Technical Advisory Council
Federal Communications Commission
Summary of Meeting
December 9th, 2015

The Technical Advisory Council (TAC) for the FCC was convened for its nineteenth meeting at 12:30 P.M. on December 9th, 2015 in the Commission Meeting Room at the FCC headquarters building in Washington, DC. A full video transcript of the meeting is available at the FCC website at http://www.fcc.gov/encyclopedia/technology-advisory-council together with a copy of all materials presented at this meeting. In addition, all materials presented at this meeting are included in electronic form in an Appendix to this document.

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

## Council present:

| | |
|---|---|
| John Barnhill, Genband | Steve Lanning, Viasat, Inc. |
| Mark Bayliss, Virginia ISP Association and the West Virginia Broadband CO-OP | Gregory Lapin, American Radio Relay League |
| Nomi Bergman, Bright House Networks | Brian Markwalter, Consumer Electronics Association |
| John Chapin, Special Government Employee | Tom McGarry, Neustar |
| Lynn Claudy, National Association of Broadcasters | Milo Medin, Google, Inc |
| Marty Cooper, Dyna LLC | Geoffrey Mendenhall, GatesAir |
| Brian Daly, AT&T | Lynn Merrill , NTCA |
| Pierre De Vries, Special Government Employee | Jack Nasielski, Qualcomm Inc. |

| | |
|---|---|
| Adam Drobot, OpenTechWorks | Ramani Pandurangan , XO Communications |
| Erik Ekudden, Ericsson | Mark Richer, Advanced Television Systems Committee, Inc. |
| Jeff Foerster, Intel Corporation | Dennis Roberson, Wireless Network and Communications Research Center |
| Dick Green, Liberty Global, Inc | Marvin Sirbu, Special Government Employee |
| Russ Gyurek, Cisco Systems | Kevin Sparks, Alcatel-Lucent |
| Dale Hatfield, Silicon Flatirons Center for Law, Technology, and Entrepreneurship University of Colorado at Boulder | Paul Steinberg, Motorola |
| Theresa Hennesy, Comcast Corporation | David Tennenhouse, VMWare |
| Farooq Kahn, Samsung | David Young, Verizon |

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

| |
|---|
| Scott Jordan |
| David Simpson |

## Meeting Overview

Dennis Roberson, TAC Chairman, began the meeting asking the TAC members to introduce themselves. He noted that the TAC work groups faced this year a very broad and important set of topics and that although a ½ hour had been added to the time for the meeting it began apparent when trying to schedule the reviews how much work had been covered over the year. Correspondingly, the TAC members had grown to 49 with the addition of 82 non-TAC members in individual work groups. There are 20 FCC liaisons work with the various work groups for a total of 151 participants.

Each TAC Work Group chairperson next provided a summary of their work activities for the year together with final recommendations. A white paper for the Cybersecurity workgroup was recommended to be tabled for further work after some discussion.

The meeting concluded with a discussion of a draft schedule for 2016 meeting and with Dennis Roberson thanking all members for their contributions and noting that TAC recommendations need to be approved by the Chairman. He thanked the working group Chairs and sub-chairs for the efforts they had expended over this past year.

A copy of all presentations is attached herein.

# FCC Technological Advisory Council

December 9th, 2015

# Agenda

| | |
|---|---|
| Introduction | 12:30 PM |
| Spectrum and Receiver Performance Work Group | 12:35 PM |
| Cybersecurity Work Group | 1:05 PM |
| NG Internet Services Work Group | 1:35 PM |
| Future Game Changing Technologies Work Group | 2:05 PM |
| Roadmap for Future Unlicensed Services | 2:35 PM |
| Mobile Device Theft Prevention Work Group | 3:05 PM |
| 477 Testing Work Group | 3:35 PM |
| 2016 Work Program Discussion | 3:45 PM |

## TAC Resources

- TAC Members: 49
- Non-TAC Work Group Participants: 82
- FCC Liaisons: 20
- Total: 151

- Contributions/viewpoints of many individuals interviewed by TAC work groups

# A Look Back – 2014 Recommendations

- The FCC TAC recommended that the FCC establish a national framework for smartphone anti-theft measures ✓
  - Work is detailed, involves multiple organizations and commitments and is based on partnering with industry
- FCC focus on Core Network Security Equipment Recommendations ✓
  - Spawned a number of activities in CSRIC and ongoing discussions
- IP Transition: Analysis of rural transition issues ✓
  - FCC established trials of rural broadband deployment strategies
- IOT recommendations on use of unlicensed spectrum and security concerns ✓
  - FCC focusing on increase spectrum unlicensed spectrum opportunities: 3.5Gz, 5 Ghz, mm bands
  - FCC focusing on IOT security concerns both thru TAC and CSRIC

# A Look Back – 2014 Recommendations

- Interference Resolution and Enforcement ✓
  - Straw man proposal incorporating TAC recommendations in discussion with CSMAC, increasing collaboration with other federal agencies
  - Increasing focus on Risk Informed assessment
    - FCC staff training on risk analysis methods
- Make additional spectrum available for sharing ✓
  - Major emphasis now placed on identifying spectrum sharing opportunities and technologies to support sharing
- Additional Spectrum, IOT, New Spectrum Frontiers (2013) ✓
  - FCC issued NPRM on mm wave bands (5G) 10/15

# Technological Advisory Council

## Spectrum and Receiver Performance

### Working Group

### December 9, 2015

# 2015 Mission

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

# Working Group

- **Chair:**
  - Lynn Claudy, NAB
  - Greg Lapin, ARRL
- **FCC Liaisons:**
  - Julius Knapp
  - Uri Livnat
  - Bob Pavlak
  - Matthew Hussey
- **Participants / Contributors:**
  - Dale Hatfield, University of Colorado
  - Pierre de Vries, Silicon Flatirons
  - Brian Markwalter, CEA
  - David Gurney, Motorola Solutions
  - Steve Kuffner, Motorola Solutions
  - Geoff Mendenhall, GatesAir
  - Robert Dalgleish, Ericsson
  - Kumar Balachandran, Ericsson
  - Robert Miller, incNetworks
  - Bruce Judson, Qualcomm
  - Dave Pehlke, SkyWorks
  - Scott Burgett, Garmin

# Working Group Areas of Focus

- Develop recommendations about statistics of interference and risk-informed decision making
- Propose basic principles for assessing compatibility for spectrum allocations
- Recommend strategies for interference resolution and enforcement in a changing RF environment

# Risk-Informed Interference Assessment

- Key concepts
  - Risk triplet: What can go wrong? How likely is it? What are the consequences?
  - Risk-informed interference assessment: Quantitative analysis of the likelihood & consequence of interference hazards, e.g. to incumbent from planned radio service → better trade-offs
- Story so far
  - April 2015 TAC paper outlined method; recommend that FCC begin developing expertise
  - TAC WG has used MetSat/LTE coexistence in AWS-3 to test proposed method
  - Working group report being presented for approval today

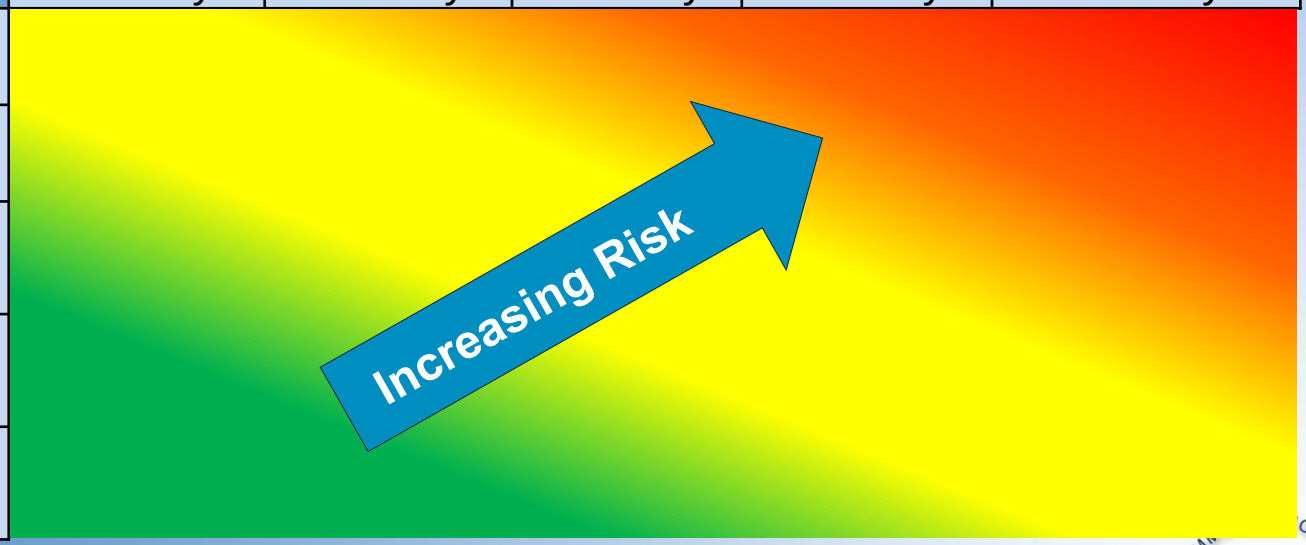
# Risk-Informed Interference Assessment

- MetSat/LTE interference case
  - Build on analysis done by CSMAC WG-1
  - Polar satellite earth stations
  - “Sea” of LTE mobiles co-ch. and adj. band

- Method
  1. Make inventory of hazards including interference modes and interference parameters
  2. Define consequence metric: ITU-R SA.1026 “long-term” and “short-term” interference protection criteria (IPC)
  3. Assess likelihood & consequence for various interference modes using Monte Carlo modeling

# Generic Risk Chart

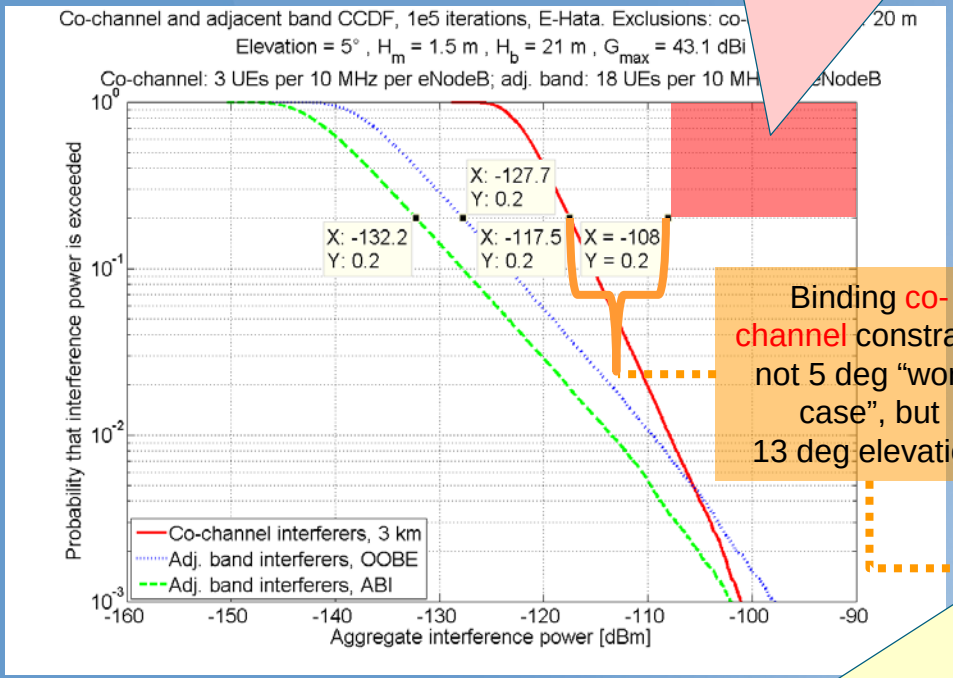
| | | Consequence | | | | |
|---|---|---|---|---|---|---|
| | | Very Low Severity | Low Severity | Medium Severity | High Severity | Very High Severity |
| Likelihood | Certain | | | | | |
| | Likely | | | | | |
| | Possible | | | | | |
| | Unlikely | | | | | |
| | Rare | | | | | |



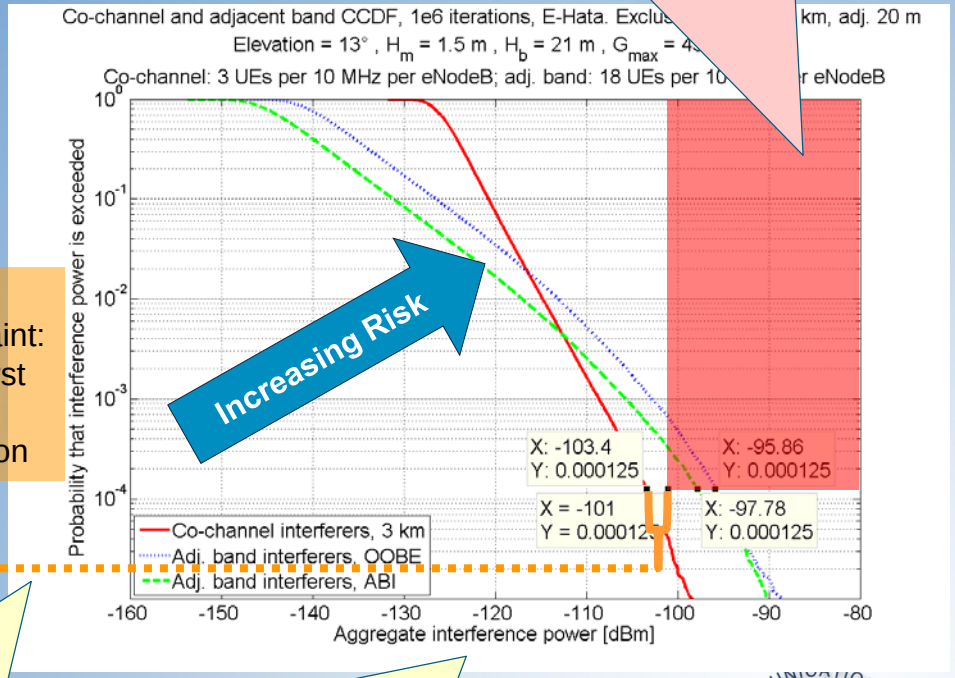
# Results: Co-ch and adj. band interferers

Long-term IPC (5 degree elev'n):
NTE -108 dBm > 20% of time

Short-term IPC (13 degree elev'n):
NTE -101 dBm > 0.0125% of time




Binding co-channel constraint: not 5 deg "worst case", but 13 deg elevation




Likelihood: Exceedance probability

Consequence: Aggregate interference power

# Conclusions

1. Method proposed in the TAC risk paper can be successfully applied to a real-world case
   - can combine fixed values and probability distribution
   - can incrementally add sophistication: location variability, ACLR
2. Yields useful insights, e.g. binding constraint is not 5 degree elevation, but 13 degree case
3. Statistical protection criteria (combine interfering signal level with exceedance probabilities) very helpful in risk assessment
4. Analysis was constrained by
   - unavailability of baseline performance data
   - inadequate ITU-R documentation of methods and values

## We recommend that the FCC:

1. Continue to pursue adoption of risk-informed interference assessment as described in April 2015 TAC paper
2. Adopt statistical service rules more widely in order to support future risk analysis
3. Encourage services seeking protection to disclose baseline system performance information
4. Encourage all parties to disclose methods underlying interference criteria and coexistence assessments

# Basic Principles for Assessing Compatibility of New Spectrum Allocations

- Presents principles to aid the Commission in the allocation of frequencies to services
- The principles apply to incumbent users of the spectrum, new entrants desiring spectral space, and regulators
- When followed they provide maximally efficient use of limited spectrum
- Requesting TAC approval for white paper

# Basic Principles for Assessing Compatibility of New Spectrum Allocations

- The principles do not propose “One Size Fits All” policies
- Instead they aim to facilitate the most efficient application of frequency allocations to realize the most effective communications in the face of interference
- ***Harmful Interference*** is not redefined, but it is envisioned more concretely

# Nine Principles in Three Categories

- Interference Realities
  - What users of the spectrum should expect in terms of interference
- Responsibilities of Services
  - What systems should do to minimize the effects of interference
- Regulatory Requirements and Actions
  - Information needed to result in the most compatible allocations of spectrum

# 1st Category: Interference Realities

- Interference exists – A fact of physics
- No service should expect to inhabit perfectly silent frequencies
- All services should expect that the interference they experience today is not likely to be the interference that they will be faced with tomorrow
- Whether or not interference becomes “Harmful” depends on the actions of all services involved

**<u>Principle 1</u>: *Harmful interference is affected by the characteristics of both a transmitting service and a nearby receiving service in frequency, space or time***

- Interference can become harmful or not due to changes by the transmitter or the receiver
- Interference between two services is affected by:
  - How much spectrum is placed between them,
  - How much physical space is placed between them,
  - If services can coordinate their operations to occur at different times

**<u>Principle 2</u>: *All services should plan for non-harmful interference from signals that are nearby in frequency, space or time, both now and for any changes that occur in the future***

- Today's interference may not be tomorrow's interference
- As new entrants are introduced to the spectrum, existing conditions are bound to change
- Planning ahead for future changes will make it easier to deal with changes when they occur

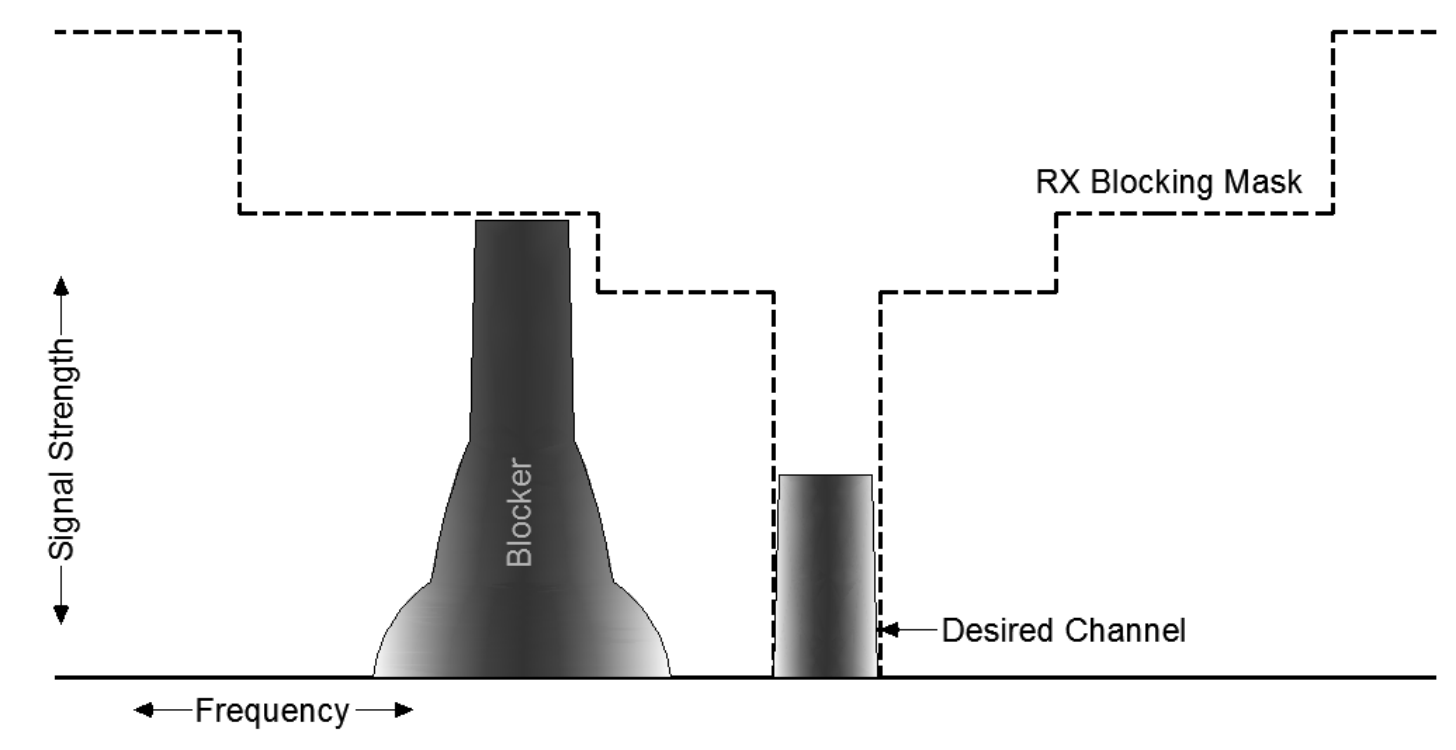
**<u>Principle 3</u>: *Even under ideal conditions, the electromagnetic environment is unpredictable. Operators should expect and plan for occasional service degradation or interruption. The Commission shall not base its rules on exceptional events***

- Propagation changes
- Intermodulation effects can be transient
- The conditions over a majority of the time must be used to set policy

# 2nd Category: Responsibilities of Services

- The FCC does not provide a Brick Wall to separate services
- Neighboring services must be Good Neighbors
- Methods that allow more closely spaced services while maintaining an acceptable interference environment should be used whenever possible
- We need to keep in mind that some services exist because of low cost devices, which may not be compatible with advanced interference avoidance

# <u>Principle 4</u>: *Receivers are responsible for mitigating interference outside their assigned channels*

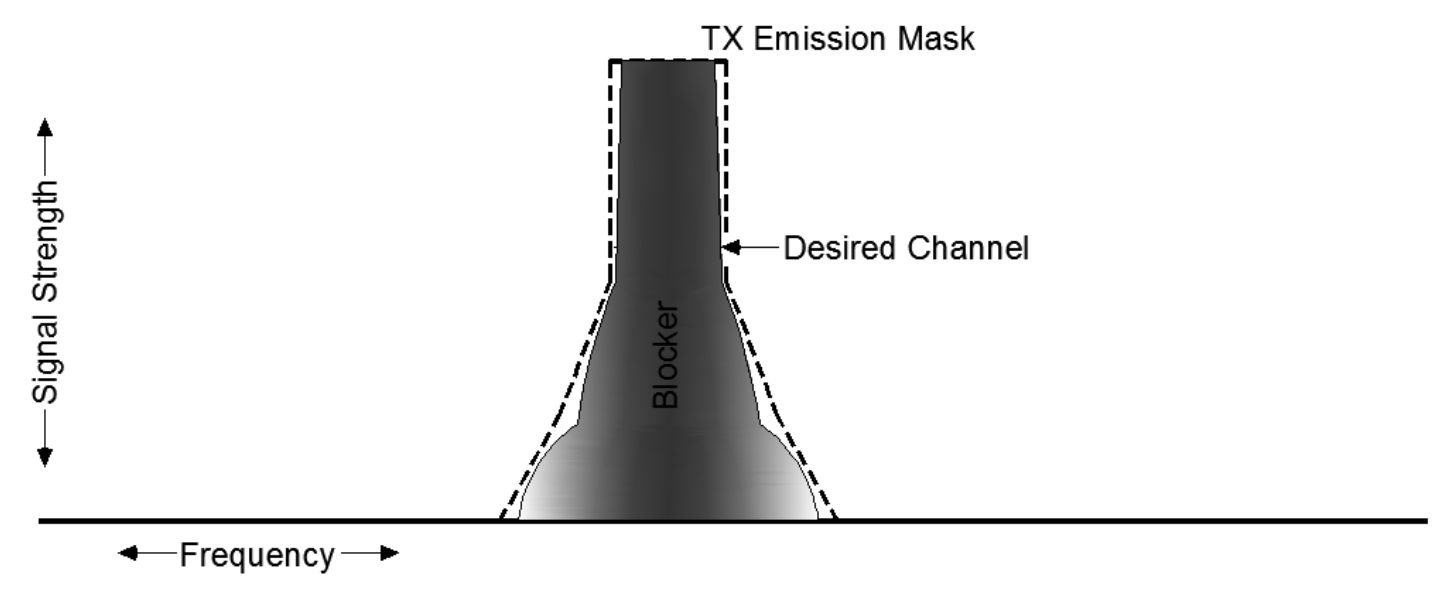


**<u>Principle 5</u>: *Systems are expected to use techniques at all layers of the "stack" to mitigate degradation from interference***

**<u>Examples Include</u>:**

- Directional Transmission
- Directional Reception
- Multi-input multi-output (MIMO) antenna systems
- Power Control
- Frequency hopping or spreading
- Adaptive Modulation and Coding
- Channel Codes
- Advanced receivers
- Time Interleaving
- Retransmission
- Scheduling

**<u>Principle 6</u>**: ***Transmitters are responsible for minimizing the amount of their transmitted energy that appears outside their assigned frequencies and licensed areas***



# 3rd Category: Regulatory Requirements and Actions

- The allocation of spectrum can be made intelligently if sufficient information about the services is available
- If the societal goal is to maximize use of the spectrum, then minimizing guard bands while keeping an acceptable interference environment is key

**<u>Principle 7</u>: *Services under FCC jurisdiction are expected to disclose the relevant standards, guidelines and operating characteristics of their systems to the Commission if they expect protection from harmful interference***

- The FCC needs full details about the operation of services to make informed decisions
- The FCC can't be expected to be as effective in avoiding interference without adequate information about the services involved

## Principle 7: *Disclosure…*

- Each service needs to define a minimum expectation of its performance so that the FCC can make allocations in order to prevent interference from becoming harmful to that service
- Services should realize that if they do not want to, or cannot, make full disclosure they are preventing the FCC from helping them
- Suggest licensee community-of-interest cooperation using Internet-based secure clearinghouse to assist FCC and speed selective interference mediation

**<u>Principle 8</u>: *The Commission may apply Interference Limits to quantify rights of protection from harmful interference***

- Two TAC papers on Interference Limits have been published in 2013 and 2014:
  - https://transition.fcc.gov/bureaus/oet/tac/tacdocs/WhitePaperTACInterferenceLimitsv1.0.pdf
  - https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/TACInterferenceLimitsIntrov1.0.pdf
- The Commission will need enough information to determine Interference Limits for services

**<u>Principle 9</u>: *A quantitative analysis of interactions between services shall be required before the Commission can make decisions regarding levels of protection***

- Standard modeling should be used by all services.
- A clear statement of assumptions and initial conditions must be provided
- The FCC should have enough detail so that the models can be reproduced
- Models of adjacent services should be harmonized into a single set of calculations

## <u>Principle 9</u>: *Quantitative analysis …*

- Transparency and Reproducibility of calculations are of key importance
  - Any interested party that wants to reproduce the results should have access to all of the information needed to do so
  - This is the best way to insure that modeling results are correct

# Basic Principles – Summary & Recommendation

- It is in the best interests of society that spectrum be utilized in the most efficient and effective manner
- Following nine basic principles will lead to the best allocations of frequencies for both the interests of society and effectiveness of the services
- **The TAC recommends that the Commission adopt these nine principles in its future deliberations of frequency allocations to new services**

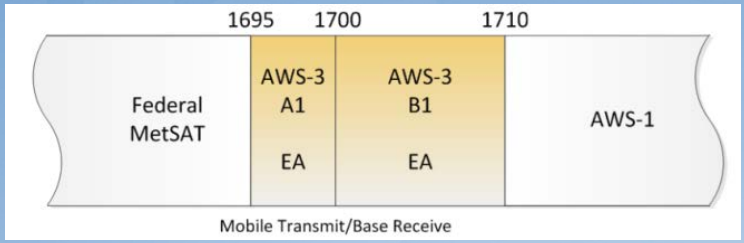
# Interference Resolution and Enforcement

- **Develop Statement of Work**
  - "Study to Develop a Next Generation System Architecture for Interference Resolution and Enforcement"
  - Document the traditional radio system environment
  - Study and document changing environment and associated challenges (for enforcement)
  - Identify, analyze and document improved enforcement capabilities
  - Identify current and evolving interference resolution and enforcement requirements
  - Develop a next generation systems architecture for interference detection, classification/identification, location, resolution, reporting and enforcement

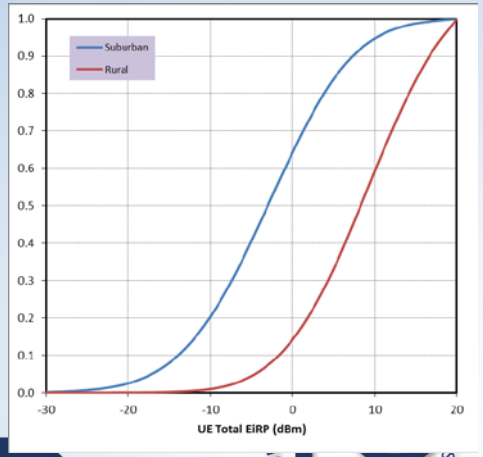
# THANK YOU

# Backup

# Step 1 : Inventory of Hazards




- Hazards
  - Non-interference hazards: desired signal fluctuation, component failure, human error
  - Co-channel interferers: LTE mobiles outside exclusion zone
  - Frequency-adjacent interferers: AWS-1 – no exclusion zone; considered OOBE, ABI; ignored intermodulation, spurious
- Interference determinants
  - Tx characteristics: location, EIRP, ACLR
  - Rx characteristics: noise figure, elevation, ACS
  - Transmitter/receiver coupling: antennas and propagation loss



## Step 2 : Consequence Metric

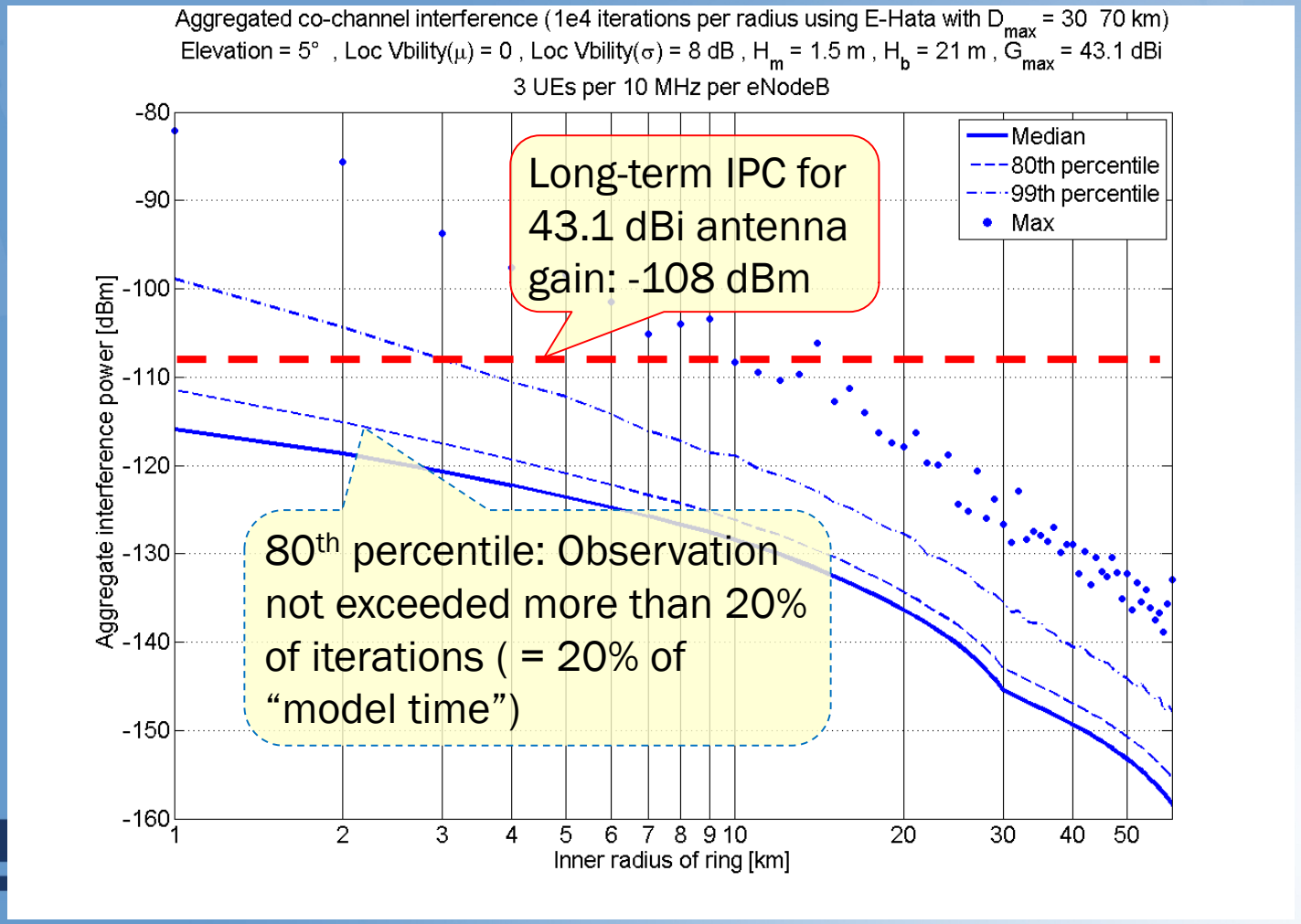
- Metric classes
  - Corporate metrics: ability to complete mission, increased capital expenditure, loss in revenue or loss of profit, …
  - Service metrics: e.g. availability (link % of time), quality (BER)
  - RF metrics: interfering signal level, I/N, SINR, …
- Use ITU-R SA.1026-4 interference protection criteria (IPC)
  - Long-term: IX power NTE > 20% of time, 5° antenna elevation
  - Short-term: IX power NTE > 0.0125% of time, 13° elevation
- For a 43 dBi antenna and 1.33 MHz receiver BW modeled
  - Long-term IX threshold power: -108 dBm
  - Short-term IX threshold power: -101 dBm

# Step 3 : Calculate likelihood/consequence

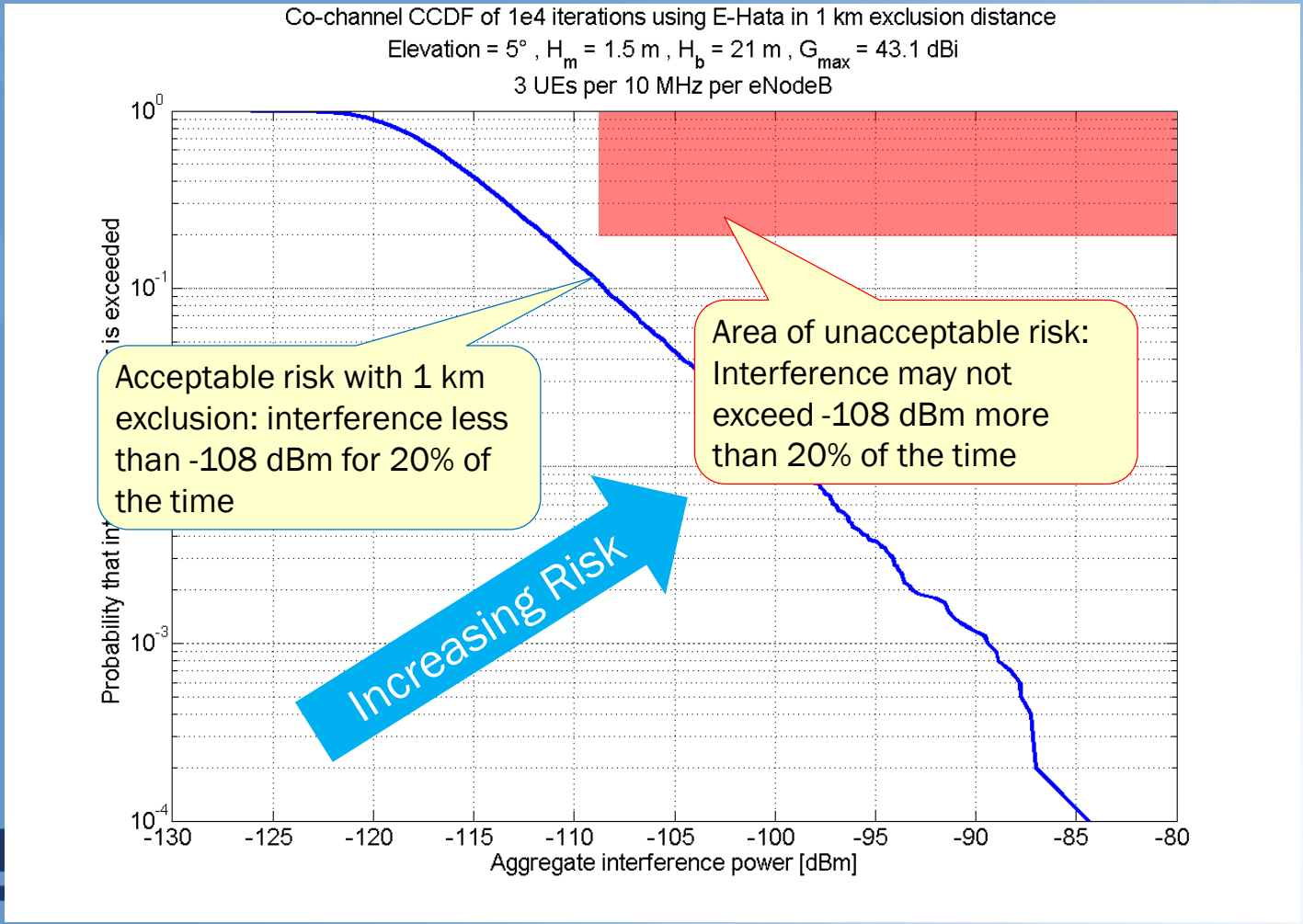
- Co-channel: Long-term and short-term protection
- Adjacent band interferers: OOBE and ABI
- Probability distributions used in Monte Carlo modeling:

| Variable | Properties |
|---|---|
| **UE transmit power** | EIRP distributions for suburban and rural deployment |
| **UE location** | Randomly sampled in the plane with suburban or rural density |
| **Path loss location variability** | Beyond 1 km: zero mean log-normal distribution with 8 dB standard deviation<br>Less than 1 km: zero mean log-normal distribution with standard deviation interpolated as a function of distance between 0 dB at 20 m and 8 dB at 1 km |
| **ACLR** | Uniform distribution between 30 and 40 dB |

# Co-channel, long term interference



# Long-term: co-channel i/f exceedance, 1 km



# Cybersecurity Working Group

| | |
|---|---|
| Chairs: | Shahid Ahmed, Paul Steinberg |
| Vice Chair: | Ramani Pandurangan |
| FCC Liaisons: | Jeffery Goldthorp, Padma Krishnaswamy, Ahmed Lahjouji |

9-December-2015

# Working Group Members

- WG Chair: Shahid Ahmed, PWC / Paul Steinberg, Motorola Solutions
- Vice Chair: Ramani Pandurangan, XO Communications
- FCC Liaisons: Jeffery Goldthorp, Ahmed Lahjouji, Padma Krishnaswamy
- Members:
  - John Barnhill, Genband
  - Mark Bayliss, Visualink
  - Nomi Bergman, Brighthouse
  - Mike Bergman, CTA
  - John Brzozowski, Comcast
  - Ken Countway, Comcast
  - Brian Daly, AT&T
  - Renato Delatorre, Verizon Wireless
  - John Dobbins, Earthlink
  - Martin Dolly, AT&T
  - Dale Drew, Level 3 Communications
  - Adam Drobot, Open Tech Works
  - Amit Ganjoo, ANRA Technologies
  - Dick Green, Liberty Global
  - Craig Greer, Samsung
  - Russ Gyurek, Cisco
  - Theresa Hennesy, Comcast
  - Farooq Kahn, Samsung
  - Dr. Prakash Kolan, Samsung
  - Tom McGarry, Neustar
  - Paul Misener, Amazon
  - Jack Nasielski, Qualcomm
  - George Popovich, Motorola Solutions
  - Katrin Reitsma, Motorola Solutions
  - Christoph Schuba, Ericsson
  - S Rao Vasireddy, Alcatel Lucent
  - Jack Waters, Level 3 Communications
  - Brian Witten, Symantec
  - David Young, Verizon Wireless
  - Lim Youngkwon, Samsung

# Sub-Working Group Activities

1. Simplifying Smartphone Security
   A. Requirements for Consumer-friendly Interface/Wizard for Security Configuration (Leaders: Martin Dolly, Renato Delatorre)
   B. Requirements for Smartphone Security Checker (Leaders: Amit Ganjoo, Katrin Reitsma)
2. Applying security to IoT Consumer Products (Leaders: Tom McGarry, George Popovich)
3. Securing SDN (Leaders: Ramani Pandurangan, Rao Vasireddy)

# 1. Simplifying Smartphone Security

**(1a: Requirements for Consumer-friendly Interface/Wizard for Security Configuration)**

- **Scope and Approach**
  - Develop platform agnostic baseline security controls, recommended settings and common vernacular for reporting on device security and application permissions.
- **Key actionable deliverables**
  - Step 1: Options (low hanging fruit) to connect the published security questions (CAC) published online into the mobile experience (not automation)
  - Step 2: Requirements for a 'wizard' approach to facilitate mobile device security configuration for users
- **Contributors**
  - Brian Daly, AT&T
  - Martin Dolly, AT&T
  - Renato Delatorre, Verizon
  - Amit Ganjoo, ANRA Technologies
  - Dr. Prakash Kolan, Samsung
  - Katrin Reitsma, Motorola Solutions
  - Lim Youngkwon, Samsung

# 1. Simplifying Smartphone Security

**(1a: Requirements for Consumer-friendly Interface/Wizard for Security Configuration)**

- **Recommendations**
  - Recommendation 1: Follow up with other key stakeholders
    - Device Vendors – Samsung, Sony, HTC, Apple, LG, etc.
    - Mobile OS representation – Google / Android, Apple / iOS, RIM / Blackberry, Microsoft / Windows Phone, alternative mobile OSs – e.g. FireOS, Sailfish, Firefox OS, Ubuntu, Tizen
    - Carriers – AT&T, Verizon
    - Security Solution providers – Lookout, NQMobile, Symantec, Intel
    - Device OEMs– Broadcomm, AMD, Qualcomm, TI, Freescale, Marvell

# 1. Simplifying Smartphone Security

## (1b: Requirements for Smartphone Security Checker)

- **Scope and Approach**
  - Derive and document requirements and development guidelines for a security checker application. The app helps consumers to configure security settings on their personal smartphones in a quick and user-friendly way according to best industry practices and reflecting individual security needs. The app is first launched during device setup and can be re-visited to make changes to security settings or view the current security status of the device.
  - Target audience is FCC and OS vendors as well as any party involved in the development, provisioning/hosting, and maintenance of the security checker app

- **Contributors**
  - Amit Ganjoo, ANRA Technologies
  - Katrin Reitsma, Motorola Solutions
  - Alex Abey, Lookout
  - Andrew Hoog, Now Secure
  - Andy Banks, Citrix
  - Youngkwon Lim, Samsung
  - Martin Dolly, AT&T
  - Renato Delatorre, Verizon

# 1. Simplifying Smartphone Security

## (1b: Requirements for Smartphone Security Checker)

- **Key Accomplishments**
  - Created a White Paper on Requirements and Guidelines for a Security Checker Application
- **Whitepaper Key Findings**
  - Key design decisions for the security checker app in:
    - App launched during initial on boarding and can be revisited later (both to modify security configurations or view the current device security status)
    - Two possible app architectures 1) fully native or 2) client/server
    - Intro questionnaire desirable for quicker & simpler security configuration
    - Use survey results to recommend appropriate security level and calculate security score
    - Use of 4-tier security levels (no/low/medium/high) for easier/faster configuration as well as easier overview of current device security status
    - Expose calculated security score to other apps using underlying OS communication framework
    - Examples for each security level of every covered security feature provided
  - Provided recommendations cover:
    - OS-based and 3rd-party security features
    - Enforceable security features that can be configured by app
    - Non-configurable security features which status should be viewable in the app

# 1. Simplifying Smartphone Security

## (1b: Requirements for Smartphone Security Checker)

- **Recommendations Summary for FCC**
  - Get mobile OS vendors (at least Apple and Google) involved for feedback and support with implementation
  - Identify suitable partners for the development, deployment and maintenance of the security checker following the provided requirements and guidelines
  - Recommend a focus group (e.g., CAC) develop an intro questionnaire and derive more detailed guidelines, based on user research, in terms of what would be an acceptable user experience for various security levels (none, low, medium, high).
  - Form a team to investigates technical feasibility of recommendations for all considered platforms (use provided WP Appendix as a starting point for this work)

# 1. Simplifying Smartphone Security

- **Suggestions for Future Work**
  - We recommend continuing the work as part of a FCC SWG only if OS vendors (or other suitable parties that offer to implement the checker) serve as contributing members (likely as chairs)
  - Once a security checker app has been implemented, another SWG could be tasked to verify whether the app meets the requirements and guidelines defined by this year's WG
  - If no party can be found to implement the checker as defined by this year's group, it could be desirable to design an intermediary solution (somewhere between a native app and wizard). For example, an app that guides users to configure their device on their own but does not enforce or display any security settings itself. Such a solution would be less desirable from a user experience, and would have the same maintenance requirements as a native security checker. However, the initial implementation of such a solution, while labor intensive, would be easier from an OS support point of view. Since requirements for such a solution have been already defined this year, such an approach rather lends itself to contracting someone to implement the app rather than having another FCC TAC SWG work on this

# 2. Applying Security to Consumer IoT Devices

- **Scope and Approach**
  - The WG will examine the special cybersecurity challenges posed by the emerging Internet of Things, and suggest actionable recommendations to the FCC with particular focus on the security and protection of IoT consumer products.
  - WG 2015 phasing
    - Q2: IoT security initiatives industry scan
    - Q3: Gap analysis, recommendations preview, and progress on the categories of **1) communication networks, 2) IoT devices, 3) best practices**
    - Q4: Recommendations addressing the takeaways and identified gaps from the Q3 update
- **Contributors**
  - Mike Bergman, CTA
  - John Brzozowski, Comcast
  - Renato Delatorre, Verizon Wireless
  - Martin Dolly, AT&T
  - Brian Daly, AT&T
  - Craig Greer, Samsung
  - Russ Gyurek, Cisco
  - Tom McGarry, Neustar (co-lead)
  - George Popovich, Motorola Solutions (co-lead)
  - Christoph Schuba, Ericsson
  - Brian Witten, Symantec
  - Peter Davis, Neustar
  - Brian Russell, Cloud Security Alliance
  - John Yeoh, Cloud Security Alliance

# 2. Applying Security to Consumer IoT Devices

**Key Accomplishments**

- Created a White Paper that covers FCC questions and subcommittee work
- Met with Underwriters Laboratory (UL) to hear about their plan to create an industry led IoT certification process (See Appendix)
- Provided FCC with requested input:
  - Provide an outline of potential actionable recommendations
  - Provide any other accomplishments of note
  - Provide any recommendations for working groups next year

# 2. Applying Security to Consumer IoT Devices

- **White Paper – Recommendations**
- The FCC should publish/promote our technical set of considerations for consumer IoT security. The items described in our paper could be used by the FCC to promote the development of best practices and guidelines with industry stakeholders in the consumer IoT market space.
  - NOTE: The group vigorously contemplated a recommendation regarding a potential FCC role in convening and/or promoting an industry led consumer IoT certification effort but was unable to achieve unanimity around such a recommendation.
- The FCC should participate in government IoT security matters with other agencies consistent with the 2014 NSTAC recommendations to address IoT cybersecurity
  - The scope and scale of IoT is vast enough that responsibility for cybersecurity issues is spread out among multiple government agencies
  - Examples of govt agencies and how they have an interest in IoT: FTC – consumers privacy and security, FTA – automotive, FERC – power grid, HHS – healthcare, NIST – technical standards, etc
- Conduct a consumer awareness campaign related to IoT security and privacy
  - This could be in collaboration with other agencies, per the 2014 IoT TAC WG recommendation

# 2. Applying Security to Consumer IoT Devices

- **Suggestions for Future Work**
  - Consider augmenting the consumer focus this year with a enterprise/ICS/critical infrastructure IoT focus next year
  - Perform a more detailed evaluation of a specific aspect of IoT cybersecurity such as the communications technologies or resource constrained devices

# 3. Securing SDN

- **Scope and Approach**
  - As the industry's adoption is still evolving there may not be a set of established practices but will capture the industry landscape with respect to security challenges and opportunities
  - Conduct research using industry resources (vendors, SPs, SDOs, Communities)
  - Consult - SDN / NFV Security SMEs from vendors, operators and communities (e.g. OPNFV, OpenDayLight)
- **Contributors**

- **Ken Countway, Comcast**
- **Brian Daly, AT&T**
- **Martin Dolly, AT&T**
- **Mike Geller, Cisco**
- **Dr. Prakash Kolan, Samsung**
- **Padma Krishnaswamy, FCC Liaison**
- **Ahmed Lahjouji, FCC Liaison**
- **Ramani Pandurangan, XO Communications (Lead)**
- **Christoph Schuba, Ericsson**
- **S Rao Vasireddy, Alcatel Lucent (Co-lead)**

# 3. Securing SDN

**Key Accomplishments**

- Created a White Paper that covers FCC questions and subcommittee work
- Surveyed / Consulted Many Industry Sources for Background, Opportunities and Best Practices (Operators, Equipment Providers, Industry Bodies/Forums)

# 3. Securing SDN

- **<u>White Paper – Recommendations</u>**
- The SDN/NFV current landscape is represented by several use cases. Since the technology and deployments are in early stages, common BCP (Best Common Practices) do not exist. It is recommended that BCPs be developed for the dominant use cases (listed in the WP)
- Work closely with the industry (e.g. ODL, ONOS, OPNFV communities) to sponsor / promote the open source communities / projects to create awareness as well as afford opportunities for innovative developers to showcase their security solutions for SDN /NFV and use of SDN/ NFV to provide enhanced security solutions
- Work closely with the industry (e.g. ODL, ONOS, OPNFV communities) to sponsor a workshop to focus on a small number of critical security challenges for dominant use cases, and candidate solution range to close the gaps identified in section 9 of the White Paper. (The FCC may also want to consider opportunities to sponsor academic research to achieve progress in this area.)
- This transformative nature of this evolution can create various ecosystems and new business models. The FCC can equip themselves by actively participating in the industry activities such as Open Source communities
- NOTE: The SWG discussed a proposed recommendation for the FCC to sponsor / convene the development of a set of technical considerations for securing SDN/NFV which could be used by Vendors and Service Providers in assessing their products and deployments, but could not reach unanimity on such a recommendation.

# 3. Securing SDN

- **<u>Suggestions for Future Work</u>**
  - Application of Threshold Cryptography across controller replicas and dynamic device association for SDN NFV
  - Use of Open Source with a view to encourage the acceleration of development in this area for SDN / NFV.

# Appendix

# Sub-Working Group Activities

1. Simplifying Smartphone Security
   A. Requirements for Consumer-friendly Interface/Wizard for Security Configuration (Leaders: Martin Dolly, Renato Delatorre)
   B. Requirements for Smartphone Security Checker (Leaders: Amit Ganjoo, Katrin Reitsma)
2. Applying Security to IoT Consumer Products (Leaders: Tom McGarry, George Popovich)
3. Securing SDN (Leaders: Ramani Pandurangan, Rao Vasireddy)

# 2. Applying Security to Consumer IoT Devices

- **White Paper – Key Findings**
- Spectrum:
  - Many IoT devices use spectrum allocated and regulated by the FCC
- Identified Gaps:
  - A CSA survey reveals that IoT investors and technology startups are not prioritizing security
  - There have been many security gaps publicly identified in existing IoT solutions
  - Many traditional device manufacturers lack cybersecurity expertise and need to implement secure systems/software development life cycle (SDLC) processes
  - Due to long development cycles, insecure products will continue to enter the market for a period of time
  - For many types of IoT devices, physical access cannot be restricted, thus devices that expose critical information on internal nodes can be compromised
- How industry is addressing these gaps:
  - Industry organizations acknowledge IoT security gaps and are prioritizing security-related technology and best practices
  - There are many publicly available best practices that provide excellent guidance on IoT security, both from a technology and process perspective
  - Processor manufacturers are responding to market needs by providing small system on a chip (SoC) processors that include security features

# 2. Applying Security to Consumer IoT Devices

- **White Paper – Key Findings (continued)**
- Standards:
  - There are a wide variety of technology standards and how security is addressed within these standards
  - Some organizations do not permit review of security requirements without alliance membership, or NDA, etc.; these barriers limit open review by security researchers and the broader industry
  - Many standards allow for different security implementations, some less secure than others
- Compliance/Testing:
  - There are a number of industry organizations providing compliance requirements and testing that includes security for the technology promoted by the organization
- Best Practices:
  - There are multiple industry best practices available, including documents from CTA, CSA, NIST, FTC, DHS, OWASP, etc. (refer to the white paper for details)
  - A few examples of specific best practices:
    - Techniques such as internal data encryption and the use of security-hardened chipsets should be leveraged to stop determined hackers, especially when physical access cannot be controlled
    - Communications of user names and passwords (UN/PW) should be encrypted
    - Password management should be more robust, e.g., different passwords for each device

# 2. Applying Security to Consumer IoT Devices

- **<u>UL Meeting – Highlights</u>**
- The CAP program focuses on SW for now, and future versions will look at HW
  - UL is viewed as a trusted partner and companies are willing to share their source code under NDA
  - Black box testing is also possible if the source code is not provided
- The CAP pilot program includes product testing (known vulnerabilities, fuzzing, malware, security controls), pen testing (ports, external services), and process audit (patch management)
  - The full program will greatly expand on the areas of focus, including static/dynamic code analysis, wireless interfaces, SDLC, supplier controls, and risk management
- UL has issued a draft of their requirements to a pilot set of collaborating companies for review
  - They have begun testing of their draft and are looking for customers (participants)
- Sources of requirements include CAPEC (Common Attack Pattern Enumeration and Classification) and CWSS (Common Weakness Scoring System)
  - CAPEC was established by DHS as part of the Software Assurance strategic initiative of the Office of Cybersecurity and Communications (CS&C)
  - CWSS is another DHS sponsored initiative, part of the Common Weakness Enumeration (CWE) project within DHS' Cybersecurity and Communications Software Assurance program
- The NIST National Vulnerability Database (NVD) is leveraged for the known vulnerabilities part of CAP
- UL is a member of the IIC
- The next vertical to be targeted by UL after ICS and medical is automotive
- The process of putting together the CAP pilot is closed thru 1Q2016
  - A broader panel of participants will be used after the pilot
- There is some focus on networking devices (e.g. routers, switches, etc,) with inclusion of wireless interfaces

# 2. Applying Security to Consumer IoT Devices

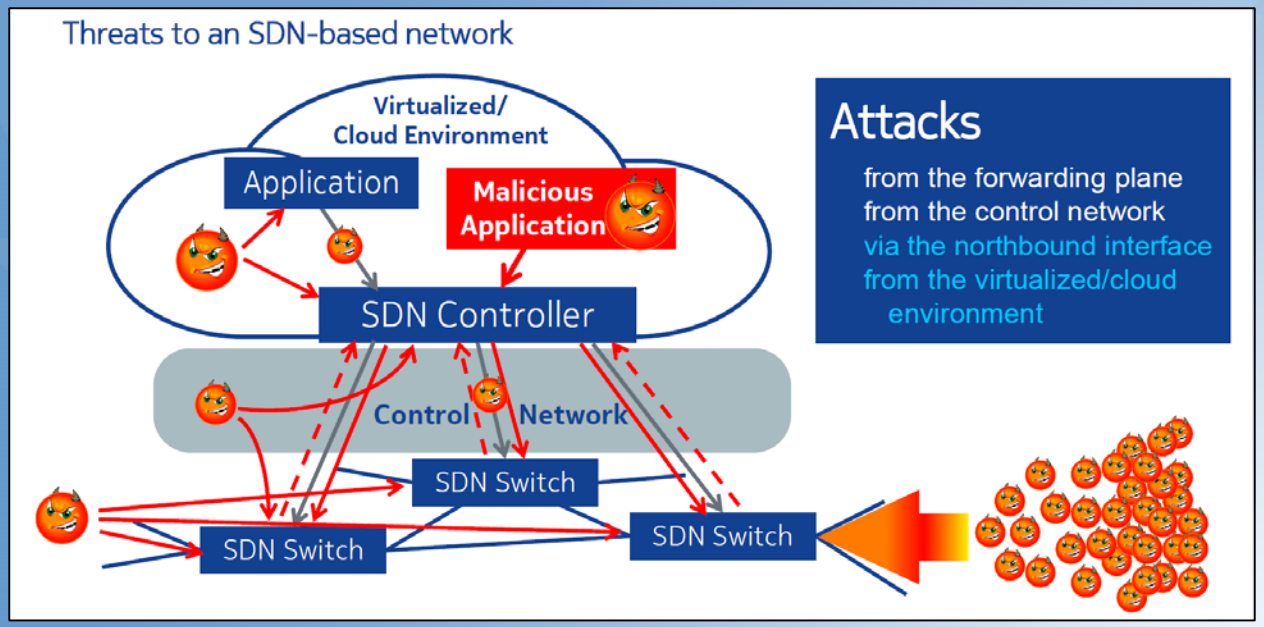
- **<u>UL Meeting – Summary</u>**
- UL is working on a Cybersecurity Assurance Program (CAP) pilot
- Goal: to help vendors manage risk by helping them reduce SW vulnerabilities and raising security awareness
- The CAP scope includes both product assessment (e.g. SW vulnerabilities, the use of security controls), and organization assessment (e.g. SW lifecycle process, including patch management)
- The first focus is in ICS (Industrial Control Systems) and medical devices, with a planned launch by 1Q2016
- The program is intended to be voluntary, with vendors incentivized to participate in a manner similar to other UL certification initiatives

# Sub-Working Group Activities

1. Simplifying Smartphone Security
   A. Requirements for Consumer-friendly Interface/Wizard for Security Configuration (Leaders: Martin Dolly, Renato Delatorre)
   B. Requirements for Smartphone Security Checker (Leaders: Amit Ganjoo, Katrin Reitsma)
2. Applying Security to IoT Consumer Products (Leaders: Tom McGarry, George Popovich)
3. Securing SDN (Leaders: Ramani Pandurangan, Rao Vasireddy)

# 3. Securing SDN

- **White Paper – Key Findings: Security Challenges**



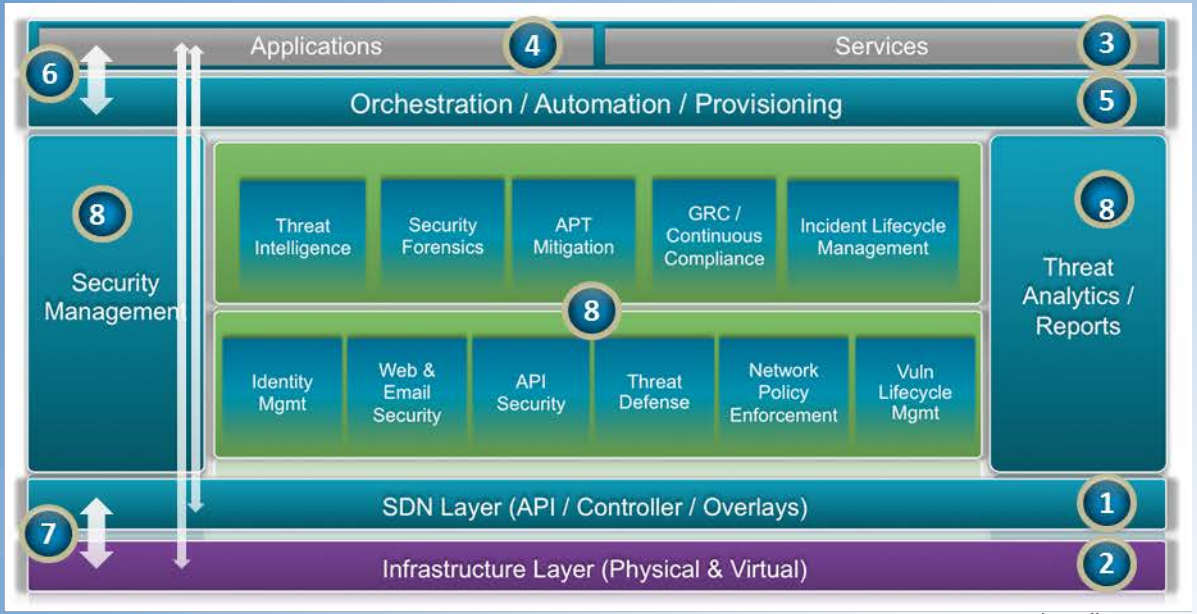

Attacks from many sources, including applications and devices, on Control and Data Planes, need to be addressed

Source: Peter Schneider, Nokia

# 3. Securing SDN

- **White Paper – Key Findings: Multiple Layers of Security**

1. Securing Controller
2. Securing Infrastructure
3. Securing Network Services
4. Securing Application
5. Securing Management & Orchestration
6. Securing API
7. Securing Communication
8. Security Technologies




Source: Mike Geller, Cisco

# 3. SDN / NFV Challenges and Opportunities (1/3)

| SDN/NFV Attribute | Challenges | Opportunities | Possible security approaches |
|---|---|---|---|
| Logical centralization of Control<br><br>Securing controller, infrastructure | Single target of high value<br>o successful attack can impact the entire network under control span of the controller. may be taken over by the attackers;<br>o attack can come from devices, applications, into controllers or through communication channel<br>o Resiliency and scaling challenges potentially impacting availability | o Centralization enables network level control and optimization resulting in: scalability, flexibility and cost savings.<br>o Dynamic control of resources can enable flexible security architecture<br>o Effective security measures for centralized networking assets. | Architecture options for Controller and underlying OS security:<br>o Active / active, active / standby, clustering, geo-redundancy deployment alternatives available<br>o Limited scope with federation may be possible<br>o Network elements may be designed to operate with the last-good-state if controllers are down |
| Disaggregation - Separation of control and data planes<br><br>Securing controller, infrastructure, Management, orchestration, API, Applications, communications | Increases attack surface;<br>o multiple devices need be protected;<br>o communication channels and protocols must be secured<br>o a compromised device may attack SDN controller<br>o State of device security is non static; a compromised device may remain undetected<br>o In Telemetry, compromised device may send false or fabricated data to the SDN controller; securing telemetry presents a significantly harder challenge* | o Each layer can scale and evolve independently; provides vendor independence to SPs. | Security for applications, underlying platform, orchestration, automation and provisioning:<br>o Clearly Define Security Dependencies and Trust Boundaries, Assure Robust Identity, Build Security based on Open Standards, Protect the Information Security Triad – Confidentiality, Integrity and Availability (CIA), Protect Operational Reference Data, Make Systems Secure by Default, Provide Accountability and Traceability |

* Source: Dr. Kireeti Kompella, CTO, JDI, Juniper

# 3. SDN / NFV Challenges and Opportunities (2/3)

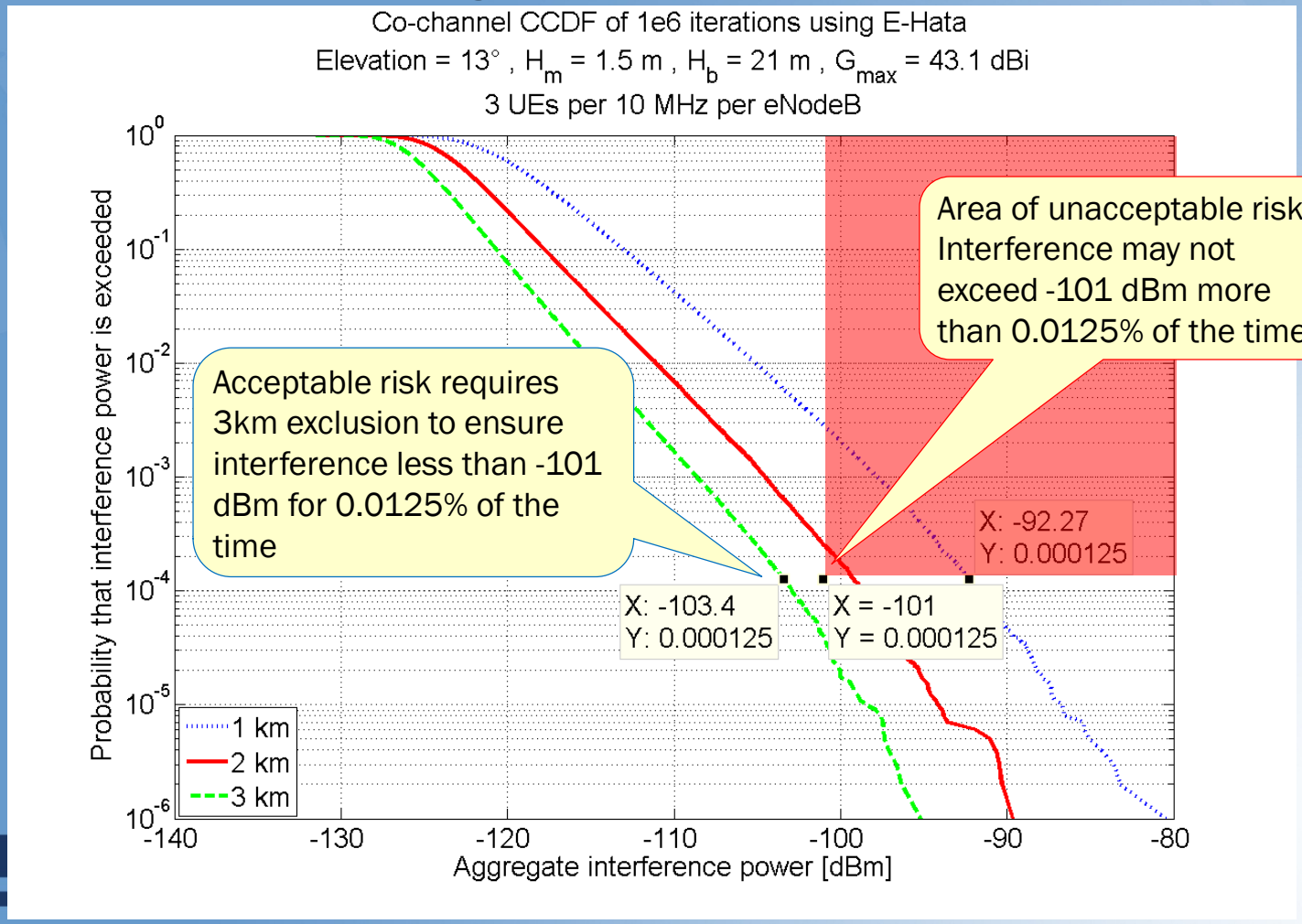
| SDN/NFV Attribute | Challenges | Opportunities | Possible security approaches |
|---|---|---|---|
| Abstraction - Programmability<br>Securing controller, infrastructure, Management,/orchestration, automation, use of security technologies | Abuse of control functions, exploiting vulnerabilities, compromising controllers. Semantic consistency between messages to a single device may be solvable; Semantic consistency between messages among multiple devices is harder to solve* | o Facilitates deployment of agile, fine-grained security solutions running as applications and Software Defined Security approaches | Securing of all communication (Northbound, Southbound, East - West) channels and messages; Authentication between communicating entities, continuous attestation, not just at the time of spawning, of functions, audits and anomaly detection may be needed . Multiple layers of security would be needed |
| Multiple Trust Domains<br>Securing controller, infrastructure, Management,/orchestration, automation, use of security technologies | New types of threats arise due to the explicit programmatic access SDN offers to clients that are typically separate organizational or business entities. Not unique to SDN is the fact that insiders represent a significant security threat, and that operator error threatens system integrity | o Provides openness to allow customer self-service and different business models | Requires strong authentication and robust security at all interfaces. Should include strong identity and credential management functions that secure all entities and their associated state. |

* Source: Dr. Kireeti Kompella, CTO, JDI, Juniper

# 3. SDN / NFV Challenges and Opportunities (3/3)

| SDN/NFV Attribute | Challenges | Opportunities | Possible security approaches |
|---|---|---|---|
| Virtual Network Functions (VNF) running in virtual machines and replace / supplement physical network functions<br><br>Securing infrastructure, applications, e2e security analytics | Union of generic threats from virtualization / cloud, threats specific to previous physical network functions and new threats from the combination | Provides elastic capacity and automated provisioning. Service Chaining allows micro services to be properly sequenced to provide great flexibility and granularity and as and when needed; operating efficiencies and rapid service innovation. Recognizing the need for more holistic solution, Server / Endpoint security vendors are integrating with Network Security vendors by correlating network and server / endpoint threat data | Best Current practices of cloud (e.g. NIST, CSRIC, CSA, previous work of TAC) available. TPM and Virtual TPM for higher level of assurance. Trusted Computing practices start being used in commercial shipments ; expected to become more common in the future (e.g. Trusted Platform Module (TPM) chip on HP-UX Integrity servers, Intel Trusted Execution Technology (TXT), industry is also developing Virtual TPM for virtualized environment. It is not either network security or security embedded in hosts / servers; both are needed; significant work ongoing in ETSI – see GS NFV-Sec documents |
| Use<br><br>Security technologies | Being open source subject to attack | The more participants examine the code, the faster will the vulnerabilities be detected and fixed. Several vendors are enhancing Open Source and making them more rugged. | Carrier grade , including security, is work in progress in the various communities. Community is working on security areas (e.g. OpenStack Trusted Compute Pools); significant work ongoing in ETSI – see GS NFV-Sec documents |

# Short-term (13 deg): set co-channel exclusion



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

Chairs: Russ Gyurek, Cisco
John Barnhill, Genband

FCC Liaisons: Walter Johnston, Scott Jordan, Padma Krishnaswamy, Alec MacDonell, Kristine Fargotstein

Date: December 9, 2015

# Working Group Team Members

- Mark Bayliss, Visualink
- Nomi Bergman, Bright House
- KC Claffy, CAIDA
- John Dobbins, Earthlink
- Adam Drobot, OpenTechWorks
- Andrew Dugan, Level3
- Lisa Guess, Juniper
- Stephen Hayes, Ericsson
- Theresa Hennesy, Comcast
- Farooq Kahn, Samsung
- Brian Markwalter, CE
- Kevin McElearney, Comcast
- Tom McGarry, Neustar
- Milo Medin, Google
- Lynn Merrill, NTCA
- Jack Nasielski, Qualcomm
- Ramani Pandurangan, XO Comm
- Mark Richer, ATSC
- Marvin Sirbu, Carnegie Mellon
- Kevin Sparks,  ALU
- Sanjay Udani, Verizon
- David Young, Verizon

# NG Internet Service Characteristics & Features Charter

- The Internet has and will continue to evolve:
  - Driven by the transition to all IP
  - From simple backbone/access network to a complex environment of dedicated links, Content Delivery Networks (CDNs), specialized routing/peering arrangements, etc.
  - Supporting : Remote terminal access/ email -> Web browsing/ media transfer -> Video streaming
- Commission Hypothesis:
  - A 'best effort' network is evolving towards one where Quality of Service (QoS) is a growing concern
  - Need for benchmarks to measure QoE and the support of rich services
  - The Internet will transition to a role of critical infrastructure

# Commission Asks Workgroup to Comment on:

**New Work Areas:**

- Network Metrics
  - QoS BIAS
  - E2E QoS
  - QoE BIAS
  - Health and Performance
- New technologies impact
  - SDN
  - 5G
  - Caching

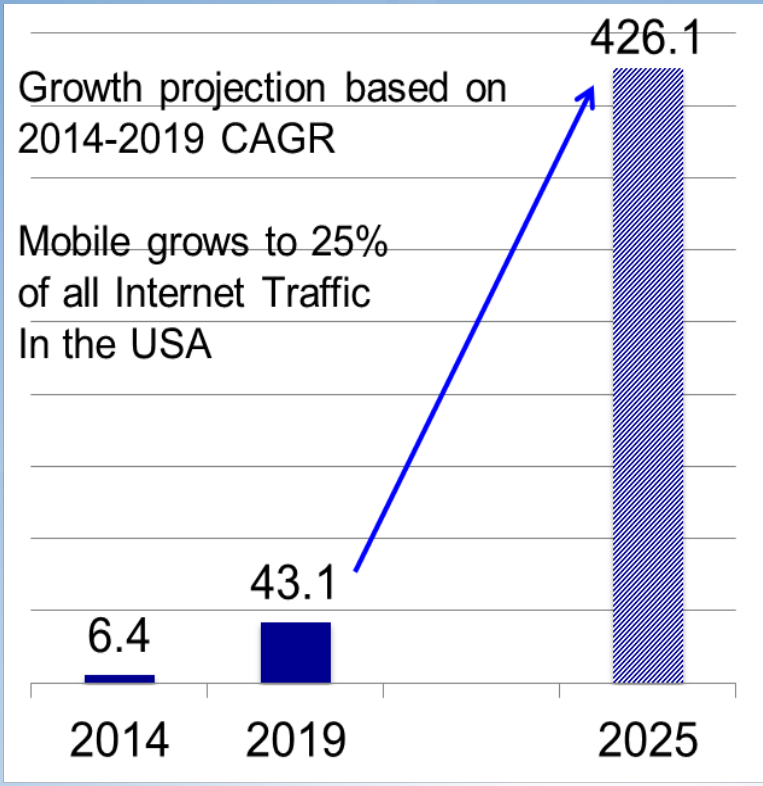
**Past Work:**

- Critical infrastructure services
- PSTN Services Transition
  - Impact on NG
- Internet of Things
  - Scale
  - Security

# SUMMARY OF WG EFFORTS

## Exec summary

- NG Internet Drivers: Video, Mobility lead the charge
- CDNs strongly impact content and Internet economics and performance
- Data encryption is the rule
- E2E QoS: No differentiation without remuneration
- QoS: Leverage MBA, Focus on Interconnect, ISP Domain, Last Mile, and CDN performance
- QoE: Begin data capture via 3rd party, correlate with QoS and BB data

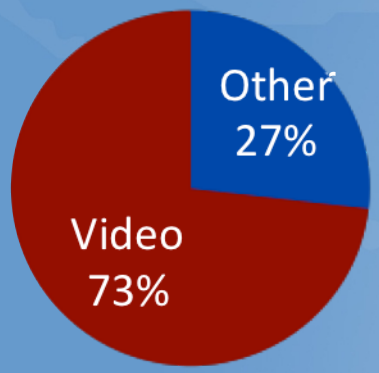


# NG Internet Drivers

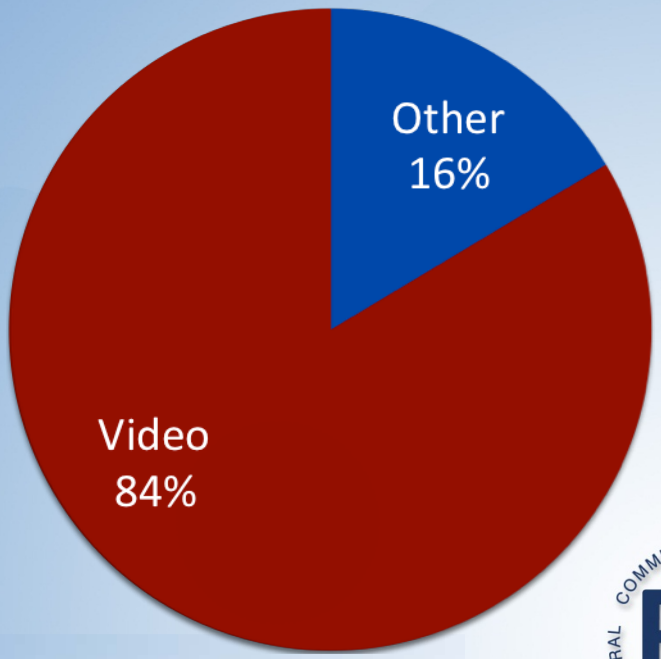
- Societal changes
  - Mobility, access everywhere
  - Encryption is new rule
  - Many devices connected per user
  - Forecast: Peak traffic growing faster than non-peak traffic
- Devices outnumber people (IoT)
  - Constant and sporadic data streams from billions of devices
- More Enterprises shifting to public Internet
  - Impacts Internet load during day (peak time)
- Pervasive Services: Video, Medical, Home monitoring, Automotive, etc
- Programmability
  - Replacing non-automated processes [provisioning] infrastructure layer impact
  - Not realistic to cross AS boundaries,
  - Used to control aggregate flows, not individual
- BIAS is critical component of End-to-end infrastructure

# Consumer Internet Traffic Growth - USA

## 2014 - 98.3 EBs




## 2019 – 314.6 EBs




Source: Source Cisco VNI – 2014 -2019

# Constant Evolution – User Driven, Technology Enabled

## Devices, Capacities, Bandwidth, Content

### Yesterday's Internet

- Limited Devices
- Wired Access
- Stationary Devices
- Human Driven Usage
- Email, Web Browsing
- Downloaded Content

### Today's Internet

- Wired or Wireless Access
- Many Mobile Devices
- Human Driven Usage
- Entertainment Content
- Content Delivered at Backbone and Metro
- Streaming Content

### Tomorrow's Internet

- Wired or Wireless Access
- Fixed & Mobile Devices
- Built-in Sensors with Data Collection
- Content Delivered at the Metro/ Edge
- "Thing" Driven Usage
- Public Safety

# Evolution Trends

| Factor | Trend | 2014 | 2019 |
|---|---|---|---|
| Devices | Smart Phones and IoT | 2.0B | 3.9B |
| Speeds | Both Fixed (W+) and Mobile (W-) speeds growing rapidly | 22.2Mbs W+<br>2.6Mbs W- | 45Mbs W+<br>6.1Mbs W- |
| Traffic Volume | Consumer Internet Traffic | 98.3EB | 314.6EB |
| Traffic Mix | Video Growth is dominant driver of consumer Internet consumption | 73% | 84% |
| Access Mix | Wireless data growth but fixed still dominant (All Internet Traffic) | 6.4EB W-<br>115.4 W+ | 43.2EB W-<br>343.3 W+ |
| Metro/ Long Haul Changes | Virtualization/ Dynamic Mgmt<br>CDN I/C Shifting from Core to Metro | 165 vs 52 EB<br>(76% of all IP) | 499 vs 49 EB<br>(91% of all IP) |

Source: Source Cisco VNI – 2014 -2019

# Content Delivery Networks (CDN) - 2015

- Small number of CDN providers deliver majority of Internet content
  - Effectiveness depends upon hit rate: success ratio of finding desired content in cache
  - Hit-rates may be declining (Democratization of content)
- Transparent caching by ISP networks
  - Dynamic caching of multi-services/general Internet content to minimize facilities issues and backbone/transit costs
  - Typically in smaller networks or wireless networks
  - Encryption will inhibit transparent caching
- CDN delivery efficiencies are evolving closer to consumer
  - Predictive pre-positioning of content …all the way to consumer premises
- CDNs evolving to provide increased computation *vs* object delivery only

**Summary: CDNs strongly impact content and Internet economics and performance**

# CDNs: Potential Concerns

- Relative role of CDN and ISP in QoE not well measured or understood
  - Emerging firms beginning to measure QoS/QoE, performance
- Limited/Weak coordination between CDNs and ISPs
  - CDN operator controls which server is used and SP ingress point
  - Lack of publisher planning for impact of major download events
    - e.g. major new software releases
    - Tendency for each party to self-optimize
      - Nash equilibrium << coordinated planning

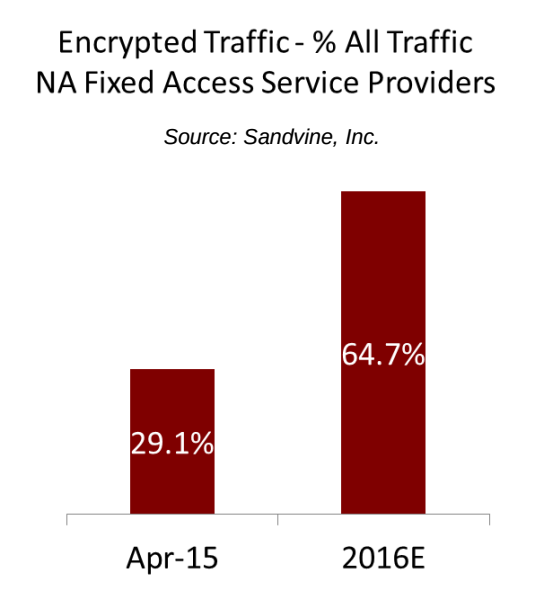
**Add measuring CDN performance as part of QoS/QoE effort**

# CDNs: Potential Concerns – cont.

- Inadequate CDN coverage in rural environments
  - Emerging consortia arrangements
  - As CDN's become larger in size due to technology advances, economic qualifiers for smaller markets to obtain CDN's become less attractive
- CDNs have greatly reduced the cost of OTT (unicast packet delivery) video delivery, making it competitive with broadcast delivery for some use cases. Relative cost and pricing of OTT vs broadcast delivery models will continue to be contentious
  - E.g. zero rating, volume pricing

# Encryption Summary

- Trend: Growth of encrypted data in the network
  - majority of traffic encrypted by end of 2016
  - Unstoppable trend driven by a variety of factors
  - Standards for trusted proxies not getting traction
  - Incorrect Implementation: EG. up to 15% invalid certs.
- Expected impacts
  - Transparent caching (wireless & wireline)
  - Value-Add Services (security, parental control, ..)
  - Network Management based on DPI/content awareness
- Aggregate subscriber service controls unaffected, but content-aware network management will be limited
- Network management (in presence of encryption) is not mature
- Conflicting industry interests make finding solutions difficult




FCC Action: *Assume encrypted data in all future policy decisions*

# QOS AND QOE

# NG-I WG Definitions

## Quality of Service (QoS) Definition

Quality of Service (QoS) is an objective set of measurements used to describe the technical performance of a network. Typical measurements include throughput, latency, jitter, bit error rate, availability and packet loss and are typically specified in service level agreements.

The network service provider typically provides layer 1-3. Higher layer services may also be offered by the network service providers, application providers or users, who in turn, may provide layer 1-3 services that interface with the network service provider services.

Different applications have varying sensitivity to these performance factors which contribute to application Quality of Experience (QoE). From the viewpoint of the end user application, QoS metrics trade off against each other and should be interpreted in the context of improving user experience. (see BITAG).

## Quality of Experience (QoE) Definition

QoE, quality of experience, is a subjective measurement of a consumer's perception of application. Many factors play a role in this subjective evaluation. These include network throughput, network latency, jitter and packet loss which are usually measured as QoS parameters. Origin and delivery route of content and/or applications also has an impact on perceived network performance.

Additionally, non-service provider factors such as the user's network, devices, device configuration, user interface design, the applications that are running, the subscribed broadband tier, and the environment in which services are consumed play important roles.

Reliable QoE measurements need to capture data for all of the items listed above to compute a "realistic" QoE measurement. Adding contextual data removes many of the factors that can lead to incorrect perceptions and measurements.

## How to measure QoS? Leverage the FCC MBA Program

- MBA program resulted from FCC's National Broadband Plan 2010
- CPE: "white-box" is Linux based HW
- Deployment today: Approximately 6000 homes
- Only performs measurements when CPE is not in use
- FCC MBA is working with ISPs/manufacturers to embed capability
- Requirements: 300KB of Flash, uses 2MB of RAM at peak load
- Test capability: Up to 1Gbps bidirectional links
- Participants: 15 ISP's covering >80% of US population
- MBA Goals: BB policy, informed consumer choice, universal service
- Program based on openness, transparency and partnerships
- Reports are published under open data with privacy protections
- Covers wireline and wireless

MBA Testing

# Measuring (Fixed) Broadband America

## Measurements

- Download Speed
- Email Relay
- Upload Speed
- Video QoE
- Web Browsing
- Video Streaming
- Voice over IP
- UDP Latency
- UDP Packet Loss
- UDP Contiguous Loss
- Multicast IPTV
- FTP Throughput
- DNS Resolution
- Peer-to-Peer
- UDP Latency Under Load

***5,500 Voluntary Samples***

MBA

Off-Net Sites

ISP

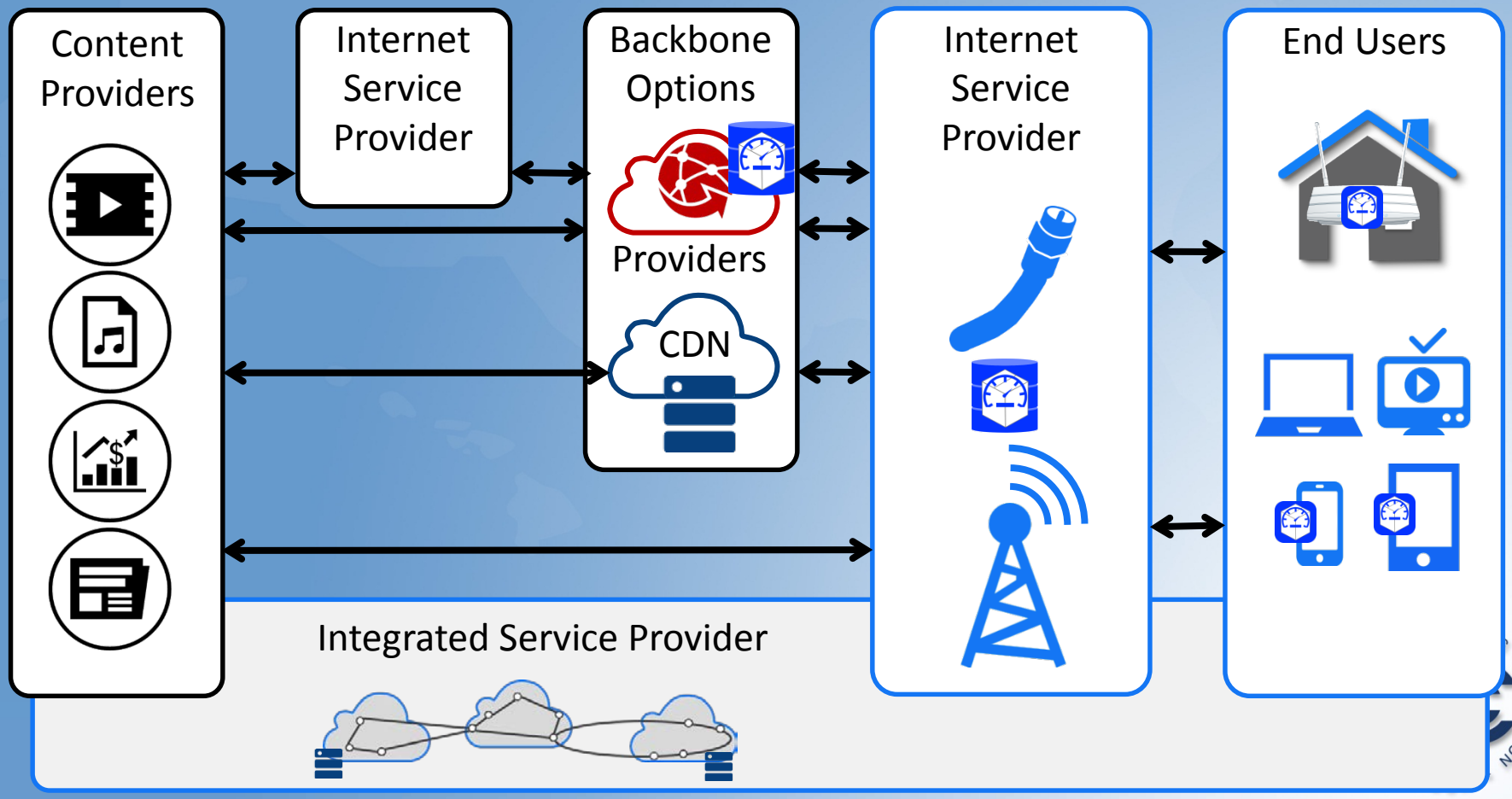
On-Net

White-box FW

## Deriving Estimated QoE

- ISPs have both on-net & off-net test nodes
- Enables end-to-end network performance
- Network Performance Comparisons for ISP
- ISP can see impact 3rd party networks have on end-user Quality of Experience (QoE)

# Simplified Example: MBA Testing (Today)



# Several Different Approaches to Measurement Solution

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

**Broadband Facts**

**15 Mbps Internet Download**

Upload Speed 1.5 Mbps

Up to 50 gigabytes (GB)

**Per Month $39.99**

**Extras**

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

**Performance***

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

BIAS to Consumer

Edge Provider to BIAS

Broadband Label

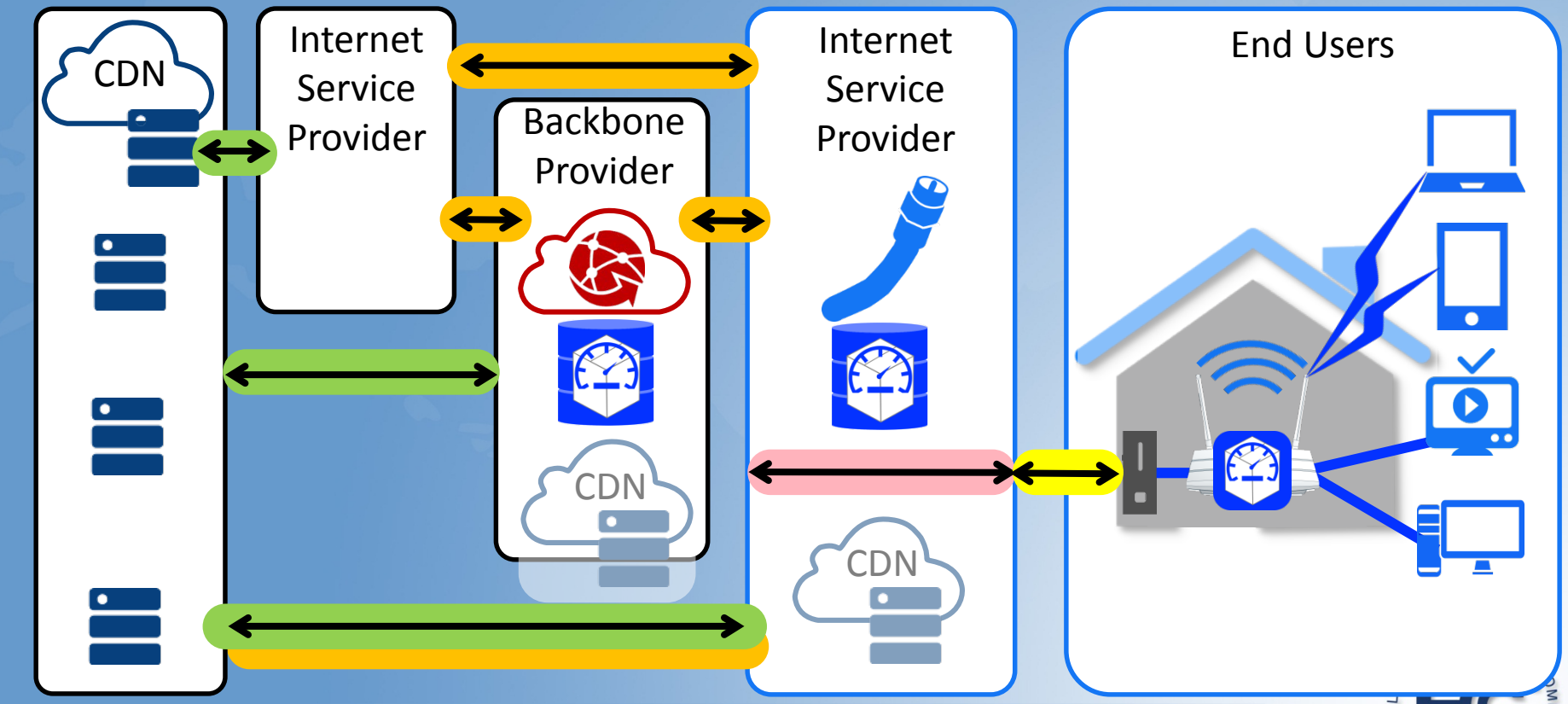
## What MBA does *not* Measure

- Enterprise Services
- Interconnect health
- Smaller providers
- Rural/Smaller ISPs
- Anchor institutions
- Network Reliability
- Network Resilience
- Network Features
- QoS and QoE
- Consumer adoption
- Content decisions
- CDN performance
- Service SLA

## Additional QoS Measurements

| Metric | Primary Measure(s) |
|---|---|
| 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 |
| 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 demarc point |
| BIAS Packet Loss | Measurement of packet loss (as between border router of ISP at interconnect point and CPE demarc point |
| BIAS Jitter | Measurement of jitter on packets between border router of ISP at interconnect point and CPE demarc point |

# MBA + QoS Testing: MBQ→ *Measured Broadband and Quality*




CDN Performance
Interconnection Health
BIAS Cloud
BIAS Last Mile
Existing MBA

# END-TO-END /QOS

# Today: E2E QoS Only Available via Managed Services

**Managed Connectivity**

Enterprise VPNs
ISP Video Services
ISP Voice Services

- Managed End-end QoS/SLAs
- Coordinated between network operators
- Essential for ensuring the integrity of ISPs' own services & many "mission critical" enterprise uses
- Applicable to fairly high end users/uses, given cost

**Internet**

Skype
OTT Video
OTT Voice
Internet VPNs
Web Browsing

- User flows undifferentiated (best effort)
- Shared resource = universally accessible
- Low cost = universally applicable
- Enabler of unrestrained innovation & rapid/viral adoption of new services

Q: Should the range of type & quality of services expand in the NG Internet?

# NG Internet – *The E2E QoS Fork in the Road*

**Undifferentiated Internet**

### Current Internet, massively scaled

- Ever higher BW applications enabled
- QoE still not predictable
- Capacity upgrades gated by ISP access ROI

**Differentiated Internet**

### New- Unpaid QoS Internet

- What users and apps get differentiation?
- If QoS traffic unlimited there's no differentiation
- Not clear model exists!

**Non-Transactional**

### New- Paid QoS Internet

- For subset of traffic only
- △cost constraints
- $: Direct user or indirect app/content provider
- Predictable QoE for wider range of uses

**Best Effort** ← → **Transactional**

# RECOMMENDATIONS

## Actionable Recommendations: NG-I WG 2015

- Encryption: Assume majority of data as encrypted in all future policy decisions
- Expand MBA program to add QoS and QoE measurements → MBQ
  - Measurements should be as automated as possible
  - Open Data/ Data transparency, while protecting privacy (ISP & consumer)
- Add/include CDN performance to metrics measured
- QoE: Contract a professional consulting company to create a questionnaire to poll consumer experience data, and to potentially administer the poll
  - Consumer data correlated with relevant MBA performance measurements and QoS data to develop valuable insights on the relationship between objective QoS data and subjective QoE consumer data
  - Purpose: Assist the FCC with future BB policy considerations, current performance programs as well as consumer awareness
- Fund a consumer education program: Variables that impact BB performance
- FCC to allocate resources to data science needs of the measurement program
- Funded research support for QoS measurements

# 2016 WORK SUGGESTIONS

## 2016 Work suggestions

Working Group Activities:

- End-to-end QoS: measurement possibilities
- How to create “automated capability” on MBQ testing and measurements
- Explore OS community for SW based measurements
- NG internet have differentiated E2E QoS, more work needed (find slide)
- How to leverage alternate sources of data. IE Crowd-sourced data
- Broadband bottlenecks and breakpoints; where are the limitations

Other:

- Create a technology transfer program through direct, time-framed relationships with tech companies. Creation of a program for industry experts to be “*Scientist’s in Residence*” working with the FCC staff on emerging technologies. Provides a way to accelerate knowledge transfer.

# THANK YOU!

# BACK-UP

## Consumer Internet QoE Definition *(FCC TAC NG WG)*

QoE, quality of experience, is a subjective measurement of a consumer's perception of application. Many factors play a role in this subjective evaluation. These include network throughput, network latency, jitter and packet loss which are usually measured as QoS parameters. Origin and delivery route of content and/or applications also has an impact on perceived network performance.

Additionally, non-service provider factors such as the user's network, devices, device configuration, user interface design, the applications that are running, the subscribed broadband tier, and the environment in which services are consumed play important roles.

Reliable QoE measurements need to capture data for all of the items listed above to compute a "realistic" QoE measurement. Adding contextual data removes many of the factors that can lead to incorrect perceptions and measurements.

*QoE will, by necessity, be a sum of end to end factors. As such, efforts such as Measuring Broadband America will likely provide more accurate indicators of user perception than traditional network performance metrics which would need to be correlated across multiple networks and providers to achieve similar end to end results.*

## Definition of Quality of Service (QoS) *(FCC TAC NG WG)*

Quality of Service (QoS) is an objective set of measurements used to describe the technical performance of a network. Typical measurements include throughput, latency, jitter, bit error rate, availability and packet loss and are typically specified in service level agreements.

The network service provider typically provides layer 1-3. Higher layer services may also be offered by the network service providers, application providers or users, who in turn, may provide layer 1-3 services that interface with the network service provider services.

Different applications have varying sensitivity to these performance factors which contribute to application Quality of Experience (QoE). From the viewpoint of the end user application, QoS metrics trade off against each other and should be interpreted in the context of improving user experience. (see BITAG).

*Additionally, network elements closer to the user will likely impact QoE more than issues deeper in the network since mitigation can be implemented transparently from the user. QoS issues impact similar applications similarly. QoE differences with similar applications are likely due to issues external to the ISP.*

## Recommendations: Parameters and Metrics

- The MBA program provides a basis for capturing data: Internet performance and QoS
  - Measuring Broadband, QoS, QoE are Big Data issues
  - Proposed new program “MBQ” Measured Broadband & Quality program
  - Today: MBA program collects data on 12 parameters, we recommend adding the following measurements:
    - Interconnect
    - Last mile
    - Video Services: CDN
    - ISP Cloud
  - All measurements should be:
    - service transparent (non-service interrupting),
    - automated to the greatest extent possible,
    - common across all equipment (Whitebox SW must be identical),
    - testing should be as lightweight to service providers as possible

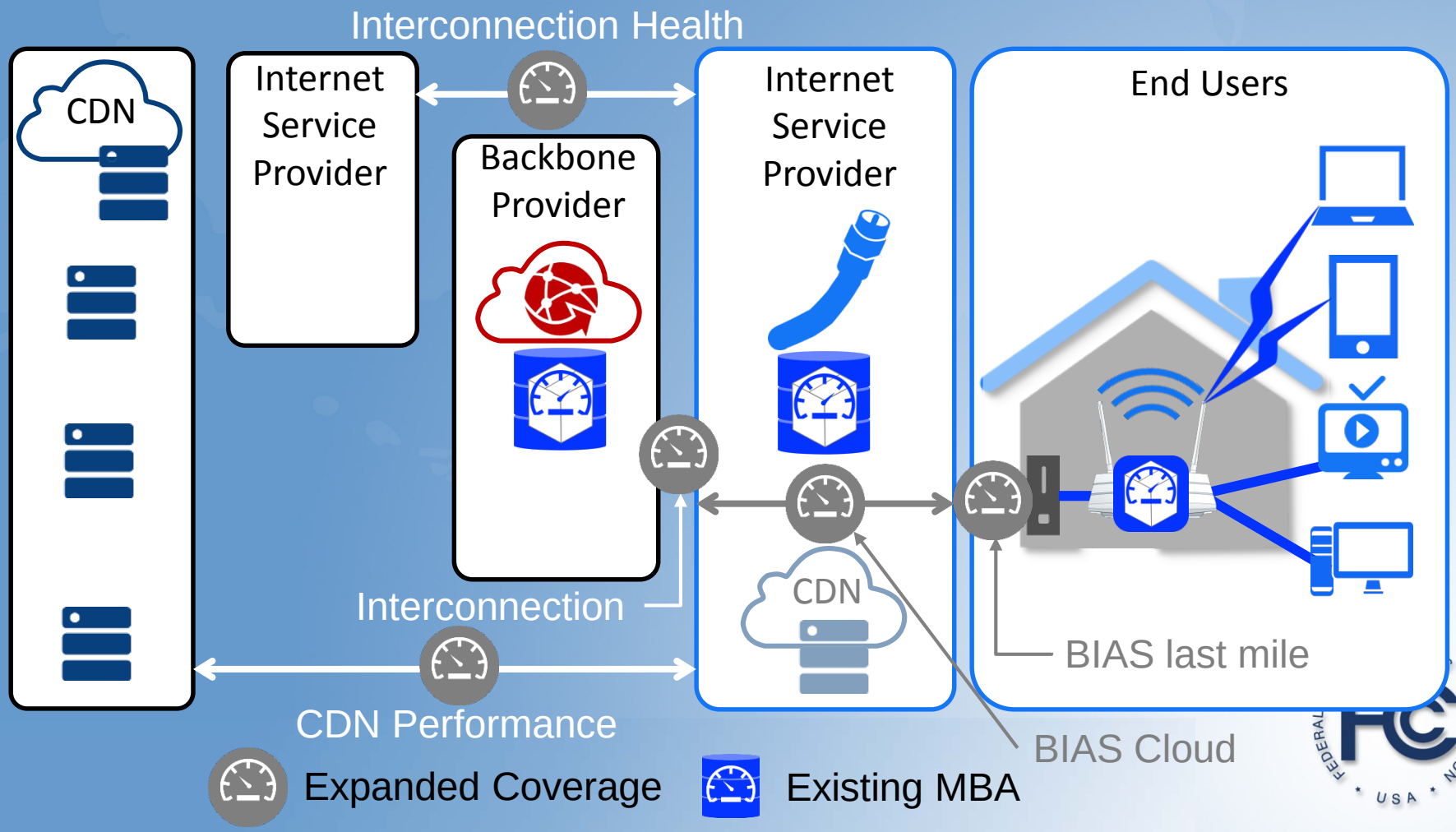
## Recommendations: QoS

- QoS: Leverage and Grow the MBA program to capture QoS data
  - Add QoS measurements a part of the MBA program
  - Participation should be voluntary for consumers
    - Assumption: there will be adequate participation to represent population and the many ISPs
  - Promote integration of "MBA whitebox/measurement Agent function" functions into consumer CPE, potentially other areas of network
  - App-like: Explore addition "agents" that can be installed on CPE equipment
  - Avoid creating a new SP data request program
  - Data transparency and openness: QoS data much be made available publicly for 3rd party tests
  - The privacy of consumers must be protected in any released data program
  - The FCC allocate resources to data science needs of this program
  - Funded research support to QoS measurements

## Recommendations: QoE

- Measuring QoE along with BB performance and QoS (Network Performance) provides a full comprehensive picture of Internet health and performance
  - Add customer "experience" polling to MBA
  - Work with professional consulting company to create a questionnaire to capture data, and potentially administer the poll
  - Data must include consumer environment: equipment, configuration, to highest degree possible
  - Data needs to be combined with relevant *rate plan data*, *MBA performance measurements* and *QoS data* to extract highest value from "subjective" consumer information
  - Fund a consumer education program on BB technologies and usage for best data value

# MBA + QoS Testing: Measuring Additional Networks & Elements



## MBA Measurements in Detail

| Metric | Primary Measure(s) |
|---|---|
| Download speed | Throughput in Megabits per second utilizing one or more concurrent TCP connections |
| Upload speed | Throughput in Megabits per second utilizing one or more concurrent TCP connections |
| Web browsing | The total time taken to fetch a page and all of its resources from a popular website |
| Voice over IP | Upstream packet loss, downstream packet loss, upstream jitter, downstream jitter, round trip latency |
| UDP latency | Average round trip time of a series of randomly transmitted UDP packets |
| UDP packet loss | Percentage of UDP packets lost from latency test |
| UDP latency/loss under load | Average round trip time and packet loss of UDP packets whilst the line is heavily loaded with downstream or upstream traffic |
| UDP contiguous loss (Disconnections) | Events of two or more consecutively lost UDP packets to the same destination – essentially internet connection is lost |

## MBA Measurements in Detail

| Metric | Primary Measure(s) |
|---|---|
| DNS resolution | The time taken for the ISP's recursive DNS resolver to return an A record for a popular website domain name |
| FTP throughput | Throughput in Megabits per second at which a file can be downloaded from or uploaded to an FTP server |
| Peer-to-peer | Throughput in Megabits per second at which a file can be downloaded from BitTorrent |
| Email Relaying | The time taken to relay an email via the ISP's SMTP servers and reach a target mail server |
| Video streaming (Generic) | The initial time to buffer, the number of buffer underruns and the total time for buffer delays of an emulated fixed-rate TCP video strea |
| Video Quality of Experience – YouTube, Netflix, BBC iPlayer | The highest bitrate that can be streamed from the content servers / caches of YouTube, Netflix and iPlayer without rebuffering (Bitrate Reliably Streamed) and the time taken for the video to start playing (Startup Delay) |
| Multicast IPTV | Time to switch IPTV channels, and the jitter and packet loss observed in the multicast stream |

# Future Game Changing Technologies Working Group

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

9-December-2015

# Working Group Members

- Members [**SWG Chairs**]:

  - Kumar Balachandran, Ericsson
  - John Barnhill, Genband
  - Mark Bayliss, Visualink
  - John Chapin, SGE
  - Lynn Claudy, NAB
  - Brian Daly, AT&T
  - John Dobbins, Earthlink
  - Jeffrey Foerster, Intel
  - Mark Gorenberg, Zetta Ventures
  - Dick Green, Liberty Global
  - Lisa Guess, Juniper Networks
  - Russ Gyurek, Cisco
  - Farooq Khan, Samsung
  - Steve Lanning, ViaSat
  - Gregory Lapin, ARRL

# Working Group Members

- Members [**SWG Chairs**]:

- **Brian Markwalter**, CEA [**Demand**]
- Tom McGarry, Neustar
- Paul Misener, Amazon
- Thyagarajan Nandagopal, NSF
- **Jack Nasielski**, Qualcomm [**Capacity**]
- Lynn Merrill, NTCA
- Bruce Oberlies, Motorola Solutions
- Ramani Panduragan, XO Communications
- Sridhar Rajagopal, Samsung
- Mark Richer, ATSC
- Marvin Sirbu, SGE
- Hans-Jurgen Schmidke, Facebook
- **Kevin Sparks**, Alcatel-Lucent [**Arch**]
- Paul Steinberg, Motorola Solutions
- Sanjay Udani and David Young, Verizon

# Future Game Changing Technologies Working Group Charter

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

# Executive Summary

- Networks will continue to experience high traffic demand growth, driven by video content, cloud, IoT, and increasingly mobile-anywhere consumption
- Telecom and IT/Cloud sectors are rapidly mixing and melding with each other, together undergoing the *most* fundamental of transformations
- Cloud virtualization, software-defined networking, and new network architectures are the *key underlying enablers*
- Two 'uber' advances emerge as the prime future 'game changers' driving transformational innovation and economic growth across many sectors:
  - **Programmable Networks**
  - **5G (RAN *and* Core)**
- It is critical that the FCC's mindset is to look ahead, be prepared, and shape rules and policy plans anticipating and embracing both key technologies

# Technologies Investigated

ATSC 3.0 (Broadcast)

Drones/UAVs

LEO/MEO Satellites

RF Full Duplex

Augmented Reality

5G Core

WebRTC

5G RAN

NFV

SDN

Massive MIMO

100G RF

Hybrid Cell/Satellite

Distributed Edge/Compute

NG PON

Virtual Reality

Cloud RAN/ vRAN

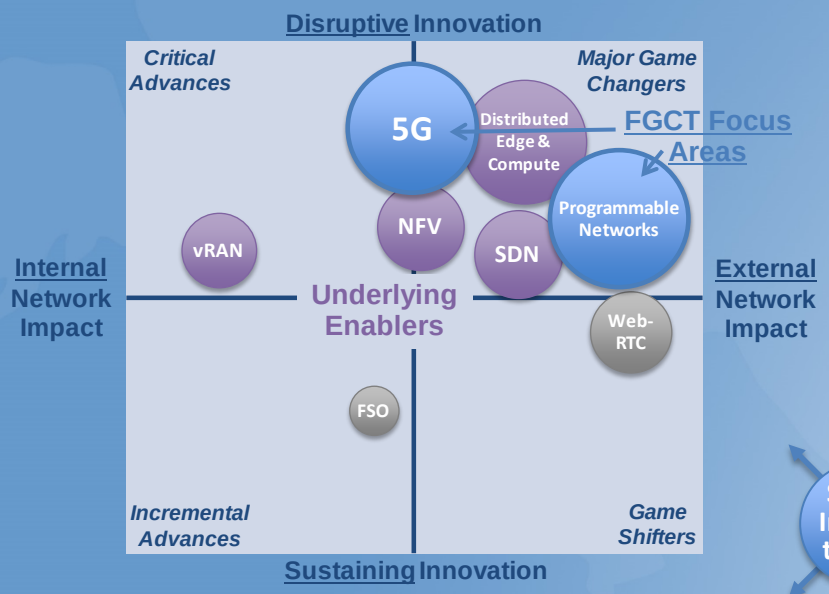
RF Mirror Worlds

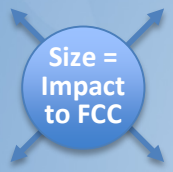
Advanced DSL

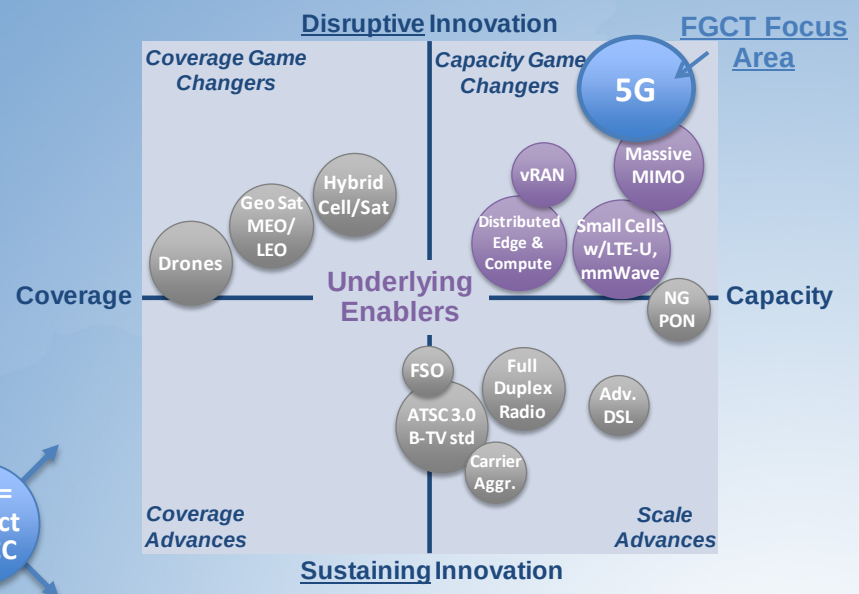
mmWave small cells

*SME sessions and discussions held on extensive range of emerging and future technologies*

# Assessment of FCGT Focus Areas




## Architecture SWG

## Capacity/Coverage SWG

# Interrelated Game Changing Technologies

Starting now; will phase in over next 5-7 yrs

**Programmable Networks**
- Network APIs enabling access to network resources

Standards-based introduction expected ~2020

**Tactile Internet**
- Apps requiring very low latency & high reliability

**Distributed Edge Intelligence**
- Compute, content close to users
- High performance, low latency

**5G RAN**
- Multi-optimized air interface (cost, BW, mobility, latency)
- Expanded spectrum (cmWave, mmWave)
- Multi-connectivity

**vRAN/Cloud RAN**
- Pooled, centralized RAN baseband processing resources
- Many variations
- Mix of specialized & x86 HW

**Intelligent Multi-RAN/RAT**
- Seamless blending of many types of wireless access tech. & spectrum

**Re-architected 5G Core**
- Converged, simplified, highly virtualized
- Resources flexibly composited & optimized per application/device type

*Access*

*Core*

**SDN/NFV (Enabler)**
- Dynamic virtualization of network functions on x86
- Automated connectivity (vNFs, network endpoints)
- Broad enabler of technologies & business models

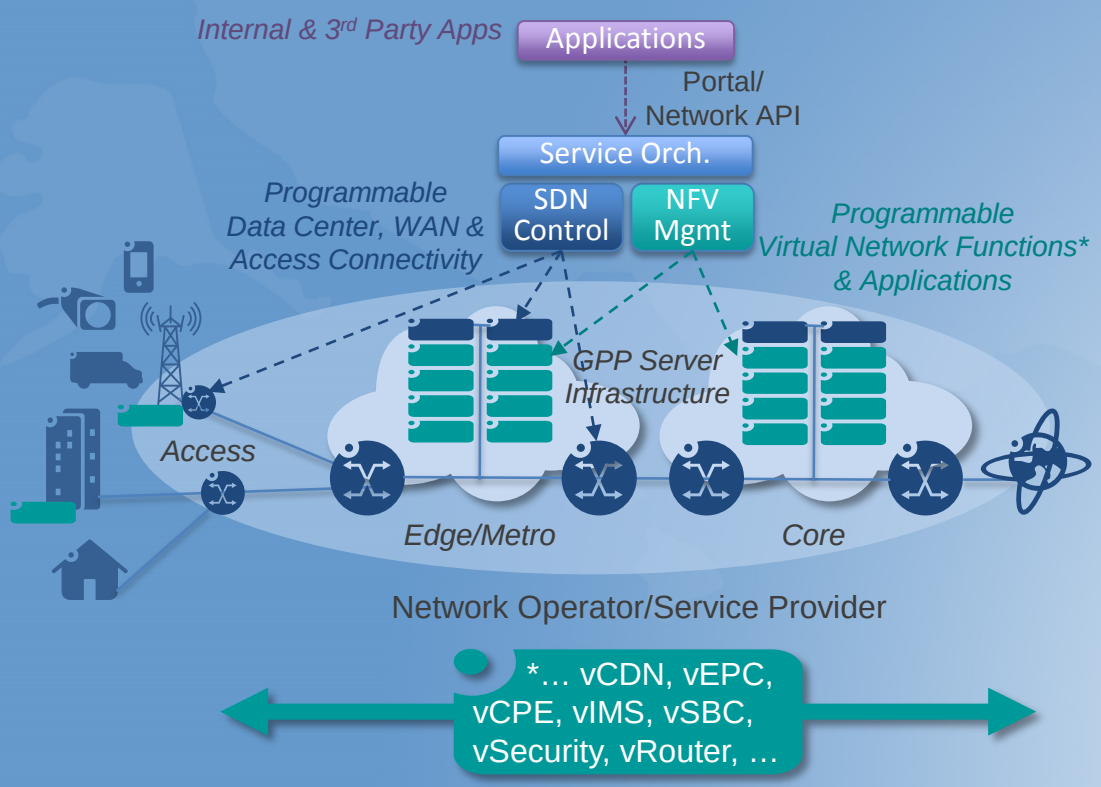
# Programmable Networks – Impact on the Industry

- What changes will they bring to the industry?
- What new business models/relationships may be possible?
- What new types of players will emerge?
- What types of displacements are likely (or possible)?

# How will Programmable Networks change the industry?

- ***Operational efficiency*** – Automated service operations and network optimization … after upfront learning curve & investment
  - low-touch service provisioning, at scale
  - auto-adaptive to traffic and network conditions, allowing higher utilization
- ***Dynamic services*** – Elastic on-demand services will become mainstream
  - wired service automation & self-service more in line with wireless services
  - increased use of Internet overlay VPNs for enterprise locations
- ***Consolidation*** – Automated "networks" tend to accentuate operational performance differences and economies of scale
  - parallels in other industries (on-line retail, travel, package delivery, etc.)

# SDN/NFV Operator Benefits & Challenges




**Benefits**

- Flexibly reusable components
- Rapid new service development
- Automated operations (high scale at lower cost)
- Dynamic on-demand services
- Shorter network update cycles

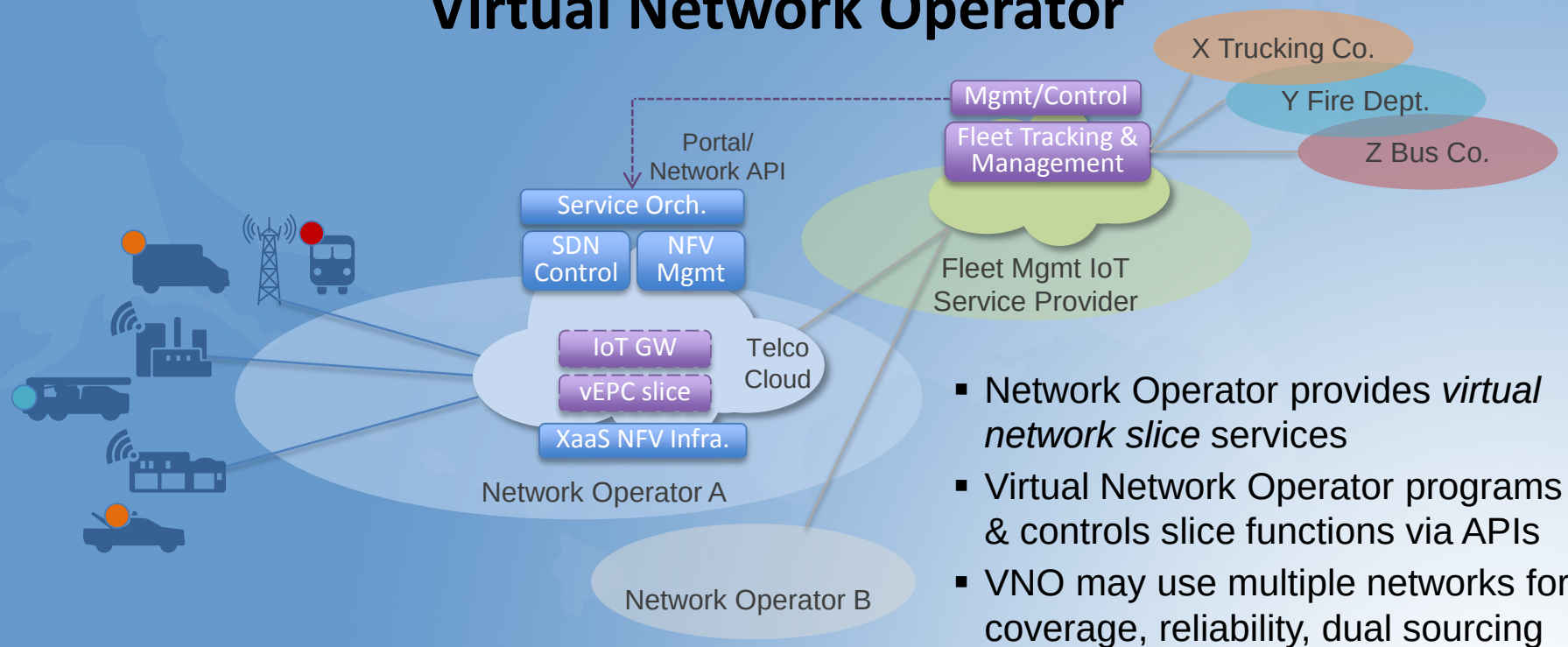
**Challenges**

- ‘Maturing’ standards/open source
- Adapting legacy infra & OSS/BSS
- Federating across operators
- Skill set changes

# How will Programmable Networks change the industry?

- ***New players*** – Disruption opens opportunities for green-field entrants, unencumbered by legacy infrastructure/operations
  - new forms of service/network providers with little to no owned infrastructure
  - potential "Uberization" of network services, starving infrastructure investment
- ***Ecosystem*** – Opens many opportunities for shared value chains between network and service providers
  - New types of virtual network operators (IoT verticals, range of MVNO-like models)
  - New low latency application providers (augmented reality, gaming, etc.)
  - New high bandwidth application providers (e.g. high resolution mass video analytics)
  - Consortiums and exchanges to deliver automated services with global reach

# Programmable Network Example: Virtual Network Operator

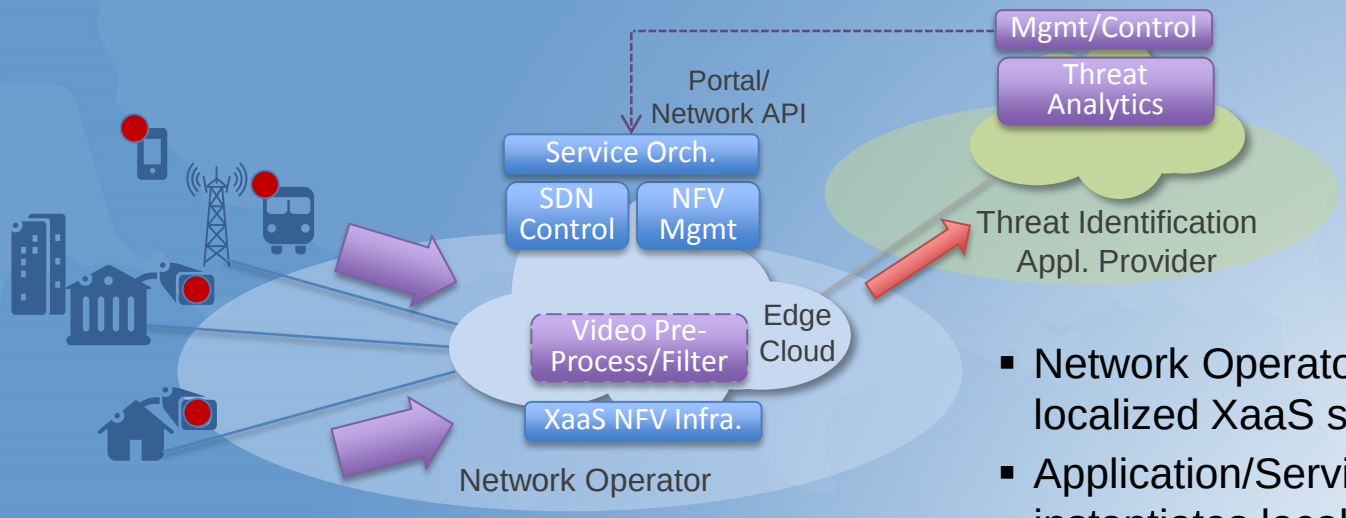



- Network Operator provides *virtual network slice* services
- Virtual Network Operator programs & controls slice functions via APIs
- VNO may use multiple networks for coverage, reliability, dual sourcing

# How will Distributed Edge & Compute change the industry?

- ***Content Delivery*** – Distributed edge enables further distribution of CDNs
  - localized delivery enhances QoE performance, reduces core network overbuild
- ***Low Latency Apps*** – Edge compute = high performance apps ecosystem
  - new low latency application providers (augmented reality, gaming, etc.)
  - edge can even extend to base stations for extreme low latency "Tactile Internet"
- ***High BW IoT*** – Efficient local processing of massive sensor data volume
  - localized analytics for performance and network efficiency
  - new high bandwidth application providers (e.g. high resolution mass video analytics)
- ***Advanced Virtual Networks*** – Enables localized vNFs as part of NaaS slice
  - extends benefits of localization to service providers w/o local infrastructure

# Distributed Edge & Compute Example: IoT Vertical Application Provider




- Network Operator provides localized XaaS services
- Application/Service Provider instantiates local functions via APIs
- Both parties benefit from performance and efficiency gains

# 5G – Impact on the Industry

- What changes will they bring to the industry?
- What new business models/relationships may be possible?
- What new types of players will emerge?
- What types of displacements are likely (or possible)?

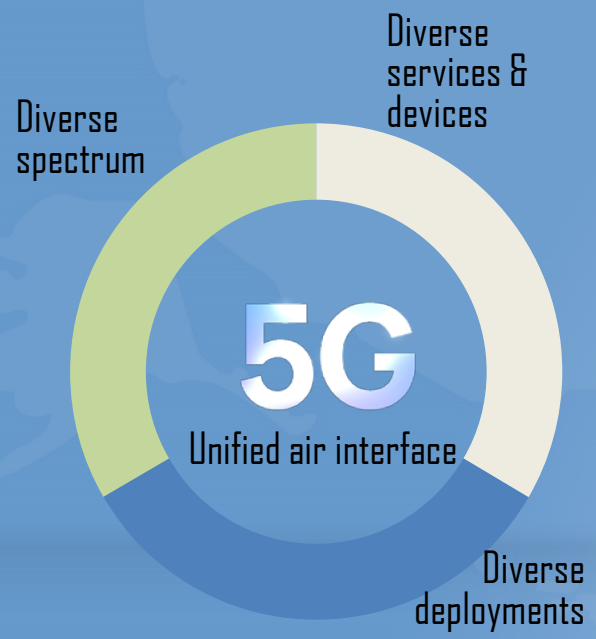
# How will 5G change the industry?

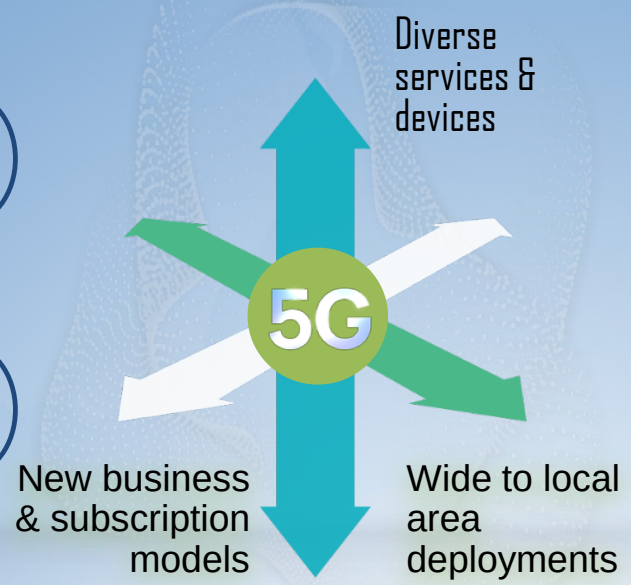
- Broad consensus on requirements
  - *Improvement in key dimensions to handle diverse demands*
  - *Use cases: enhanced mobile broadband, IoT, and mission critical applications*
- Requires spectrum above and below 6GHz
  - *5G designed from scratch for all spectrum types, from pure licensed to shared to pure unlicensed*
- Provide increased Capacity, Efficiency, Scalability
- Multi-connectivity
  - *Always best-connected 4G/5G/Wi-Fi,...*

# How will 5G change the industry?

- 5G is an end to end network transformation, not just a new radio access
- New radio interface unconstrained by previous designs
  - *OFDM based waveform, flexible framework to handle wide ranging requirements*
  - *Massive MIMO, increased spectral efficiency with spatial diversity*
  - *Integrated access and backhaul.*
- 5G standardization has started in 3GPP
  - *Planning for initial deployments around 2020.*

# Flexible end-to-end 5G system architecture






OFDM-based waveforms under a flexible framework that scale to support extreme variation of requirements

Multi-connectivity Framework

Simultaneous connectivity and aggregation across access technologies

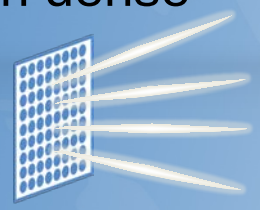
Flexible Network Architecture

Configurable connectivity with distributed network functionality to dynamically create services.

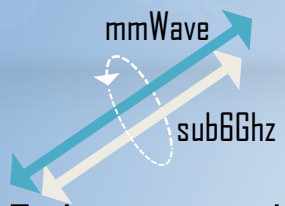
# “mobilizing” mmWave

- Large bandwidths, e.g. 100s of MHz
- Multi-Gpbs data rates
- Flexible deployments (integrated access/backhaul)
- High capacity with dense spatial reuse

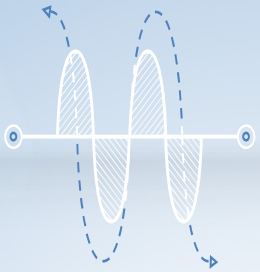
- Robustness due to high path loss and susceptibility to blockage
- Device cost/power and RF challenges at mmWave frequencies



Smart beamforming & beam tracking

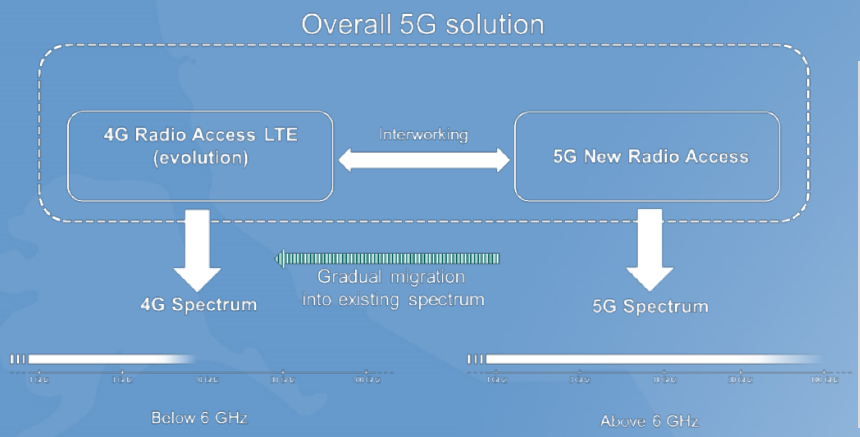


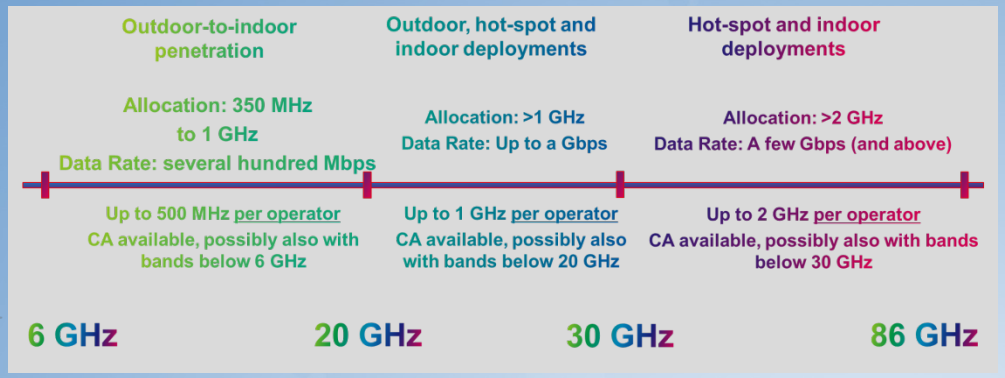

Tight interworking with sub 6 GHz



Optimized mmWave design for mobile

# Diverse Spectrum Assets for 5G

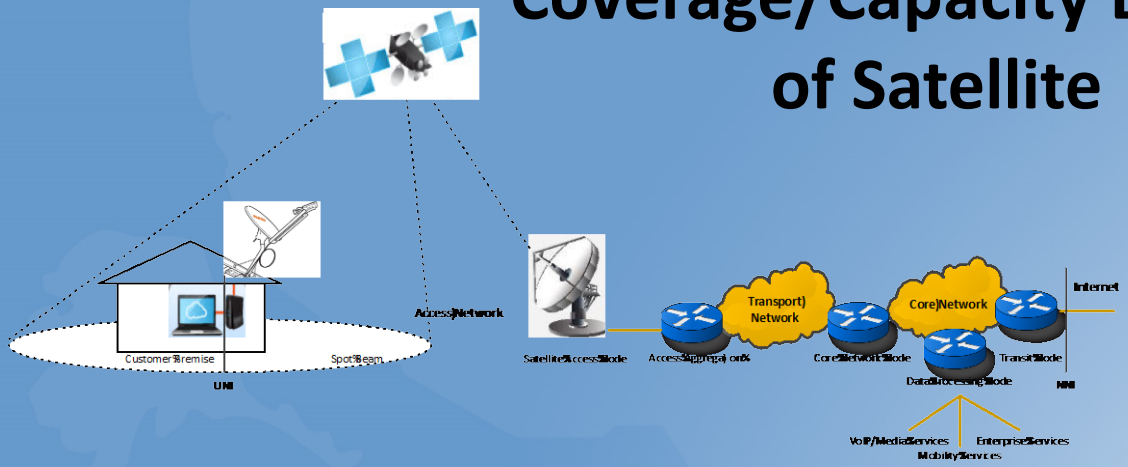



- Extreme Mobile Broadband (xMBB) needs diverse spectrum assets to balance coverage and capacity requirements to meet demand
- xMBB features:
  - Scalable OFDM for freq. and BW flexibility
  - adaptive beamforming and beamsteering
  - Interference reduction and improved SNR

- Sub 6 GHz: Needed for capacity and eventual coverage (5G)
- 6-20 GHz: Still possible to provide outdoor-to-indoor coverage and crucial for 5G
- 20-100 GHz: Separation of outdoor and indoor, smaller cells, dense deployment, high targeted capacity

# Coverage/Capacity Benefits of Satellite




- FSS Broadband satellite capacity & economics are improving year over year
- NGSO satellite capacity is increasing and capacity economics are improving
- Broad coverage for serving rural areas
- Hybrid networks address latency issues
- SDN/NFV improves feasibility of hybrid networks, makes capacity more elastic
- FCC needs to be sure current rules do not hinder adoption of satellite as a competitive alternative

# Programmable Networks & 5G - Impact on FCC Roles & Goals

- What environments should the FCC be encouraging?
- What should the FCC do to encourage innovation?
- What should the FCC do to avoid discouraging innovation?

# How will Programmable Networks impact the FCC?

- ***Virtual Networks*** *(VNs)* – Network slicing will facilitate many new forms
  - federal certification required only of facilities-based networks (FBN)
    - but CALEA rules will apply to VNs
  - VNs which provide BIAS will be classified as common carriers under OI
    - outage reporting may become more complex (more variations)
  - VNs that use slices from multiple FBNs may increase wholesale competition
  - key question: When do responsibilities of an FBN transfer to a virtual network?
- ***Dynamic environment*** – VNs can instantiate, expand, & contract rapidly
  - common carrier classification/definition may need updating
  - processes (e.g. CALEA, 911 establishment) will need to be streamlined/automated
  - rules regarding VN vs. FBN responsibilities will likely need refinement

# How will Programmable Networks impact the FCC?

- ***Open Internet*** – Largely indirect impacts of network slicing
  - generally *managed* resource slices (w/SLAs), separate from Internet traffic
    - in shared pipes, managed/private and Internet aggregate capacity limits must be managed
  - programmable networks will enable higher QoE for Internet apps via localized IaaS
    - e.g. distributed CDNs, low latency applications
- ***Network metrics*** – SDN-based implementations open some new options
  - centralized network resource management provides a more global view
  - facilitates flexible placement of virtual monitoring points, and better "top-down" collection of aggregate usage metrics
  - doesn't resolve issues of mass fine-grained data volume and storage

# How will 5G impact the FCC?

- ***Spectrum policy***
  - Larger blocks across a wide range of bands
  - Consideration of licensed, unlicensed and shared licensed access
- ***Broader 5G policy questions***
  - Internet policy with Gigabit access via mobile networks
  - Support for massive IoT and mission critical applications
  - Support for new business models
- ***Reliability and Security***
  - Native support for applications requiring high reliability, extremely low latency, and high security.

# Future Game Changing Technologies

# WG Recommendations

# FGCT Recommendations – Programmable Networks

- FCC would greatly benefit by building up SDN/NFV and Programmable Networks technology & applications awareness and expertise
- Lower FCC barriers to Programmable Networks-driven innovation and economic growth
  - Evaluate dynamics of FCC processes against needs of dynamically elastic service providers
  - Evaluate challenges of establishing FCC mandated functions in a fluid SP environment
    - CALEA, 911,outage reporting, etc.
  - Review rules for when Facilities-Based Network requirements apply to Virtual Networks
- Proactively seek ways to bring programmable network service benefits to non-prime markets
  - Consider application of 'universal service' funds for establishing edge cloud 'XaaS-enabling' infrastructure in rural areas

# FGCT Recommendations – 5G & Satellite

- Leverage Prog. Networks & 5G to scale and enhance wireless Internet & IoT
  - All-in spectrum approach (low bands, high bands; licensed, unlicensed, LSA, 3-tier)
  - Maximize capacity and reliability via multi-band optimization
  - Balance coverage and capacity for high bandwidth systems through spectrum allocation
  - Avoid spectrum policy barriers to maximizing utilization via intelligent integrated multi-band, multi-connectivity
  - Encourage investment in high capacity, high spatial reuse localized cells
- Leverage 5G, NGSO satellite, & programmability for broad coverage benefits
  - Maximize coverage and QoE to rural areas via hybrid connectivity (e.g. cellular/satellite)
  - Satellites for global coverage of critical functions where the highest data rates are not required
- Applications specific performance requirements should be accommodated using common wireless infrastructure

# FGCT Overall Recommendations (1/2)

***With such sweeping and accelerating changes, it is 'mission critical' that the FCC fully understand, adapt to, and promote the impending technological transformation of networks***

**Awareness/Expertise**

- Ramp FCC technical/business capability to anticipate & understand transformational FGCTs
- Continue to tap industry, academic, and government sources of expertise by creating venues and conducting emerging tech reviews
- Continue to monitor global efforts, focused on infrastructure and smart cities
- Openly disseminate findings/analysis, including an annual "hotlist" of emerging technologies

**FCC Policy & Process Agility**

- Review existing rules and regulations to identify, eliminate or modify those that have been made obsolete by technological advances
- Ensure that policies, rules and regulations do not hinder fast-paced FGCT-driven innovation, investment, and competition

# FGCT Overall Recommendations (2/2)

***With such sweeping and accelerating changes, it is 'mission critical' that the FCC fully understand, adapt to, and <u>promote</u> the impending technological transformation of networks***

**<u>Encouraging Innovation</u>**

- Encourage better utilization of network resources via programmable consumption and optimization
- Consciously and explicitly evaluate actions going forward with agile, programmable networks and dynamic service/network ecosystems in mind
- Maintain technology neutral stance, allowing new services demand to be met by market forces

**<u>Leveraging FGCTs for Rural/Underserved</u>**

- Needs of disenfranchised parts of the market for essential services should be accommodated through appropriate incentives
- Continuously examine the National investments it spearheads to maximize leverage of FGCTs

# Suggestions for Next Year's TAC

- WG suggests continued analysis for FGCT focus technologies
  - Maturity of technologies underlying 5G and impact on spectrum policy
  - Scenario analysis of new business models and regimes
  - Assessment of current FCC rules, policies, … w.r.t. dynamic, programmable networks
  - Scanning for new emerging technologies
- Demand drivers should be revisited, ensuring that innovation is encouraged to meet the FCC's goals of technology leadership and economic growth
- WG focusing on technologies for global ubiquitous coverage (including rural)

danke
謝謝
ngiyabonga
teşekkur ederim
спасибо
thank you
gracias
dziękuję
obrigado
sukriya
go raibh maith agat
merci

# Roadmap for Future Unlicensed Services Working Group

Chairs: Mark Bayliss, Milind Buddhikot

Vice Chair: John Barnhill

FCC Liaisons: Michael Ha

December 9, 2015

## Working Group Members

- WG Co Chairs: Mark Bayliss, Milind Buddhikot

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

- Members:
  - John Barnhill, GENBAND
  - Mark Bayliss, Visualink
  - Nomi Bergman, Brighthouse
  - Milind Buddhikot, Bell Labs
  - Adam Drobot, Open Techworks
  - Dick Green, Liberty Global
  - Russ Gyurek, Cisco
  - Jeff Foerster, Intel
  - Theresa Hennesy, Comcast
  - Farooq Kahn, Samsung
  - Jack Nasielski, Qualcomm
  - Mark Racek, Ericsson
  - Brian Markwalter CE.org

## Roadmap for Future Unlicensed Services

Unlicensed services have played an unexpectedly vital role in the evolution of communication capabilities and in providing a 'wireless commons' for innovation. It is critically important for the Commission to understand both the potential pathways for continued evolution of unlicensed services as well as potential threats to the continued viability of the 'commons'.

## Work Group Focus

(1) Evolving and novel applications
- (e.g. low power WANS, internet-of-things (IOT), unlicensed LTE).

(2) New business models
- (e.g. managed vs. unmanaged vs. private, indoor-only services).

(3) New candidate spectrum bands to increase available spectrum.

(4) Voluntary etiquettes for unlicensed service applications that will help protect the commons model

(5) The potential impact of present EMC limits for consumer and industrial devices on the continued growth and vibrancy of unlicensed services.

**$220B**

*Annual economic activitiy due to unlicensed spectrum

**$62B**

**Annual Retail Sales of Wi-Fi Devices USA

**48%**

%Total IP Traffic over Wi-Fi in 2019, up from 33% in 2014

**66%**

by 2019

% of Mobile Originated IP Traffic Over Wi-Fi - Up from 57% in 2015

**53%**

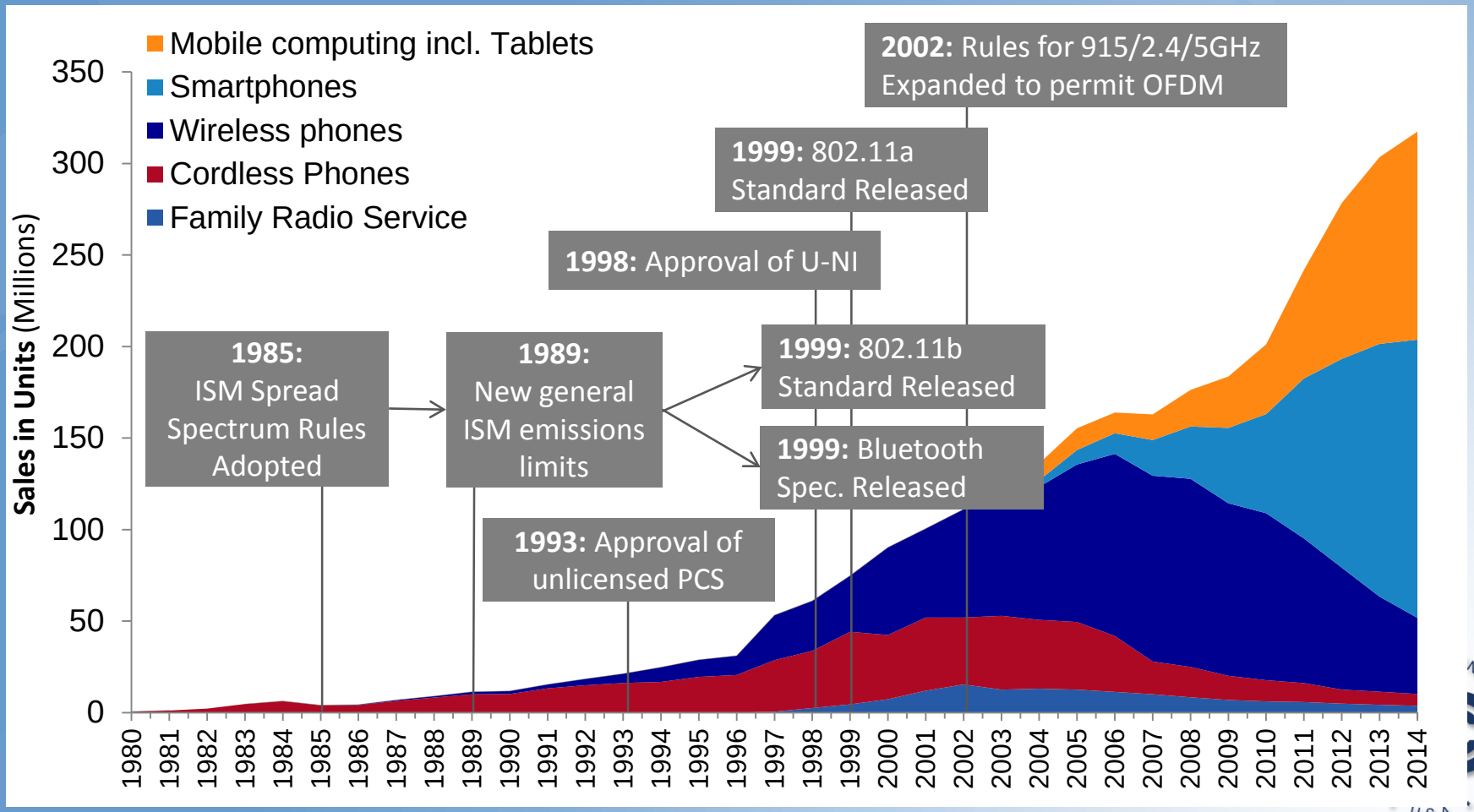
% of VoIP traffic originating on Wi-Fi vs LTE by 2018

Graphic Courtesy NCTA.org

*Telecom Advisory Services , Jan 2014, wififorward.com

**UNLICENSED SPECTRUM AND THE U.S. ECONOMY, June, 2014, ce.org

# Unlicensed Spectrum Growth - Selected Categories




Source: http://www.ce.org/CorporateSite/media/gla/CEAUnlicensedSpectrumWhitePaper-FINAL-052814.pdf

## Presidential Memorandum:
## "Unleashing the Wireless Broadband Revolution", June 28, 2010

(a) …make available a total of **500 MHz** of Federal and nonfederal spectrum over the next **10 years**, suitable for both mobile and fixed wireless broadband use.

The spectrum must be available to be licensed by the FCC for **exclusive use** or made available for **shared access** by commercial and Government users in order to **enable licensed or unlicensed wireless** broadband technologies to be deployed;

# Unlicensed Spectrum Action Summary

| 2012 | 2013 | 2014 | 2015 | 2016 |
|---|---|---|---|---|
| Spectrum Act - *Includes 5GHz band for unlicensed* (Mar 2012) | Aug 2013: Modified Part 15 rules for 60GHz band to improve unlicensed usage | Mar 2014: FCC adopts rules improving use of 5GHz for unlicensed | Apr 2015: 3.5GHz Order 100MHz *Licensed by Rule*; Spectrum Frontiers NPRM (Nov 2015) | Mar 2016: 600MHz Incentive Auction |

# Spectrum Available for Unlicensed Applications

| Band | Current | Pipeline | Comments |
|---|---|---|---|
| TV White Spaces | 0-150 | + | Future TV White Space availability subject to results Incentive Auction |
| 902-928 MHz | 26 | - | |
| 2400-2483.5 MHz | 83.5 | - | |
| 3550-3700 MHz | 150 | - | Licensed-by-rule under Part 96 - April 2015 |
| 5150-5350 and 5470-5825 MHz | 555 | | |
| 5350-5470 and 5850-5925 MHz | | 195 | Proposed U-NII-2B and U-NII-4 bands are under discussion |

Currently an additional 7GHz is available in the 60GHz band (57-64, +7)
Plus there are other bands spread out that use unlicensed

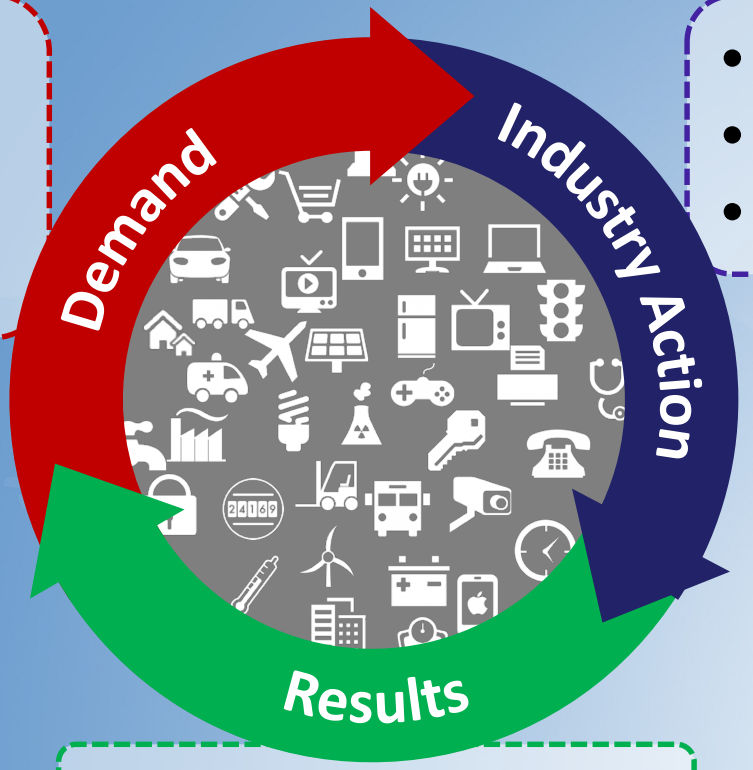
+ Represents where multiple initiatives are underway but additions aren't quantified

Please note that this is for unlicensed broadband use and there are more spectrum available for other unlicensed applications

# Unlicensed Spectrum – Demand Growth Cycle

- Increased Traffic
  - More Users, Devices
- New Providers
- Better Prices

- *Service Providers*
- *Enterprises*
- *Consumers*




- More Spectrum
- Better Sharing
- Effective Etiquette

*Technology & Policies evolve as needed to ensure usability*

*Availability Stimulates Usage and Services*

- Increased Capacity
- Better Utilization

# Industry Engagements

## Service Providers

verizon

T-Mobile

Sprint

## Associations

atis

WiFi ALLIANCE

WISPA
Wireless Internet Service Providers Association

## Equipment

QUALCOMM

UBIQUITI NETWORKS

## Standards Bodies

IEEE 802.15

## Key Observations from Industry Interviews

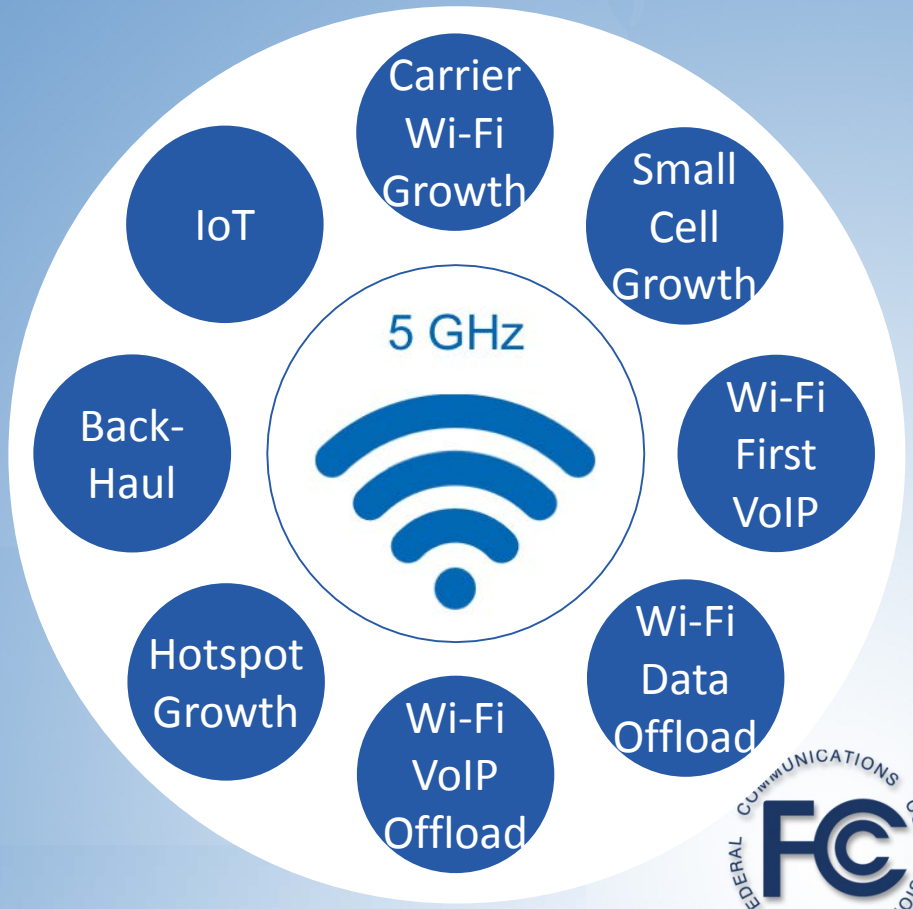
### Demand Drivers

1. Growth in connected devices from users and things
2. Growth as carriers, users, gov, & enterprises add coverage
3. Communications app growth & Wi-Fi First mobile providers
4. Licensed providers shifting traffic to unlicensed spectrum
5. Unlicensed spectrum economics

- General Agreement:
  - More Spectrum is needed; licensed and unlicensed
  - Light-touch regulation preferred
- Over subscribed bands –
  - 900 MHz, 2.4 GHz, with concern about 5GHz
- Life-essential services have emerged using unlicensed spectrum
  - E.g. traffic control

## Increasing Demand for 5GHz Services

- Spectrum will be shared by both Wi-Fi and LTE variants
  - Agreement that mechanisms are needed to ensure fair co-existence
  - Industry Groups engaging with each other and FCC to resolve
- Interested parties responding to commission ET 15-105.
  - Working group will defer specific technical recommendations as this is an open proceeding



# Carrier Wi-Fi Growth – Primary Use Cases

## Extended Voice Footprint

**T-Mobile**

11M Wi-Fi

Calls per day

Infoworld Online 8-27-15

T-Mobile

Sprint

verizon

**Wi-Fi–First Carriers**

Project Fi

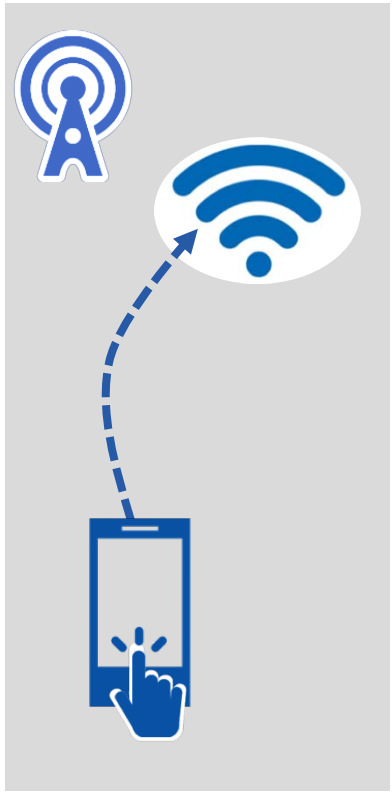
republic WIRELESS

FREEWHEEL

FreedomPop

SCRATCH WIRELESS

## Cellular Data Offload



**2018 Wi-Fi**

expected to contribute **20%** additional mobile data capacity plus **21%** additional from small cells

(Wireless BB Alliance)

## Factors Evaluated

- More dedicated spectrum for unlicensed usage
- More efficiently share available spectrum
- Better utilize allocated spectrum (spectral efficiency) by managing interference potential of certain applications
- Co-existence between competing technologies with bands

# Relieving Congestion: More Spectrum

**Additional Spectrum Allocations**

- Additional Spectrum for unlicensed (64-71GHz from the Spectrum Frontiers NPRM)
- Potential sharing with other users (certain restrictions may be required); FSS/FS/AMT services could be examples; potential use of database similar to 3.5GHz SAS)
- Enforcement issue may be considered

**Better Unlicensed Spectrum Utilization**

- High price tag of licensed bands drives the spectral efficiency
- Traditionally, capital efficiency/simplicity triumphed the spectral efficiency for unlicensed band
- Is there room for additional capacity in the unlicensed band?

# Avoiding Congestion: Improving Utilization

**Current FCC Rules**

- Everyone has an equal right to transmit as long as each transmitter satisfies the relevant Part 15 rules
  - Overlapping usage patterns are potential problems (similar usage leads to coexistence challenges)
- Unlicensed band transmitter cannot cause harmful interference to licensed band user and must accept interference
- Industry standard organizations often balance the "spectral efficiency" and "capital efficiency" for a given app (but usually not "cross-application")

**Application Compatibility**

- Likely Performance Indicators
  - Indoor vs. Outdoor?
  - Long range vs. Short range?
  - Wide BW vs. Narrow BW?
  - High Duty Cycle vs. Low Duty cycle?
  - Apps that can't perform under interference conditions may not be suitable for bands under unlicensed rules.
    - Life-critical services – Traffic Systems
    - Utility Services
- High duty cycle + Wide Bandwidth + Medium to Long Range will create likely sharing challenges.

# Considerations for Avoiding Congestion: Greater Spectral Efficiency

**Technical Rules**

- The rules have been in place for decades and seem to have served the industry well
  - Part 15 – Must accept Interference and not cause harmful interference to licensed users
- In shared bands with licensed incumbent users, different rules may apply

**FCC Policy**

- Which applications or areas of FCC rules would deliver the most value?
- What are the future areas of interest on the TAC WG for enhanced efficiency?
- How should the Commission interact with standards organizations to enhance spectral efficiency and ensure adequate co-existence?

Acknowledging continuous technology advancement, should the Commission routinely revisit rules to enable greater efficiency?

# RECOMMENDATIONS

## Part 15 Rules

CONNECTING AMERICA:
THE NATIONAL BROADBAND PLAN

*…the creation of the flexible Part 15 rules allowed for the growth and proliferation of unlicensed devices…*

5.6 “Expanding Opportunities For Innovative Spectrum Access Models" Page 94

Consensus: Between rules and certification testing, we believe additional Part 15 rules are unnecessary at this time. However, technology changes are constant and the commission should continue to monitor.

## Recommendations #1: More Spectrum

- Evaluate bands between 6GHz and 57GHz to address the demand for unlicensed spectrum
  - Propose initially 1GHz of spectrum for (exclusive or shared) unlicensed use to bridge the benefits of propagation characteristics of 5GHz and 60GHz bands
- Accelerate proceeding to release 7GHz of additional bandwidth above 64GHz for unlicensed spectrum.

## Recommendations #2: Better Sharing (Unlicensed/ Licensed)

- Promote spectrum sharing between unlicensed/ licensed bands
  - When evaluating candidate bands, Commission and NTIA should consider unlicensed applications and encourage other agencies to add this consideration to all future spectrum studies.
  - Identify specific bands to study, including FSS (Earth to Space), FS, AMT, EESS/SR/RAS and others
  - Identify restrictions (i.e. lower transmit power, geographical restrictions, etc) that could potentially increase shared bandwidth
  - Consider initial deployments with controlled usage (i.e. factories vs. general consumers) with database-like approach

## Recommendations #3: Spectral Efficiency

- Consider rules to improve spectral efficiency as new/shared unlicensed bands are released while retaining flexibility
  - Include physical layer characteristics, protocols for interference mitigation, and the overall performance
  - These concepts and questions to be included during the future unlicensed band rulemaking process
- Encourage an industry-led effort to develop a Best Practices Guide for unlicensed operation for current and new applications. (Similar to licensed wireless and public safety communications guides)
- Once proven to be effective, consider applicability to existing unlicensed bands

## Recommendations #4: Industry Co-existence

- Promote industry-driven co-existence across various standards in unlicensed bands
  - Consensus: Existing model has worked well
    - Simple technical rules and reliance on industry standards bodies to promote the efficient use and co-existence
    - As bands get more crowded, co-existence among various standards can provide more efficient use

# THANK YOU

# Mobile Device Theft Prevention WG
# Report to the FCC TAC

**December 9, 2015**

# Contents

- Mission
- FCC Request for Further Advice
- Results & Conclusions
  - On-device Theft Prevention Features
  - IMEI Hardening
  - Database
- Recommendations
- Next Steps

# 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

- Asaf Askenazi, Qualcomm
- Jay Barbour, Blackberry
- Alan Bersin, DHS
- Brad Blanken, CCA
- Jeff Brannigan, DHS
- Matthew Bromeland, Metropolitan DC Police Department
- Craig Boswell, Hobi
- Eric Feldman, ICE/Homeland Security Investigations
- Thomas Fitzgerald, New York City Police Department
- Les Gray, Recipero
- Shelley Gu, Microsoft
- Joseph Hansen, Motorola
- Jamie Hastings, CTIA
- Joe Heaps, National Institute of Justice
- Gary Jones, T-Mobile
- Sang Kim, LG

- Jake Laperruque, Center for Democracy and Technology
- Irene Liu, Lookout
- John Marinho, CTIA
- Samuel Messinger, U.S. Secret Service
- James Moran, GSMA
- Jason Novak, Apple
- Kirthika Parmeswaran, iconectiv
- Greg Post, Recipero
- Deepti Rohatgi, Lookout
- Mark Romer, Asurion
- Mike Rou, eBay
- Matt Rowe, Gazelle
- Christian Schorle, FBI
- David Strumwasser, Verizon
- Maxwell Szabo, City and County of San Francisco
- Ron Schneirson, Sprint
- Samir Vaidya, Verizon Wireless

# MDTP WG Mission

- Emphasis will be on longer term initiatives that will combat more sophisticated theft scenarios
  - Developing recommendations on next generation anti-theft features
  - Processes including recommendations for hardening of existing device identifiers and the possible need for new, more secure identifiers
  - Security mechanisms with higher consumer acceptance (e.g. biometrics)
  - More focused analysis of overall theft ecosystem including how stolen devices re-enter the marketplace (e.g. recycling industry).
  - Further recommendations on improved reporting mechanisms

- Consideration will also be given to the efficacy of extending theft prevention mechanisms to other classes of devices.

- Provide an assessment of progress made in the area of device theft prevention as some of these recommendations have been applied

# FCC Requests for Further Advice

At the initial 2015 meeting of the TAC, the FCC Chairman requested the MDTP WG consider the following tasks (details as provided by the FCC are in the backup material), :

- Task 1 – On-Device Theft Prevention Features Template
- Task 2 – Hardened Device Identifiers
- Task 3 – Database

Tasks 1 and 2 - an interim report was provided May 1, updated report Dec 9

Task 3 – report presented Dec 9

# Task 1 Update - On-Device Theft Prevention Features

- As reported in September, Chairman Wheeler asked CTIA to update its voluntary commitment to include "opt out“ functionality, as well as all of the MDTP WG’s other recommendations.

- CTIA and Participating Wireless Companies Announce New Effort to Help Consumers Combat Stolen Smartphones and Protect Personal Information - October 2, 2015.
  - The Commitment updates are in section B part I, which promotes the widest possible adoption of anti-theft tools while respecting the importance of consumer choice and privacy.
  - In addition, CTIA developed a list of apps to locate, erase and/or lock, many of which are free, for the various operating systems.
  - CTIA also created step-by-step video instructions on how to set up a PIN/password on various mobile devices.

## Chairman Wheeler's Statement

- "CTIA and its members understand that smart-device theft remains a serious problem. **Their enhanced voluntary commitment to adopt anti-theft features and educate consumers demonstrates their resolve in combatting it. I am encouraged that the industry has taken action in response to the recommendations recently submitted by the FCC Technical Advisory Committee's stolen phones working group, and I am hopeful that this new voluntary commitment will make a meaningful difference for consumer safety**. **As the enhanced commitment recognizes, these solutions work only if they are adopted widely.** The FCC will remain vigilant in this area by pushing for further improvements to the theft-prevention toolbox, and also by monitoring closely whether the efforts of industry and others are producing meaningful results."

# Task 1 - Two Types of On-device Anti-Theft Features

- First type is a passive “background feature” – like Reset Protection, Activation Lock, Reactivation Lock, on device passcode and encryption, etc.
  - That is enabled at initial device activation (or subsequently) by the authorized user.
  - These background features place the device in a constant state of protection, without any additional user action regardless of theft/loss.

- Second set of anti-theft features are remote lock/erase and require additional user action after a device is lost or stolen in order to be triggered (e.g., going to a website to activate the action).

# Task 1 - Comparison of Anti-Theft Tools (“Template”)

| Anti-Theft Tool: | CTIA Commitment | California Law (SB962) | Minnesota Law | Working Group View |
|---|---|---|---|---|
| **Date: July 2015** | Required | Required | Required | Required |
| **Smartphones** | Required | Required | Required | Required |
| **No Cost to Consumer for devices sold at retail** | Required | Silent | Required | Required |
| **For retail sale, preloaded** | Required if not Downloadable | Required if not Downloadable | Required if not Downloadable | Required if not downloadable with no additional purchase |
| **For retail sale, downloadable** | Required if not Preloaded | Required if not Downloadable | Required if not Preloaded | Required if not preloaded with no additional purchase |
| **“shall include a technological solution at the time of sale”…….. “once initiated and successfully communicated to the smartphone” - SB962 Sec 2 (b) (1)** | Required | Required | Required (“sold or purchased in MN” S.F. No. 1740, 2014) | Required |
| **Remote Wipe** | Required | Silent | Silent | Required |
| **Allow the Authorized User to Render Essential Features Inoperable to Unauthorized Users Once Communicated** | Required | Required | Silent | Required |
| **Continue to function for 911 calls** | Required | Not incompatible with 911 | Silent | Required |
| **Continue to function for emergency numbers programmed by the user.** | Optional | Unclear | Silent | Optional |
| **Prevent reactivation by unauthorized user including factory reset** | Required to the extent technologically feasible | Required | Silent | Required to the extent technologically feasible |
| **Restore user data to the extent feasible** | Required | Silent | Silent | Required |
| **Reverse inoperability if recovered by authorized user** | Required | Required | Silent | Required |
| **Initial Setup “prompt an authorized user to enable the technological solution” - SB962, Sec 2 (b) (1)** | Silent | Required | Silent | Required |
| **Opt-Out by Authorized User or Authorized User Designee, at any time SB962 Sec 2 (b) (2)** | Silent | Required | Silent | Required |
| **In addition, permit use of additional solutions if available - SB962 Sec 2 (3) (f)** | Required, if available for users’ smartphone | Allows, but does not require | Silent | Allowed but not required |

## Task 1 - GSM Association's Anti-Theft Device Feature Requirements

- GSMA refined and revised the guidance and published an updated version of its "Anti-Theft Device Feature Requirements" on 18th May 2015.
  - GSMA is actively encouraging OS developers and device manufacturers to support the rollout of robust anti-theft features for the protection and benefit of device owners.

- Focused on providing the following features for smartphones:
  - Render essential features of the device inoperable
  - Prevent reactivation of the device unless by the owner or someone authorized by the owner
  - Wipe all user data
  - Allow the authorized user to re-enable their device and restore erased data that was stored to the cloud.
  - Withstand hard reset

- Further updates of its "Anti-Theft Device Feature Requirements" expected in early 2016

## Task 1 - On-Device Theft Prevention Features Conclusions

- Industry has invested significant resources and effort to develop mechanisms to help smartphone owners reduce the impact of smartphone theft and to assist their recovery if they fall victim.
- United States has led the world in seeking device based solutions and initiatives such as the TAC MDTP efforts, wireless providers voluntary commitment to deploy database solutions, the CTIA's Smartphone Anti-Theft Voluntary Commitment, and the introduction of legislative provisions in California and Minnesota have been particularly instrumental in facilitating and promoting the emergence of a range of anti-theft features.
- The availability of anti-theft features on all smartphones is expected to increase following the effective date of the CTIA Voluntary Commitment and the California and Minnesota laws.
- Analyzing trends in consumer usage and obtaining an empirical understanding of consumer usage patterns will provide a data-driven basis for determining whether any further action is needed to increase customer usage of anti-theft features and, if so, provide a clear understanding of factors that either encourage or discourage consumer use.
- In doing so, remedial efforts can be targeted to resolve empirically identified obstacles.

# Task 2 - Hardening of the IMEI

- Mobile network operators have the ability to block specific devices from accessing their networks.
- GSMA Device Security Group is revisiting the entire IMEI security topic as it has already identified this topic as being a priority
  - The work will, at a minimum, involve a review of the technical design principles and reporting and correction process
- GSM Association's North American Regional Interest Group "North American Fraud Forum & Security Group" liaison to the GSMA Device Security Group:
  - Conduct a study to better understand the duplicate IMEI landscape and to what extent IMEI reprogramming is an issue today
  - Review the technical security design principles to assess if they remain fit for purpose or if they need to be updated
  - Consider how the IMEI changing ecosystem can be monitored and reported on going forward
  - Study if IMEI implementation security requirements could be defined in the industry standards and if there is merit to such an approach

# Task 2 - Hardening of the IMEI Conclusions

- The effectiveness of device blocking on mobile networks is dependent on the secure implementation of device identities.
- Mobile technology standards provide that mobile identities must be unique per device and that they must be protected against alteration after the point of manufacture.
  - No details or guidance are provided as to how exactly these security goals are to be achieved
- Significant efforts were made to improve device identifier security with real commitment and engagement by the device manufacturing community
  - These led to a series of initiatives that have been central to improved device identity security levels.
- Following detailed analysis, industry concluded that standardization is unsuitable as a means to deal with device identity issues and that incorporating enhanced security features in the standards could be problematic and undesirable.
  - Standardizing the technical means to protect device identities could expose devices to even greater risk if the prescribed safeguards are compromised as that would expose all devices if one method fits all.
  - Currently, OEMs and chipset suppliers have different security implementations, some better than others, but mandating a single solution would most likely remove the enhanced level of protection offered by some manufacturers.

# Task 2 - Hardening of the IMEI Conclusions (continued)

- GSM Association led the development of two major industry initiatives designed to enhance the security of mobile device identity implementations.
  - 21 of the largest device manufacturers formally signed up to support both initiatives.
  - Number of devices with vulnerable identities had decreased by 77%, the number of manufacturers with vulnerable products reduced by 45% from 11 to 6 and the number of available and effective hacking tools had shown a 72% decrease.
  - Problems did persist with two manufacturers that, between them, accounted for 83% of compromised device models and their failure to respond appropriately to reported security problems was regrettable.
- Modification of device identities is a criminal offence in some jurisdictions but not in the United States where websites and outlets exist and are on the increase that openly advertise the ability to change device identities.
  - Developers of attacks against device identities are known to the based in the USA, Israel, India and Eastern Europe.

## Task 2 - ATIS Best Practices for Obtaining Mobile Device Identifiers

- ATIS standards effort resulting from TAC MDTP WG recommendation in December, 2014:
  - Recommendation 1.5: The FCC TAC recommends that ATIS in coordination with other appropriate industry groups (e.g., GSMA-NA Regional Interest Group) be tasked with developing standards, methods and procedures to obtain device identifiers from smartphones including those which are locked or rendered inoperable.
  - Published in October 2015
- Device Disabled By Owner Initiated MDTP Procedures
  - Recommended that upon disabling of a mobile device the mobile device display screen show the device IMEI
- IMEI Display on Disabled or Locked Devices
  - Objective is to provide a method where access to the device IMEI does not require specific knowledge of a proprietary user interface
  - Examples could include:
    - When an emergency call is initiated from a device locked screen or a device disabled screen, a pre-call window (emergency dialogue box) appears asking the user if they really want to make an emergency call. In that dialogue box the IMEI can be displayed
    - The IMEI could always be displayed on the device locked or device disabled screen
- IMEI Display on Unlocked Devices
  - Enter *#06# into the mobile phone

# Task 3 – Database

- Working Group studied various use cases to shape the requirements for a database
  - Law Enforcement Use Cases
    - Victim reports stolen device to law enforcement
    - Law Enforcement comes into possession of one or more cell phones in the field
    - Law Enforcement comes in contact with smartphone robbery victim
  - Consumer Use Cases
    - Consumer's device is lost
    - Consumer's device is stolen
    - Consumer wants to purchase a cell phone through online reseller
    - Consumer wants to purchase a cell phone through a storefront or private party
  - Resellers of 2nd Hand Devices Use Cases
    - Device presented to a reseller for recycling
    - Bulk devices are presented to a reseller for recycling

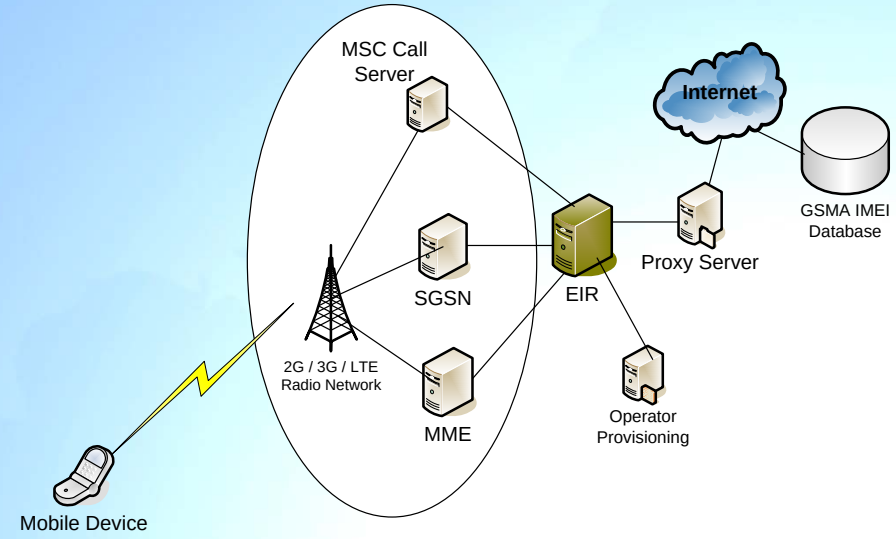
# Task 3 – Database Solutions

- Database solutions may be characterized into the following categories:
  - Databases used by network operators containing device identifiers which are used to deny access to known stolen devices on their networks
  - IMEI/MEID Database provided by the GSM Association to facilitate the sharing and distribution of stolen device identities between mobile network operators
  - Some OEM/OS vendor databases which specify the enrollment state of the on device theft prevention solution
  - Aggregator databases which provide device checking services and/or portals to network operator and OEM/OS vendor databases

- GSM Associations North American Regional Interest Group "Analysis and Recommendations for Stolen Mobile Device Issue in the United States" provides example implementations that can be used by the network operators to deny services for stolen mobile devices on their networks
  - Equipment Identity Register
  - CDR Analysis
  - Network Transaction Trigger

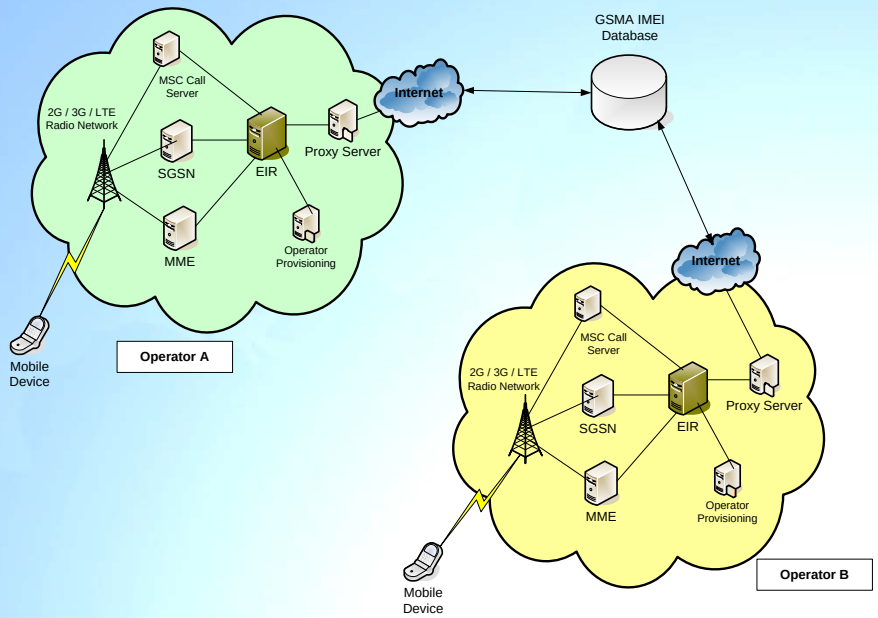
# Task 3 – Database Solutions (continued)

- Equipment Identity Register (EIR) by a wireless operator is the most common network-based implementation to identify and prevent the use of stolen mobile devices
- EIR is a standards-based network infrastructure implementation that has been defined by the 3rd Generation Partnership Project (3GPP), the global standards development organization for the GSM family of technologies



# Task 3 – Database Solutions (continued)

- GSMA's IMEI/MEID Database is based on a data platform run and maintained by the GSM Association
- GSMA Database takes the black lists from the various operators around the world that are connected to system and it compiles the data into one global black list.
- Designed to share stolen device data between network operators to enable them to prevent known stolen devices from being used on any operator network that subscribes to the Database and that has the necessary technology in place within its network to check for and deny service to blacklisted devices



# Task 3 – Database Conclusions

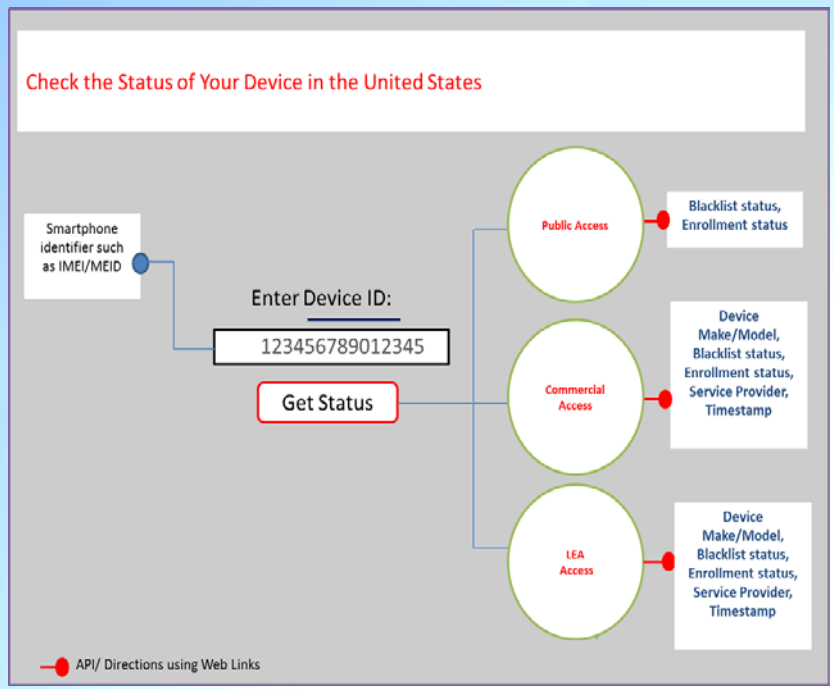
- Law Enforcement related:
  - Across the US, law enforcement officers may not be aware of the significance or existence of the device identifier (IMEI, MEID, etc.)
  - Procedures to obtain the IMEI or ESN on devices vary among manufacturers and this complicates law enforcement abilities to acquire that information. Also, if the device will not power-on, this further complicates abilities.
  - Across the US, law enforcement officers are not fully aware of how to access information that is in the GSMA IMEI Database.
- Consumer related:
  - A fragmented system of consumer outreach exists in which no single government agency, group, manufacturer, or carrier providing a uniform and comprehensive outreach program or source for information.
  - Consumers don't always report the theft of their devices to law enforcement and/or carriers.
  - Consumers need instructions and clarity of the process and procedures for the reporting of stolen devices.
  - Potential buyers of smartphones do not have access to complete information to verify that the smartphone is not a stolen mobile device
    - Potential buyers of smartphones may not understand the importance of identifiers and how to identify their smartphones

# Task 3 – Database Conclusions (continued)

- Mobile device information is dispersed across different stakeholder databases such as local/global blacklists, insurance databases, OEM device check services, MEID/IMEI databases, etc.
  - A lookup across more than one database is required to get comprehensive information.
- Timeliness of information is too long and is dependent on reporting frequency as well as upload/download frequencies of most of the databases.
- Effort is underway within the GSM Association to harmonize the practices and policies of blacklisting devices.
- Many mobile network operators in other countries do not block stolen services or share relevant data with other operators.
  - Consequently stolen smartphones in those countries could still be operational.
- Some US mobile network operators, especially the smaller mobile network operators, do not block devices or share stolen device data

# Task 3 – Database Portal Solution

- Device Information Portal (Conceptual View)
  - Enables stakeholders to get information on how to determine the status of a device using a portal
  - Could be utilized as a platform to provide instructions on how to obtain information about a device and aggregate available device information across different solutions (GSMA, Operator, OEM platform, OS platform and other aggregators) to enable credible, synthesized information to all stakeholders in the mobile ecosystem



# Task 3 – Database Portal Solution (continued)

- Provides consolidated view of information from diverse sources in a uniform and easy to understand fashion.
- Specific to IMEI and MEID to launch query.
- Accessible from the Internet.
- Publicly Accessible at no cost to consumers based on defined number of queries per day.
- Law enforcement accessible at no cost to law enforcement (basic level of service).
- Simple and easy to use UI (User Interface).
- Available around the clock (24X7).
- Limited to queries launched within the US (e.g. US IP Addresses).
- Provides useful consumer advisories in the event of device loss or theft.
- Provides Internet links to mobile device industry resources (e.g. Carrier website, OEM website).

# MDTP WG Recommendations

- The FCC TAC recommends that CTIA – The Wireless Association and the GSM Association, on behalf of the industry, implement the Device Information Portal based on the objectives contained in the TAC MDTP Analysis and Recommendations Report for 2015.

- The FCC TAC recommends that CTIA-The Wireless Association update their ongoing study and research on consumer usage and trends for smartphone security prior to July 2016.
  - In particular, the study should aim to determine whether uptake for anti-theft features continues to improve once the features are available across all new smartphone models that make their way into consumers' hands.

- The FCC TAC recommends that the FCC work with industry on developing effective outreach initiatives to educate the consumer.
  - An example is to create a website/consumer education portal and outreach program that informs users about the anti-theft initiatives and legislation industry is committing to support, and link to each of the smartphone manufacturers' webpages that describe their anti-theft features.
  - Explore the use of social media to expand outreach initiatives

# MDTP WG Recommendations (continued)

- The FCC TAC recommends a deeper investigation by industry into the causal factors for the increase in consumer use of MDTP functions that could be used for determining how to optimize further efforts to incentivize greater consumer use of anti-theft features, if necessary.

- The FCC TAC recommends an industry-led investigation into whether the increased availability of anti-theft functionality on new smartphones as well as the upcoming initial device setup prompts that are required by California legislation have any effect including increasing consumer use of these features.

- The FCC TAC recommends 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: IMEI; Requirements and Use of databases; Future theft prevention opportunities

# MDTP WG Recommendations (continued)

- The FCC TAC recommends industry adoption of the voluntary framework for a set of on-device capabilities to guide industry based on the “working group view” column of the Best Practices Template: Comparison of Anti-Theft Tools.
  - CTIA should maintain a publicly available list of OEMs/OS Providers reflecting the CTIA Smartphone Voluntary Commitment and voluntarily support of the “working group view” column of Table 3.

- The FCC TAC recommends the GSM Association develop a Best Practices/Implementation Guideline for device blacklisting, device blocking, and data sharing.

- The FCC TAC recommends the GSM Association, working with the mobile device manufacturing community, review the 2005 published technical design principles to ensure they remain relevant and take into account current threats and attack scenarios.

# MDTP WG Recommendations (continued)

- The FCC TAC recommends that the GSMA and CTIA coordinate a survey of the US carriers to assess and measure the extent to which invalid and duplicate device identities may be in use on their networks.

- The FCC TAC recommends that the industry reinstate a service to monitor for and report device identity security issues to provide statistical data and to ensure identified device identity problems are notified to the affected device manufacturers.

- The FCC TAC recommends the FCC work with Congress to enact legislation to criminalize the unauthorized changing of device identities and to supply or possess equipment to undertake this activity and it should be enforced and offenders prosecuted as a disincentive to engage in this activity.

- The FCC TAC encourages the FCC to facilitate the convening of Operational Law enforcement subject matter experts to discuss mobile device theft with regard to response, outreach, education, prevention, tactics, best practices, tools, analytics, and collaboration across jurisdictions.

# 2016 Proposed MDTP Topics

- Develop recommendations on next generation anti-theft features to promote widest possible adoption by consumers.

- Continued studies to determine whether implementations post July 2015 have the desired affect on mobile device theft
  - Refers to the planned recurring survey effort for continued monitoring of improvements
  - 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.
    - Consumer adoption rates of background anti-theft features in light of the California requirement and voluntary commitment (effective in July 2015) to prompt users to enable the feature at initial device setup.
    - Better tracking of actual phones stolen – investigate as part of the MDTP working group task 3 deliverable

- Enhanced consumer outreach and education
  - Contribute to  a tutorial on anti-theft features of the different mobile operating systems that lives on fcc.gov
  - Investigate use of social media to amplify outreach and education

# 2016 Proposed MDTP Topics (continued)

- Reporting for Law Enforcement
  - 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.
- Additional methods to increase consumer adoption of anti-theft features
- 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.
- 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.
- Industry to reinstate a service to monitor for and report device identity security issues, to provide statistical data, and to ensure identified problems are notified to the affected device manufacturers

# BACKUP

# Task 1 - On-Device Theft Prevention Features Template

- Password protection, Remote lock/wipe/restore functionality
- Most effective only if they are part of a package of practical solutions that consumers actually use, and today the majority of U.S. consumers don't
- WG asked to explore developing a proposed template approach that would ensure wider and easier use
- The template should cover:
  - A relatively uniform approach to these features (from the end user perspective) so that consumers do not need to re-educate themselves whenever they change devices
  - An "automatic on" approach, or something similar, under which consumers can set up a new device only if they select a screen-saver password (whether digits, biometric, or something else) and activate lock/wipe/restore features
  - A feature making it easier for consumers to report thefts to providers and/or police, including reporting the device's IMEI
  - General consideration of the implications of Wi-Fi only connectivity.

# Task 2 - Hardened Device Identifiers (IMEI)

- Reliable IMEIs are critical not only for theft prevention, but also for improving the integrity of the wider provisioning system that uses the identifiers
- GSMA and 3GPP have begun discussions in this area, we need more urgency
- The WG was asked to assess rapidly whether there are any constraints that would prevent 3GPP and/or GSMA from developing a standard for a hardened IMEI by the end of this year
  - Note it is recommended that the WG work through ATIS as the North American 3GPP Organizational Partner

# Task 3 - Database

- The WG is asked to study database systems that effectively track stolen items (phones, cars, funds) and develop a spec sheet for an effective stolen phone database that might be focus on North America

- GSMA already hosts a configurable stolen phone database which is facilitating pan operator blocking and information distribution. There is an opportunity for ecosystem participants to make greater use of this resource through optimized configuration and adoption

- The WG should finalize the proposed spec sheet by October 1

**477 Testing**

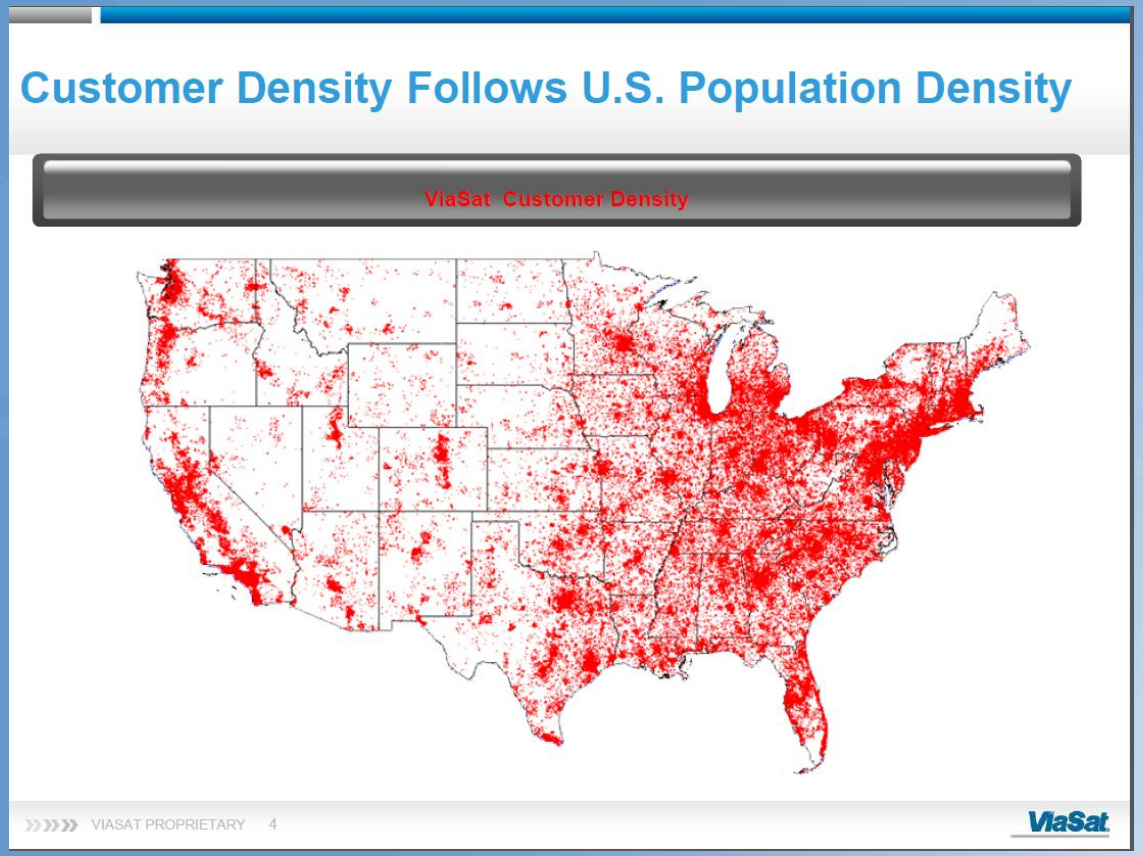
Steve Lanning
Chelsea Fallon (FCC liaison)
Ken Lynch (FCC liaison)
Chris Feathers (Brighthouse)
Tom Wilson (Brighthouse)
Lynn Merrill (NTCA)
Megan Stull (Google)
John Barnhill (Genband)
Russ Gyurek (Cisco)

**2015Q4**

- No Testing Assistance Requested by FCC
- 477 Updates
  - Released Broadband deployment data December 2014
  - No further changes made to 477 input

**Investigate How Well Incidence Of Satellite Subscribers Follow Broadband Map**

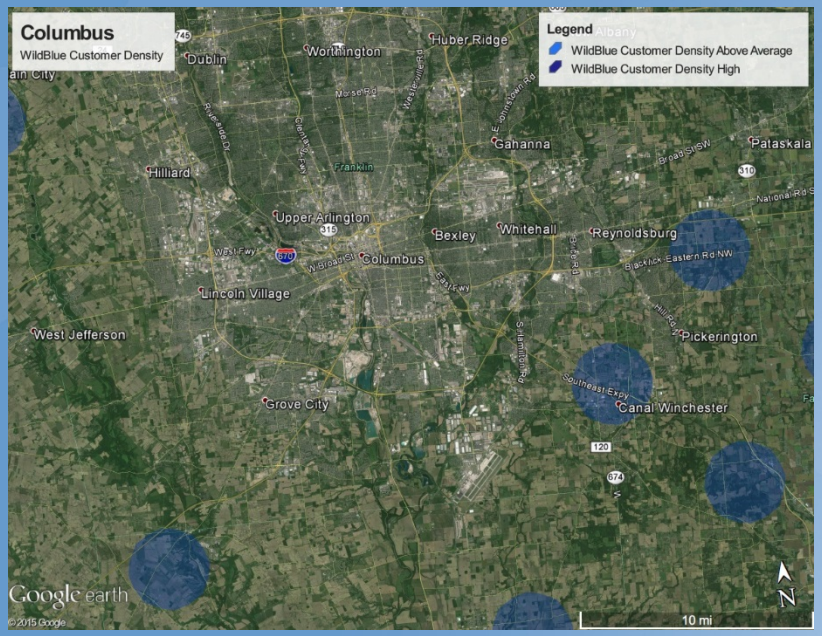
- 2014 June National Broadband map CBLOCK data
  - Code Served At 6 mbps  or more - downstream
  - Underserved As 6 mbps or less - downstream
  - All end-user categories, except government
- If clusters of subscribers occur in served area, code as Unvalidated
  - Implies some homes in area is not served by comparable terrestrial or wireless alternative or satellite was preferred to available terrestrial alternatives
- If clusters of subscribers occur in under served areas code as Validated

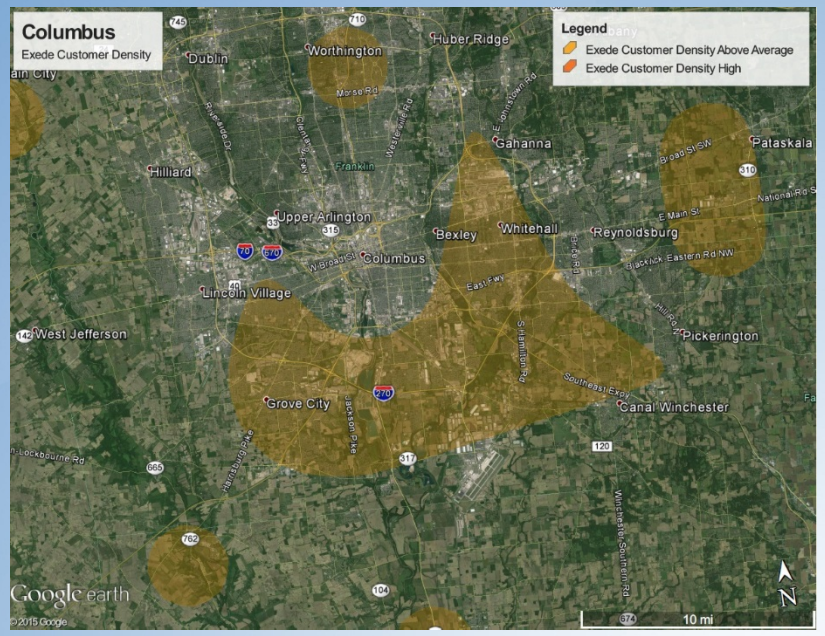



Available from google search:

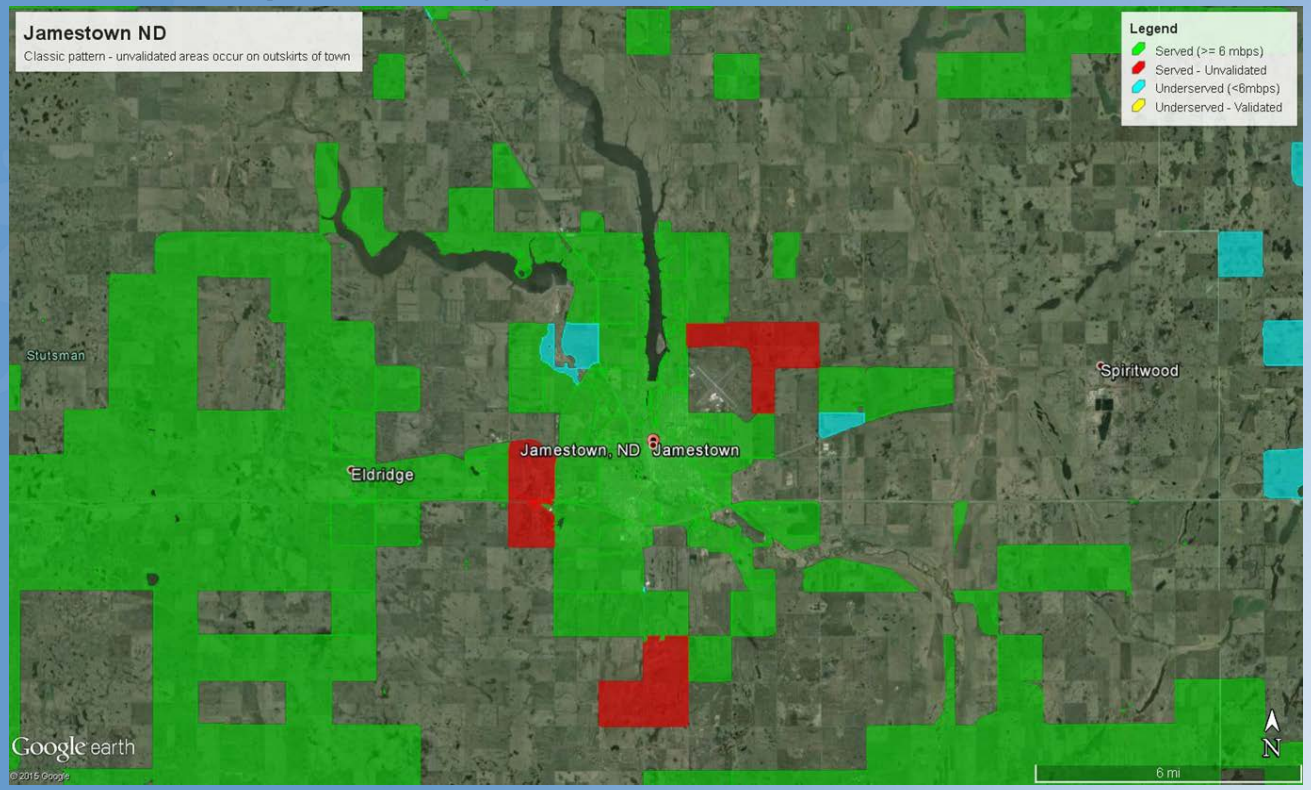
https://prodnet.www.neca.org/publicationsdocs/wwpdf/92012viasat.pdf

## Satellite subscriber areas of density increase with higher capacity satellite

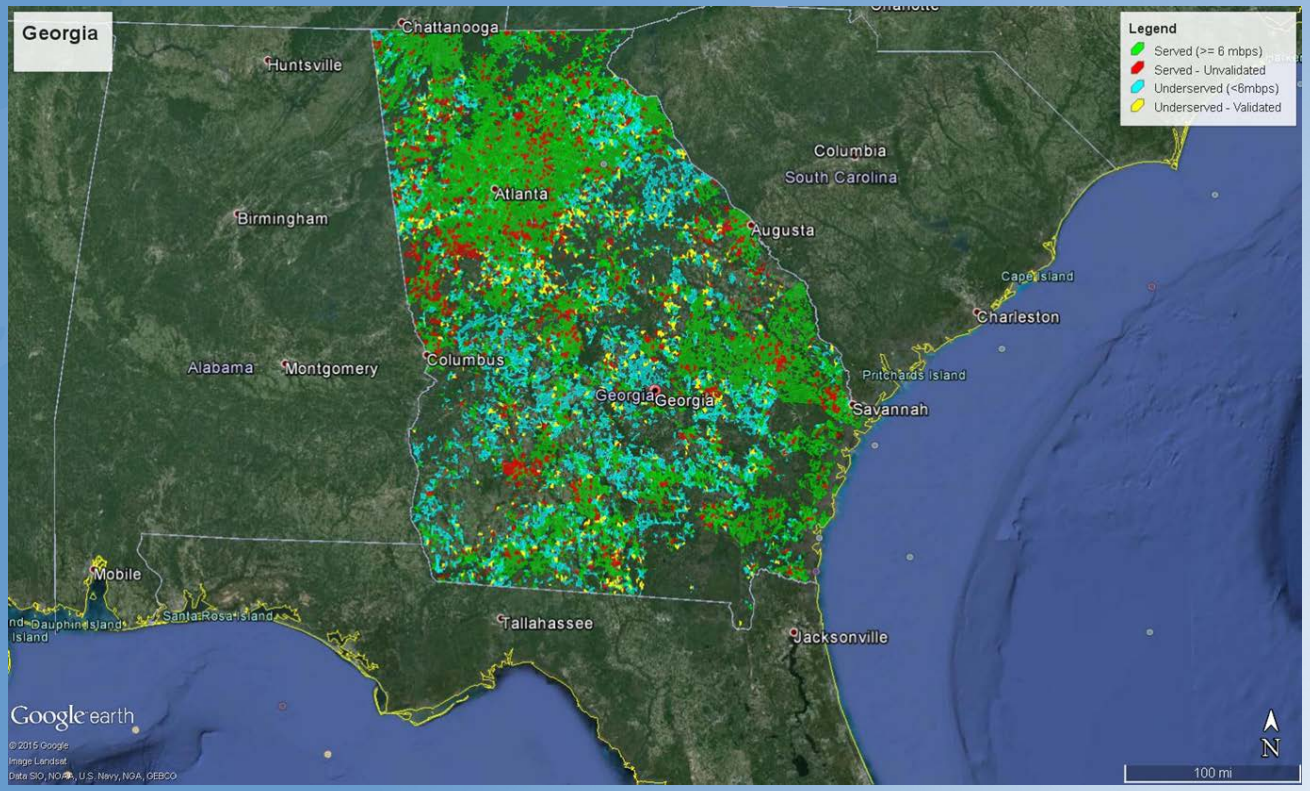


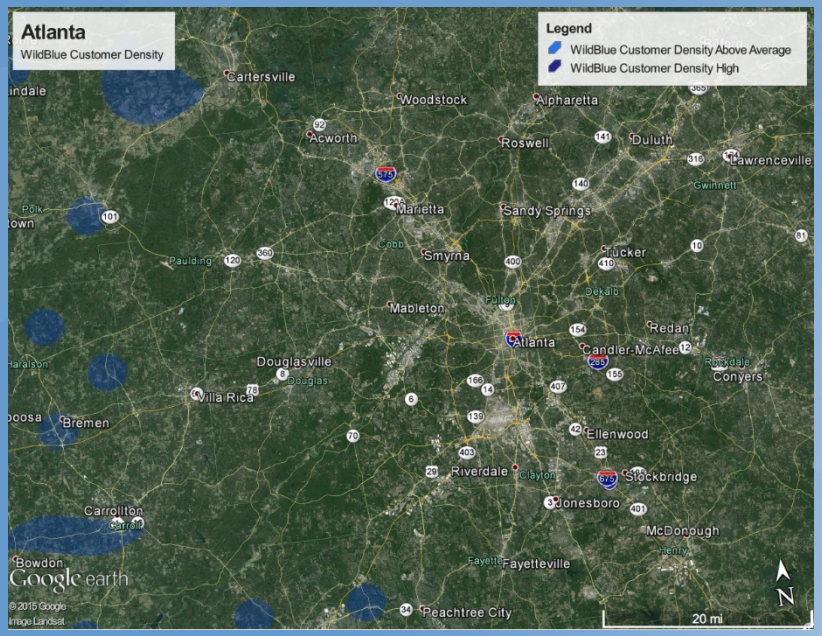
## Classic Example: coverage at center of town and Unvalidated areas on outskirts

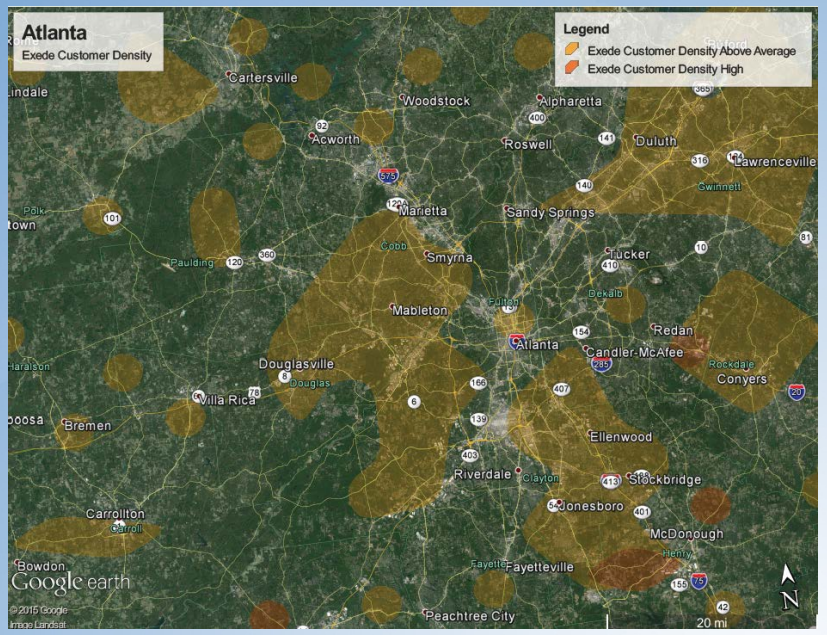


# The pattern appears in larger context, example: Atlanta GA



# Satellite subscriber areas of density increase with higher capacity satellite



## Summary

FCC already aware of some differences

| Satellite Evidence | Served | Underserved | Grand Total |
|---|---|---|---|
| Unvalidated | 11% | | 11% |
| Validated | | 27% | 1% |
| No Validation | 89% | 73% | 89% |
| Grand Total | 120,635,903 | 2,893,014 | 123,528,917 |

## Recommendations

- Resume work on 477 data collection improvements for accuracy, consistency in reporting and streamlined workflow
- Apply improved 477 data to improve National Broadband Map
- Make collection of data from consumers not able to get broadband service at their address through FCC website as addition to 477 reporting easier to use
- Resurrect WG when FCC has specific goals – Put On Hold For Now

## TAC Schedule

- 2015 Introduced Long/Short format which appears to have worked well
- However, slightly extended final meeting leaves limited time for discussion
- 2016 Schedule Proposal
  - Keep Long/Short format
  - Begin final meeting @ 10am and end at 4pm

- Proposed 2016 TAC Meeting Dates
  - Wednesday, March 09. 2016
  - Thursday, June 09, 2016
  - Tuesday, September 20th, 2016
  - Wednesday, December 7, 2016 (alternative Wednesday, November, 30th, 2016)