack of, and possibility for, creating a shared database of noise location methods and amelioration techniques

RF Noise Assessment

- In search of answers to the study of noise from the general public, we issued a TAC Technical Inquiry that asked for detailed answers to the following broad questions:
  - Is there a noise floor problem?
  - Where do problems exist (spectrally, spatially, temporally)?
  - Is there quantitative evidence of harmful interference from noise?
  - How should a noise study be performed?
- FCC ET Docket 16-191 was posted on the FCC Website on 6/15/2016 and accepted public responses until 8/11/2016.

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

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

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.

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 73 different people/entities.
  - 93 submissions to ECFS, some duplicates
  - 7 direct submissions to the committee by email are not in ECFS
- The breakdown on responders (with some overlap between groups):
  - 23 Companies/Industry Organizations.
  - 39 RF Professionals.
  - 31 Licensed Radio Amateurs.
  - *9 Responders did not reply to the questions asked.*

Responding Entities

- ARRL (Amateur Radio)
- NAB (Broadcast)
- SBE (Broadcast)
- DTS Inc (Broadcast)
- Wisconsin Public Radio (Broadcast)
- V-Soft (Broadcast)
- CTIA (Cellular)
- AT&T Services (Cellular)
- Verizon (Cellular)
- NPSTC (Public Safety)
- Calif Office Emerg Serv (Public Safety)
- Pericle Communications (Noise Hunter)
- GPSIA (GPS)
- Deere and Company (GPS)
- Exacter, Inc (Power Lines)
- Shure Inc
- Cohen, Dippell & Everest
- EM Radiation Policy Institute
- Ingenious, Inc.
- NEMA (Lighting)
- Philips Lighting (Lighting)
- American Lighting Assoc (Lighting)
- LHW Consulting

Technical Inquiry Responses

- In the Technical Inquiry, we did not necessarily ask for answers
  - Rather, we asked for opinions on how the answers could be obtained
- We received a broad sampling of opinions:
  - 26 responders provided quantitative or semi-quantitative data
  - 8 responders suggested ways in which the subject could be studied
  - Most responders opined on what they believe are the major sources of noise

Technical Inquiry Responses

- Incidental and Unintentional Radiators were the most commonly cited noise sources
  - RF Lighting and Power Lines were often mentioned
  - Switching Power Supplies were identified as problems
- Affected frequencies were distributed across the bands between MF, HF, VHF and UHF
  - Trend was higher noise levels at lower frequencies
  - Evidence was presented of increasing noise levels at UHF and higher; is this a trend?

Technical Inquiry Responses

- Indications of aggregation of noise sources that resulted in harmful interference
  - Individual devices met standards but the aggregate was significantly above regulatory limits
- Several responders blamed insufficient enforcement
  - Other responders suggested that allowable radiated noise limits in the regulations are too high.
- Virtually all responders felt that a comprehensive noise study is needed

What's Next?

- Interesting omissions in the responses:
  - No University Researchers responded to the docket
  - No other government agencies responded
  - There were no comments submitted from the satellite industry
- We would like to better advertise the Technical Inquiry to those communities and get their input
- An extended Comment Period for the docket from September 22 to October 21 would give them 4 additional weeks to submit comments

What's Next?

- A complete report describing the responses will be presented at the December 7, 2016 TAC Meeting
  - Several actionable recommendations based on the responses will be included with that report
- Anyone who would like to view the responses received by the Electronic Comment Filing System should go to:

  https://www.fcc.gov/ecfs

  and in the "Specify Proceeding" field, enter: 16-191
  - *Some responses were sent by email to the S&RP Subcommittee and are not available on ECFS*

THANK YOU