Technological Advisory Council

Mobile Device Theft Prevention WG

September 23rd, 2014

Agenda

- Overview & Mission Statement
- Sub-Working Group Updates
- Next Steps
- Backup Material

MDTP WG Mission Statement

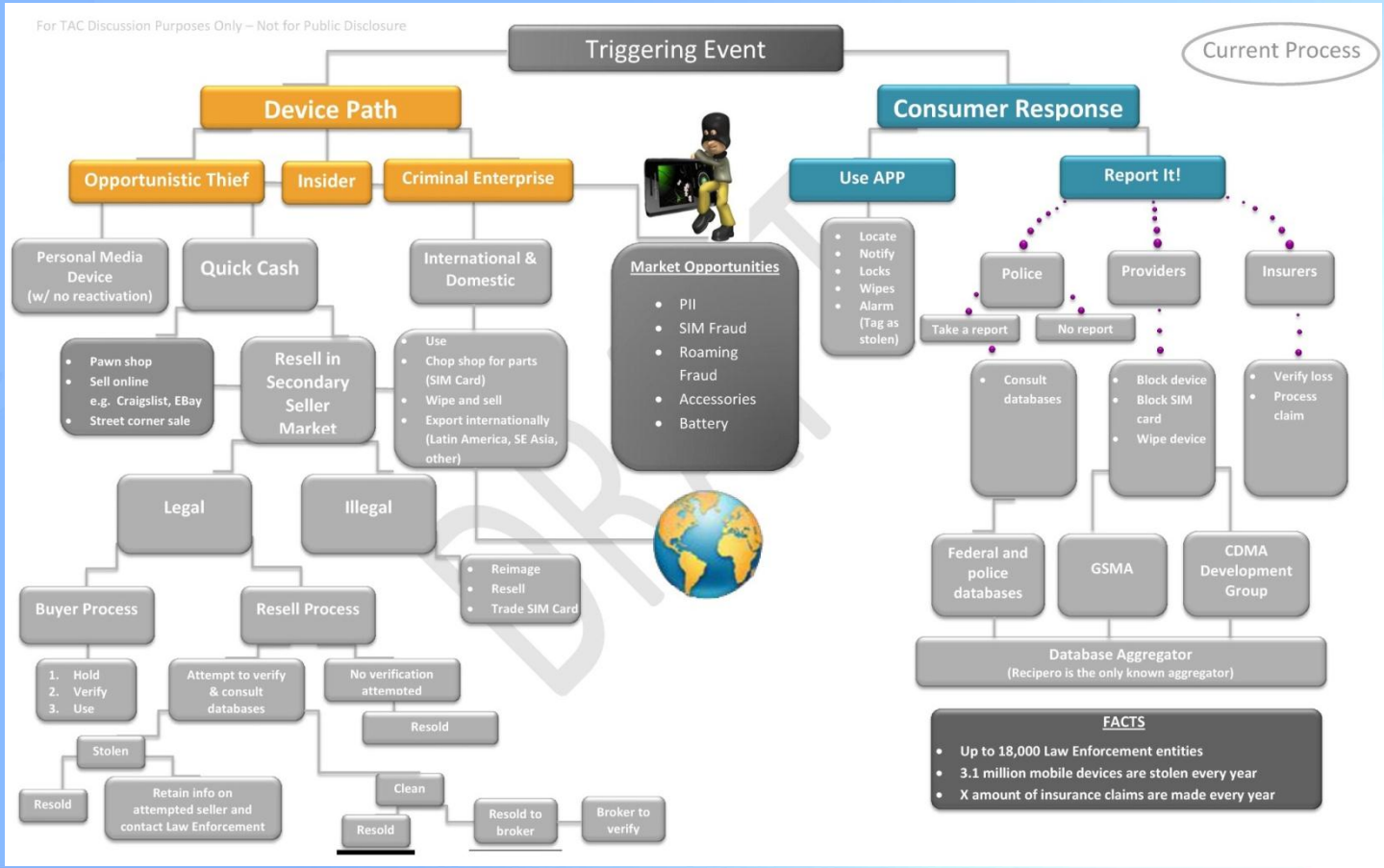
- The TAC Mobile Device Theft Prevention Working Group, to fulfill its charge of exploring the problem of mobile device theft and developing industry-wide recommendations for the FCC to deter and mitigate mobile device theft, should:
  1. define key terms that are central to this matter;
  2. develop best practices for consumer engagement and education;
  3. explore stakeholder coordination and data sharing;
  4. ensure appropriate considerations of cybersecurity concerns;
  5. identify gaps with existing solutions;
  6. analyze the potential necessity and value of new technical and operational solutions to deter thefts and enable the recovery of stolen devices; and
  7. identify standards organizations and industry fora to implement solutions.

- The Working Group has the opportunity to bring together diverse perspectives to analyze the problem and provide recommendations that address the unique scale of mobile device theft.

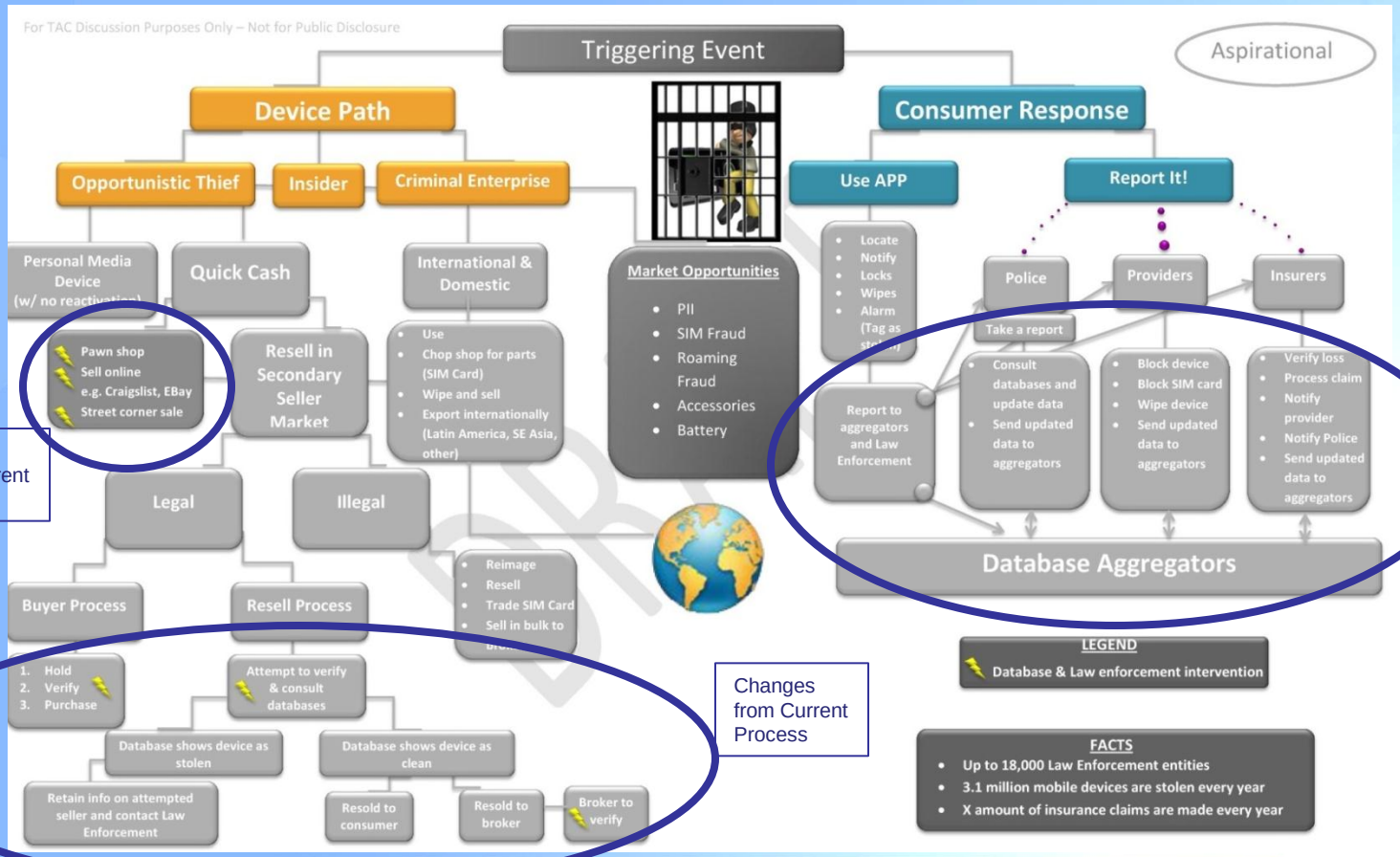
Background

- Following the Commission's workshop on "Prevention of Mobile Device Theft," the FCC's Technological Advisory Council established this working group committed to exploring multilayered solutions to mobile device theft. .
- The MDTP WG is exploring the widespread problem of mobile device thefts and to propose actionable, evolvable, and multi-layered solutions across a diverse base of stakeholders by the end of 2014.
  - Mobile device theft is a significant concern.
  - Some sources report that the number of mobile device thefts has nearly doubled from approximately 1.6 million in 2012 to 3.1 million in 2013.
- Mobile device theft is a complex issue that is present on both local and global levels.
  - Perpetrated as a "crime of opportunity," as well as part of a larger criminal enterprise.
  - Opportunistic thieves may use a stolen device as their own personal media devices (*e.g.*, camera, music player, Wi-Fi device), or sell the stolen device locally or online for "quick cash."
  - Larger criminal enterprise may be quickly shipped out of the country.
    - The stolen devices, or parts thereof (*e.g.,* battery, displays, memory), may then be resold (with or without cellular capability) in areas of high demand;
    - SIM cards may be exploited to perpetrate roaming fraud; and
    - Personal identifying information on the devices may be utilized to facilitate identity theft or other fraudulent activities.
- Mobile device thefts have continued to increase in spite of ongoing efforts to decrease incidents of the crime.
  - Increase could be a result of any number of factors.
  - Consumers may not properly report device thefts (or even know where this reporting should take place) and, similarly, may not be aware of tools that would aid the recovery of stolen devices.
  - Law enforcement entities are hindered by a lack of data and by the sheer number of device thefts that occur.
  - Current stolen device databases are not integrated and not easily accessible to most law enforcement entities.

Flow Chart – Current Process



Flow Chart – Aspirational Process



FCC ET Docket 14-143 (September 5, 2014)

- Federal Communications Commission Office of Engineering Technology, and Consumer & Governmental Affairs and Wireless Telecommunications Bureaus established a new docket relating to the Technological Advisory Council (TAC) Working Group on Mobile Device Theft Prevention (MDTP)

- The new docket allows industry and consumers to share information to supplement the efforts of the working group
  - Seeks comment and input from the public on proposals, efforts, and materials that will aid the TAC MDTP Working Group in accomplishing the goals and objectives of the Mission Statement and better serve the needs of consumers

- 120 Illinois Institute of Technology students have taken on the challenge of identifying possible theft deterrents as a component of the Inter-professional Projects Program class
  - Since many of these students have direct experience with having their devices stolen, their proposed solutions will have a useful validation background. We will expect their proposals (and others) to be integrated into the Working Group's results through the new FCC MDTP docket.

WG Participants

- Co-Chairs:
  - Brian Daly, AT&T
  - Rob Kubik, Samsung
- FCC Liaisons:
  - Walter Johnston
  - Charles Mathias
  - Elizabeth Mumaw

- Participants:
  - Asaf Askenazi, Qualcomm
  - Brad Blanken, CCA
  - Christian Schorle, FBI
  - Craig Boswell, Hobi
  - David Strumwasser, Verizon
  - DeWayne Sennett, Editor (AT&T)
  - Samir Vaidya, Verizon
  - Ayal Yogev, Lookout
  - Irene Liu, Lookout
  - Eric Feldman, ICE/Homeland Security Investigations
  - Gary Jones, T-Mobile
  - Greg Post, Recipero
  - Les Gray, Recipero
  - Ian Robertson, Motorola Mobility (Lenovo)
  - Jake Laperruque, Center for Democracy and Technology
  - Jason Novak, Apple
  - Jay Barbour, Blackberry
  - Joe Heaps, National Institute of Justice
  - John Foust, Metropolitan Police, Washington, DC
  - John Marinho, CTIA
  - Jamie Hastings, SME (CTIA)
  - Kirthika Parmeswaran, iconectiv
  - Mark Romer, Asurion
  - Ben Katz, Gazelle
  - Maxwell Szabo, City and County of San Francisco
  - Mike Rou, eBay
  - Nick Tucker, Microsoft
  - Ron Schneirson, Sprint
  - Samuel Messinger, U.S. Secret Service
  - Sang Kim, LG

Timelines

	Full WG Meeting Date	Milestone
1	August 1	Kick off work, Form Sub-Working Groups
2	Week of Aug 11	MDTP Conference Call working Session
3	Week of Aug 25	MDTP Conference Call working Session
4	Week of Sept 8	MDTP Conference Call working Session
5	Week of Sept 22	Deliver Progress Update to TAC
6	Week of Oct 6	MDTP Conference Call working Session
7	Week of Oct 20	MDTP Conference Call working Session
8	Week of Nov 3	Target for Sub-Working Groups to complete their work
9	Week of Nov 17	Final Draft of Recommendations & Document Editorial Review
10	December 4	Deliver Recommendations to TAC

Initial Sub-Working Group Assignments

MDTP WG

- Problem Definition
- Existing Solutions
- Gap Analysis
- Cybersecurity & Privacy
- Consumer Outreach

Problem Definition Sub-Working Group Report

Sub-WG Facilitator: Brad Blanken, CCA

Problem Definition Sub-WG Scope

- The Problem Definition (PD) Subgroup will be responsible for the documentation of the Mobile Theft problems & issues consistent with FCC Technological Advisory Council as it relates to Mobile Device Theft Prevention tools and solutions. These will include:
  - Definition of terms;
  - Identification of scope, scale for MDTP current challenges;
  - Identification of challenges positioned from various stakeholders.

- Document and report back the Problem Definition to the FCC TAC Mobile Device Theft Prevention Working Group in order to address the problem of mobile device thefts that are aligned with final recommendations to the Chairman by end of year 2014.

Existing Solutions Sub-Working Group Report

Sub-WG Facilitator: Ron Schneirson, Sprint

Existing Solutions Sub WG Scope:

Deliver high-level representations of existing and pending solution components from across the globe, identify capabilities and impacts as they associate to the "aspirational" Consumer Response Flow

Accumulated Content / Participants

SOLUTION	LEAD	DATA Provided	Presented to Team
Qualcomm	Asaf Askenazi		
Lookout	Asaf Askenazi	X	
iconectiv	Kirthika Parmeswaran	X	X
Subscriber Registry	Kirthika Parmeswaran	X	X
GSMA Database	James Moran	X	X
Device Blocking	James Moran	X	
Law Enforcement	Les Gray	X	X
Recipero	Les Gray	X	X
Recipero E-to-End	Les Gray	X	
Absolute LoJack	Rob Kubik	X	
Insurance	Mark Romer		
Samsung	Rob Kubik	X	
LG	Sang Gook Kim	X	
Google	Ron Schneirson	X	
Microsoft	Nick Tucker	X	X
Blackberry	Jay Barbouron	X	
Apple	Jason Novak	X	
Sprint	Ron Schneirson	X	X
ATT	Brian Daly		
T-Mobile	Gary Jones	X	
Verizon	David Strumwasser	X	
Dcoumentation Lead	DeWayne Sennett		

Existing Solutions Sub-Working Group Initial Findings

Device-Based Solutions

- Major OS Providers and Several OEM's Deliver Kill-Switch Solutions directly to consumers, further capabilities imminent to accommodate state laws
- Other Device-Based solution components are in various levels of maturity, consideration, or adoption

Database Solutions

- GSMA Daily Sync Adopted across Major Carriers (for LTE and GSM)
  - Small number of LEA's accessing
- Recipero used only by Sprint for CDMA devices
- FBI's NCIC, Crime reports from LEAs for local access, little impact on problem, no info from other stakeholders, Extremely limited availability

Operator Implementations

- Operator-Owned "Blacklists" (Internal Databases) Near-Real time Activation blocking
- Carriers Synchronize with GSMA Central Database for GSM and LTE devices
- Limited support for CDMA database
- Operators Direct End-Users to OS Providers and Device Manufactures for Kill Switch Support

Gap Analysis Sub-Working Group Report

Sub-WG Facilitator: John Foust, Metropolitan Police, Washington, DC

Gap Analysis Defined & Sub-WG Methodology

- *A technique that businesses use to determine what steps need to be taken in order to move from its current state to its desired, future state.*
  Also called need-gap analysis, needs analysis, and needs assessment.

http://www.businessdictionary.com/definition/gap-analysis.html#ixzz3BWPV2qla

Starting with the end in mind

Step 1. Identificaiton of Desired Outcomes

Step 2. Identification of Existing Practices

Step 3. Identification of the Gap(s)

Step One- Identification of Stakeholders and Desired Outcomes

- Step one has been a time consuming and involved process
- The group discovered there are many stakeholders, sometimes with diverse desired outcomes.
  - Stakeholders include:
    - Law enforcement
    - Owners/consumers (personal and enterprise)
    - Service Providers/Carriers
    - Device & Platform Manufacturers
    - Insurance Providers
    - Third-party Vendors
    - Government and Regulators

Step Two - Identification of Existing Practices

- The group in currently in this process.
- This step will be easier to accomplish as the group will only have to identify what is currently being done.
- The Existing Solutions group will be able to provide input here.

Step Three - Identification of the Gaps

- In about one week the group will move to the actual identification of gaps.
- Existing practices will be compared against desired outcomes.
- Although this seems to be straightforward process, the group expects much discussion as Gaps as explored.

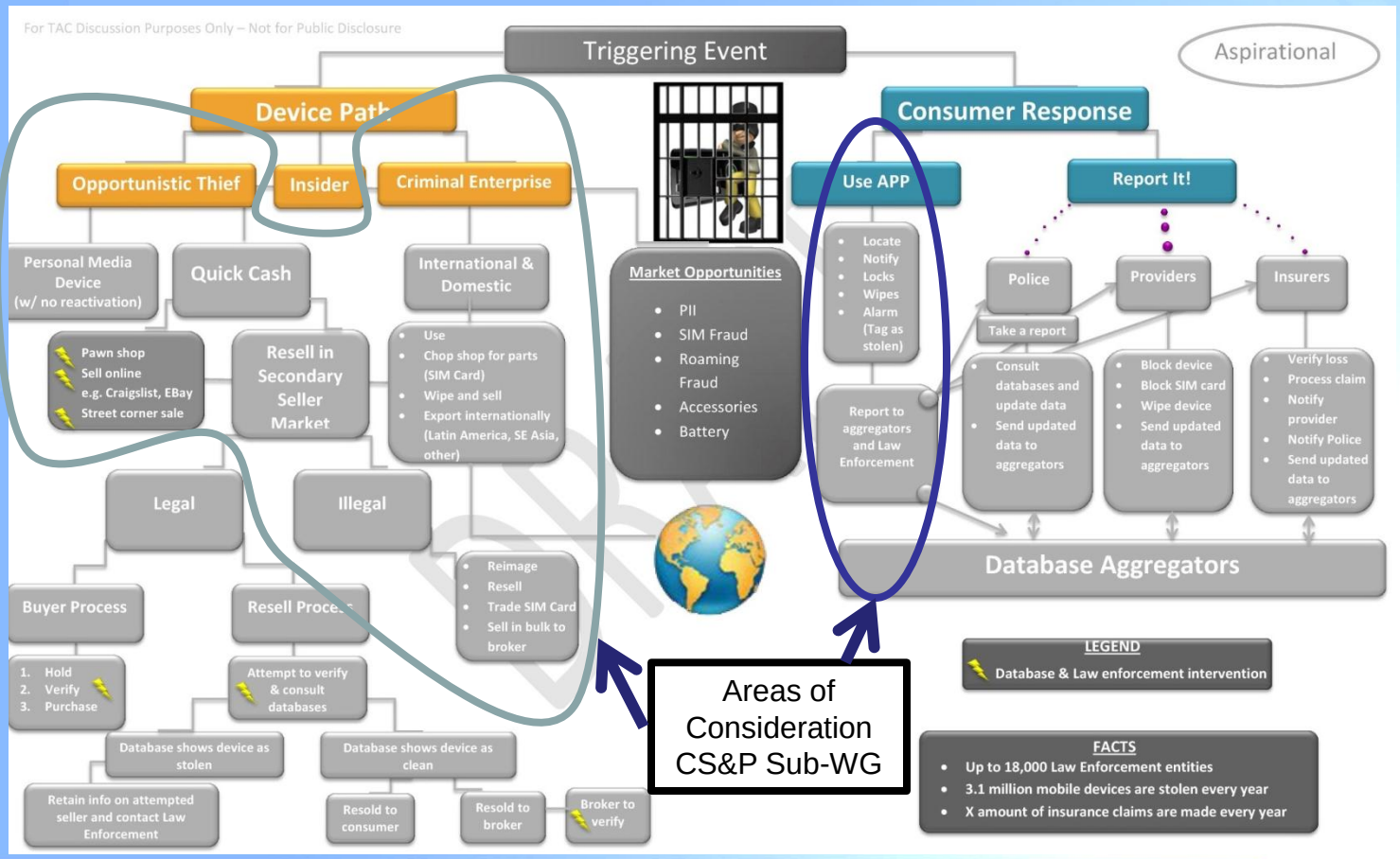
Cybersecurity & Privacy Sub-Working Group Report

Sub-WG Facilitator: John Marinho, CTIA

Cybersecurity & Privacy Sub-WG Mission

- The Cybersecurity & Privacy (CS&P) Subgroup will address cybersecurity and privacy issues consistent with FCC Technological Advisory Council as it relates to Mobile Device Theft Prevention tools and solutions. These will include:
  - Definition of terms;
  - Identification of threats and vulnerabilities for MDTP solutions;
  - Use cases to illustrate the threats and vulnerabilities;
  - Identification of mitigation strategies, existing or new;
  - Use cases to illustrate how the mitigation strategies may be applied; and
  - Identify standards organizations and industry venues that are relevant to the development of best practices.
- Actionable recommendations to the FCC TAC Mobile Device Theft Prevention Working Group in order to address the problem of mobile device thefts that are aligned with final recommendations to the Chairman by end of year 2014.

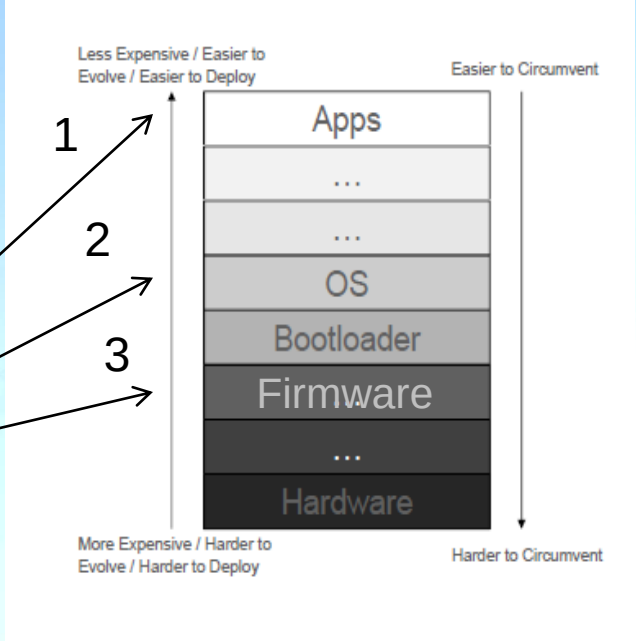
Flow Chart – Aspirational Process



Existing Anti-Theft Categories/Types

- Software approaches
  - Cost effective to implement
  - Fastest to implement and deliver to market
  - Easy deployment
  - Easy software maintenance and evolution
- Hardware approaches
  - More costly to implement
  - Longer to implement and deliver to market
  - Harder deployment
  - Harder maintenance and evolution
- Network/Server/Cloud/MDM based approaches
  - More Secure, approaches not mutually exclusive
  - Cheaper & easier to evolve than hardware alone
  - Device Software/Firmware & Server based
  - Some: Hardware Root-of-Trust, Software/Firmware & Server based
  - Paired Network Access Blocking: IMEI or MEID

Mobile Device



Assumptions: Capabilities

- In event of Smartphone Theft or Loss:
  - Remotely Lock/Unlock Device, prevent unauthorized use and network access
  - Locate (implicates Privacy considerations)
  - Remote Access to Device Data, e.g. Call Log(implicates Privacy & Lawful Access Reqts.)
  - Disable Apps (Non-Emergency & Non-Recovery)
    - Except: Emergency Service Requirements
  - Remotely Wipe the Device
  - Prevent Reprogramming
  - Re-enable if found or returned to authorized user
    - Restore user data if possible, e.g. Back-Up
  - Wi-Fi-only device/use case
  - User enabled recovery by 3rd Party/Reverse Logistics
  - Secure re-activation absent authorized user, 3rd party logistics
- Information Sharing Requirements – IMEI, MEID – Lost/Stolen
  - Provider/Carrier
  - Law Enforcement
  - Data Aggregators
  - Insurers
  - OEMs
  - OS Providers
  - Solutions Developers
  - Consumer

Risks, Vulnerabilities & Limitations

- Exploits of device APIs
- Root attacks and Rooting/Jailbreak device
- Mobile device malware/ransomware
  - Root attacks, Inter-Process-Communications Attacks, BotNets
- Cross-platform malware, e.g. Laptop and Smartphone
- Software Updates & Spoofing
- Roll Back Attacks
- IMEI/MEID Spoofing
- MitM Attacks
- Implementation Bugs - Exploits
- Bootloader Attacks
- Server based attacks, e.g. DDoS, Hacking
- Security Credentials Brute Force

Limitations:

- Social Engineering/Trick-Consumer
- Physical Attack: “Faraday Cage”, stolen briefcase/purse/luggage
- Component Value – i.e. striping smartphone for parts

Consumer Outreach Sub-Working Group Report

Sub-WG Facilitator: Jamie Hastings, CTIA

Consumer Outreach Mission Statement & Scope

- The Consumer Outreach (CO) Subgroup will consider and develop best practices for consumer engagement and education that are consistent with the FCC Technological Advisory Council as it relates to Mobile Device Theft Prevention tools and solutions. The steps taken will include:
  - ✓ Definition of terms;
  - ✓ Identification of current industry efforts and gaps;
  - ✓ Understanding consumer behavior regarding reporting thefts and use of anti-theft solutions;
  - ✓ Identification and review of best practices for similar types of consumer engagement and education programs;
  - ✓ Identification of key stakeholders and industry fora that are relevant to the development and implementation of best practices.
- Actionable recommendations to the FCC TAC Mobile Device Theft Prevention Working Group in order to address the problem of mobile device thefts that are aligned with final recommendations to the Chairman by end of year 2014.

Review of Current Outreach Government Stakeholders - FCC, DOJ, DHS, etc.

FCC

- Fact sheet when you search stolen phones
- 10 Steps to Smartphone Security - for Windows, Apple iOS, Blackberry and Android
- Collaboration with international government stakeholders, especially in Latin America and Europe
- July 3, 2014 Joint Consumer Advisory with CGB and D.C. Metropolitan Chief of Police Cathy Lanier (http://www.fcc.gov/document/tips-protecting-your-mobile-device-theft)
- June 19, 2014 Workshop pulling together a comprehensive and extensive group of experts, including international experts, in the field to delve into Mobile Device Theft Prevention (http://www.fcc.gov/events/fcc-announces-workshop-focus-prevention-mobile-device-theft)
- Established a working group at the direction of FCC Chairman within the TAC to make actionable recommendations to the Commission (to include Consumer outreach) by end of year 2014.
- Consumer guide - Stolen and Lost Mobile Devices – Main Consumer Guide Page (http://www.fcc.gov/guides/stolen-and-lost-wireless-devices)
- Consumer guide - Contact info: How to report stolen phones (http://www.fcc.gov/stolen-phones-contact-numbers)
- April 2012 PROTECTS initiative implemented by Chairman Genachowski.
- Established official docket for the filing of consumer comments to inform the initiative, including consumer outreach efforts.

US Department of Justice

- Breaks down consumer information by subject and provides online resources for various topics
- No consumer call center unless caller knows exact individual to speak to
- Provides more legal precedents than consumer education

Federal Bureau of Investigations

- National Consumer Protection Week 2014
- FBI and FTC work together to provide “tips and guidelines” for education consumers on fraud, scams, etc.
- No stolen phone specific initiatives, but encourages consumers to “be crime smart”
- Offers one-pagers and other online information
- Consumers can use social media to contact the FBI on consumer issues but no call center exists

Industry Efforts

- CTIA developed BeforeYouLoseIt.org, a website that offers comprehensive tips on how to avoid losing your smartphone and what to do if a phone goes missing
- CTIA also developed a PSA, The Five Stages of Losing a Smartphone, to illustrate what can be done to prevent any loss
- CTIA created business card-sized tip sheets on this issue that have been distributed to law enforcement agencies across the country
- Top US carriers have websites, tips, and consumer hotlines where customers can prevent or solve lost phone issues

MPDC Poster

National Crime Prevention Month

Be Cautious When Leaving the Store with Your New Gadgets

The officers of the Metropolitan Police Department would like to remind members of the public to be cautious when making electronic purchases, particularly on days of new releases of popular devices and gadgets. If you have plans to make a major purchase of a popular computer, tablet, or phone, please remember these important safety tips:

1. If an **online tracking system** is available for your device, get the extra assistance in the store for setup before exiting the store.
2. **Don't be distracted** as you exit local cell phone stores and other electronic specialty stores that sell these items. Be deliberate as you exit these stores, concealing your purchase(s) and focusing on getting to your next destination. Cell phones and other music devices are major distractions when in use.
3. **Report suspicious people.** *Inside a store*: Do you notice people who are paying more attention to the purchases being made, rather than checking out new products? *Outside a store*: Do you see suspicious people standing at or near the exit for no real purpose? Report these behaviors to police.
4. **Try to shop with a friend.** Most victims who report crimes that involve snatching new products are people who have shopped alone. If you have an elderly parent, please make preparations to accompany him or her to make these kinds of purchases or suggest ordering them online.
5. Never hesitate to **point out suspicious activity** or people to local officers or security guards. Remember the "See Something, Say Something" campaign and dial 9-1-1 if you need an officer dispatched to your location.

Office of Community Outreach and
Patrol Services & School Security Bureau

Review of Best Practices – Other Initiatives

Government

Consumer Financial Protection Bureau

- Offers online financial education services for adults, students and kids
- CFPB call center has quick pick and short wait times – Markets other programs during hold time on calls
- Blog is an important source of information, often quoted in lieu of press releases
- CFPB officials tour the US to raise the profile of various agency Programs

Office of the Comptroller of the Currency

- Offers links to related agencies and organizations that can help consumers
- Features online information on consumer financial protection issues
- An internal OCC organization, the Consumer Assistance Group (CAG), processes questions and complaints about consumer issues

Consumer Behavior

CTIA commissioned survey done by Harris Interactive entitled "Cybersecurity Research" published in January 2013:

1. Three Quarters of consumers believe the responsibility to keep their device safe falls mostly to them.
2. Approximately one half use a password or PIN to access their smartphone, but this is much less than with computers.
3. Of the small percentage who have lost or had their smartphone stolen, almost half contacted their wireless service provider.
4. Consumers are more apt to protect themselves against tangible threats (like loss of a mobile device) versus intangible threats (hacking malware, etc.).
5. Though not a majority, many consumers have an app that remote locks.

Key Initial Findings

- Opportunities exist as most consumers believe that it is their responsibility to keep their devices safe
- Opportunities exist on government websites for education and information
- Best practices in other areas include things such as social media, on hold messages at call centers, awareness activities
- Use of relationships with other stakeholders such as law enforcement to get the message out locally may be beneficial

Mobile Device Theft Prevention WG Summary & Next Steps

- Sub-working groups continue to gather/analyze data and develop recommendations
- December TAC Meeting - Present final report and recommendations

Backup Material

Problem Definition Sub-Working Group

Initial Assignments

MDTP WG

- Problem Definition
- Existing Solutions
- Gap Analysis
- Cybersecurity & Privacy
- Consumer Outreach

For TAC Discussion Purposes Only - Not for Public Disclosure

Problem Definition Sub-WG Timelines

	Full WG Meeting Date	Milestone
1 √	August 1	Kick off work, Form Sub-Working Groups
2 √	August 15th	Initial kick-off of PD subgroup and introduction of members. Scope of work definition
3 √	Week of Aug 25	Outreach to various stakeholders
4 √	Week of Sept 8	Document framework/ Outline
5	Week of Sept 22	Deliver Progress Update to MDTP WG for TAC update
6	Week of Oct 6	Continue drafting
7	Week of Oct 20	Continue drafting
8	Week of Nov 3	PD Document Delivery to MDTP Working Group
9	Week of Nov 17	Final Draft for Editorial Review & Comment
10	December 4	Deliver Recommendation to TAC

Existing Solutions Sub-Working Group

Existing Solutions Sub-WG Participants

Name	Company
Asaf Askenazi	Qualcomm
Brian Daly	ATT
David Strumwasser	Verizon
DeWayne Sennett	ATT Document Editor
Chris Bender	Motorola Mobility (Lenovo)
James Moran	GSM Association
Jay Barbour	Blackberry
Les Gray	Recipero
Mark Romer	Asurion
Robert Kubik	Samsung
Nick Tucker	Microsoft
Sang Gook Kim	LG
Kirthika Parmeswaran	iconectiv
Les Gray	Recipero
Ron Schneirson	Sprint

Existing Solutions Sub-WG Next Steps

- Integrate Sub-Group Findings with Working Group Document
- Consume Input from other Subgroups
- Formulate Recommendations

Gap Analysis Sub-Working Group

Gap Analysis Group

- John Foust (MPD)
- Asaf Askenazi (Qualcomm)
- Craig Boswell (Hobi)
- David Strumwasser Verizon)
- Gary Jones (T-Mobile)
- Jay Barbour (Blackberry)
- Kirthika Parmeswaran (iconectiv)
- Les Gray (Recipero)
- Max Szabo (City & County of San Francisco)
- Robert Kubik (Samsung)
- James Moran (GSM Association)
- Mike Rou (ebay)
- Brian Daly (AT&T)
- DeWayne Sennett (editor/AT&T)

Schedule and Timeline

Date	Event
August 1	Kick off work, Form Sub-Working Groups
Week of Aug 11	Initial kick-off of Gap Analysis subgroup and began broad discussions.
Week of Aug 25	Wrap-up identification of Stakeholders and complete identification of Desired Outcomes
Week of Sept 8	Identify Existing Procedures, will involve gathering information from other groups.
Week of Sept 22	Began Identification of Gaps Deliver Progress Update to MDTP WG for TAC update
Week of Oct 6	Continue Identification of Gaps
Week of Oct 20	Continue Identification of Gaps
Week of Nov 3	Finalize Identification of Gaps, submit Initial Report to MDTP Working Group
Week of Nov 17	Prepare and submit Final Gap Analysis Report to MDTP Working Group
December 4	MDPT Delivers Recommendations to TAC

Cybersecurity & Privacy Sub-Working Group

Company	CS&P Member
ATT	Brian Daly
ATT Document Editor	DeWayne Sennett
ICE/Homeland Security Investigations	Eric Feldman
ICE/Homeland Security Investigations	Jeff Brannigan
Motorola Mobility	Chris Bender
Apple	Jason Novak
Blackberry	Jay Barbour
CTIA	John Marinho (Sub-group lead)
iconectiv	Kirthika Parmeswaran
Recipero	Les Gray
Asurion	Mark Romer
ebay	Mike Rou
Microsoft	Nick Tucker
Samsung	Robert Kubik
US Secret Service	Samuel Messinger
GSM Association	James Moran
FCC	Walter Johnston
FCC	Sarah Weeks

Illustrative Use Cases (Post-paid and Pre-paid)

- **Sunny Day Scenario – Device Lost or Stolen**
- **Snatch & Grab Opportunistic**
- **Ecosystem (Organized Processing of Stolen Devices)**
- **False Acquisition**
  - **False ID, Subsidized Phone**
    - Bundle and Ship (No report of theft or loss)
  - **Contract Fraud, Subsidized Phone**
    - Limited usage and sell (No report of theft or loss)
- **Reverse Logistics, Recovery of Device**
  - Authenticated/Authorized Actors
- **IMEI/MEID Spoofing**
- **Social Engineering/Trick Consumer**
- **Security Credentials Brute Force Attack**

	Full WG Meeting Date	Milestone
1 √	August 1	Kick off work, Form Sub-Working Groups
2√	Week of Aug 11	Initial kick-off of CS&P subgroup and identification of members
3√	Week of Aug 25	Existing industry practices and solutions – security & privacy considerations, Draft of Section 5 of MDTP Report
4	Week of Sept 8	Scenarios/Use Cases & OET Questionnaire
5	Week of Sept 22	Deliver Progress Update to MDTP WG for TAC update
6	Week of Oct 6	Analysis of Threat Vectors and Privacy Concerns
7	Week of Oct 20	Analysis Best Practices and Generic Use Case Examples
8	Week of Nov 3	CS&P Recommendations to MDTP Working Group
9	Week of Nov 17	Final Draft of Recommendations & Document Editorial Review
10	December 4	Deliver Recommendation to TAC

Consumer Outreach Sub-Working Group

Consumer Outreach Sub-working Group

Company	Participant
ATT	Brian Daly
ATT	Jonathan Norton
ATT Document Editor	DeWayne Sennett
Center for Democracy and Tech	Jake Laperruque
CTIA	Jamie Hastings
Hobi	Craig Boswell
Motorola Mobility (Lenovo)	Michael McCallum
Recipero	Greg Post
Samsung	Robert Kubik
Samsung	Megan Pollock

Consumer Outreach Sub-WG Next Steps

- Continue to gather information about law enforcement outreach in the US
- Continue to gather information about consumer behavior
- Begin to formulate and finalize recommendations

Consumer Outreach Sub-WG Timelines

	Full WG Meeting Date	Milestone
1 √	August 1	Kick off work, Form Sub-Working Groups
2 √	Week of Aug 11	Initial kick-off of CO subgroup and identification of members
3 √	Week of Aug 25	Review of current industry practices and identification of gaps
4 √	Week of Sept 8	Identification and review of best practices for similar types of outreach
5	Week of Sept 22	Deliver Progress Update to MDTP WG for TAC update
6	Week of Oct 6	Identification of key stakeholders and organizations relevant to outreach-begin outlining best practices
7	Week of Oct 20	Development of best practices for consumer engagement and education
8	Week of Nov 3	CO Recommendations to MDTP Working Group
9	Week of Nov 17	Final Draft of Recommendations & Document Editorial Review
10	December 4	Deliver Recommendation to TAC

Technological Advisory Council

477 Testing

Working Group

23 September 2014

Working Group Members

- Jim Janco (Comcast)
- Megan Stull (Google)
- Sara Cole (TDS Telecom)
- Linda Manske (EarthLink)
- Gregory Wagner (AT&T)
- William Trelease (Dehli Telephone)
- Tom Wilson (Bright House)
- Chris Feathers (Bright House)
- Joan Engler (Verizon)

Special thanks to the FCC members: Chelsea Fallon and Ken Lynch for their contributions.

Today's Discussion

- Review mission
- Update on work effort to date
- Share results to date
- Receive feedback from the rest of the TAC

Mission

Improve accuracy of data collected and minimize time required to submit

- Phase I
  - User Testing Of 477 Submission
  - Identify Defects
  - Defects fixed
  - Defects not fixed
  - Likely burden of defects not fixed
  - Recommendations to fix remaining defects
  - Recommendation for improvements
- Phase II (not yet started)
  - New methods of data collection that utilize software run by users prior to submission
  - Users input customer level data to software and that produces appropriate summary data

Defects Identified And Fixed

- 499 filer number not found. Updated list and improved instructions.
- Chrome: census tract drop-down menus on the Fixed Broadband Subscription and Fixed Voice Subscription interactive data entry pages did not work and buttons not displayed.
- Reduced complexity for satellite filers: if every record would be same in a state or group of states, one block level record per state is sufficient.
- Improved time for fixed voice subscription (FVS) file to move to interactive state entry.
- “Next State” button in the state-level FVS interactive data entry pages improves navigation through these pages.
- Helpful Hint below the “Continue to State” button on the FVS File Upload Click once because it can take more than a few seconds for the interface to process the tract-level FVS data and proceed to the state-level FVS pages.

Defects Identified And Fixed - 2

- Accept .txt and .TXT extensions for README in zipped Mobile Broadband Deployment and Mobile Voice Deployment (previously required .txt)
- Error 500 “technical error has occurred” after being automatically logged out for session timeout. Users now are returned automatically to the login page after timeout.
- Unclear messaging after submission. After a filing has been submitted and its status has changed to “Original-Submitted,” a message at the top of the Submission Menu page appears stating: “This filing has been submitted and is now read-only. To edit, go to the Main Menu and click Revise.”

Instructions Improved

- Clarified Instructions and User Guide that the DBA Name used in the fixed and mobile broadband deployment data does not need to match the company name associated with the FRN.
- Added text to the Instructions and User Guide on the upload and file processing times that users should expect and informed them that leaving the page or logging out would not interrupt the upload.
- Added text to the Instructions that bandwidth/speed data should be entered in Mbps with up to 3 decimal places.
- Added language to the Instructions and User Guide clarifying that the list of Form 499 Filer IDs used by the Form 477 Filing Interface is not updated in real-time and giving filers guidance on what to do if their Form 499 Filer ID does not appear in the Form 477 Interface.

Instructions Improved - 2

- Clarified that if filers replace any of their tract-level Fixed Voice Subscription data after entering state-level totals, they need to re-enter all of the state-level totals.
- Highlighted that companies that participated in the NTIA State Broadband Initiative can download census block-level data on broadband deployment from the National Broadband Map website or possibly obtain such data from their state's mapping entity.

Defects Not Fixed	Implications
▪ Slow processing of large file uploads	▪ Ongoing issue ▪ Onerous To Filers

Suggestions – Defect Fixes

- Faster processing of large file uploads
- Even largest file sizes required by national providers are small by IT standards – no reason it should take so long to validate and accept file
- Once file is uploaded processing (virus check, validation, unique records) should be measured in seconds and not minutes or hours
- Service level agreement for developer to meet reasonable processing time

Suggestions – New Features

- Ability to download data that has been uploaded
- Certification page – something to submit to state as proof (can take a screen shot today or print out status)
  - Section by section report at state level of what has been successfully submitted.
- Offer filers the option to submit data for multiple sections in a single file based on the smallest geography (census blocks) – reduce redundancy – example coverage and customers could be done once with zeros where there is coverage but no customers
- Ability to submit all data for the filing in a single, bulk XML upload

Next Steps for TAC 2014 Work

- Report on actual experience from submissions
- Update on improvements
- Start Phase II

THANK YOU

Technological Advisory Council

Spectrum and Receiver Performance

Working Group

September 23, 2014

2014 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 proposed interference limits policy
- Conduct analysis and make recommendations related to enforcement issues in a rapidly changing RF environment

Working Group

- **Chair:**
  - Lynn Claudy, NAB
- **FCC Liaisons:**
  - Julius Knapp
  - Uri Livnat
  - Bob Pavlak
  - Matthew Hussey
- **Participants / Contributors:**
  - Dale Hatfield, John Cook, University of Colorado
  - Greg Lapin, ARRL
  - Pierre de Vries, Laura Littman, Silicon Flatirons
  - Brian Markwalter, CEA
  - David Gurney, Motorola Solutions
  - Geoff Mendenhall, GatesAir
  - Rauf Hafeez, AT&T
  - Hossam H'Mimy, Ericsson
  - Jesse Russell, Robert Miller, incNetworks
  - Patrick Welsh, Kitty O'Hara, Max Solondz, Verizon
  - Doug Brake, Information Technology & Innovation Foundation
  - Mike Marcus, Marcus Spectrum Solutions
  - Scott Burgett, Garmin
  - Dennis Roberson, Illinois Institute of Technology

Working Group Areas of Focus

- **Develop recommendations about statistics of interference and risk-informed decision making**
- **Interference resolution, enforcement & radio noise**
  - **Recommend strategies for interference resolution and enforcement to address new RF environment challenges**
  - **Coordinate with CSMAC in the development and recommendation of enforcement strategies for a shared spectrum environment with federal incumbents**
- **Explore technical topics on receiver performance and emerging radio technologies for a shared spectrum environment**

Impact of Emerging Receiver Technologies on Changing Standards and Spectrum Allocations

- On June 10, three work group members briefed FCC staff and TAC members about emerging receiver technologies, including:
  - Receiver hardware
  - Dynamic interference mitigation
  - Software defined radios
- The Spectrum and Receiver Performance working group proposes to the TAC to approve this presentation for posting on the TAC website

Risk-informed interference assessment

- **Situation**
  - **Coexistence analysis involves many variables**
  - **Variables can take a range of values**
  - **Worst case values are the “safest”, but at the price of spectral efficiency**
  - **Complement worst case by statistical risk analysis of interference scenarios**
  - **FCC has to find a balance between new entrants and incumbents. Worst case favors incumbents; need a complementary method to strike a better balance**

- **Goal**
  - **Make recommendations about the use of statistical methods and risk-informed decision making**

Risk-informed interference assessment

- **Opportunity**
  - **Risk can be managed if it is well understood: bring variability into the open**
  - **Over-conservatism of worst case analysis risks spectrum under-utilization**
  - **Combine insights from worst-case and probabilistic analysis to improve regulatory decision making**

- **Work done so far**
  - **Reviewed statistical risk analysis used by Nuclear Regulatory Commission**
  - **Reviewed examples of statistical techniques used in 3GPP**
  - **Discussed fixed / non-fixed interference scenarios**
  - **Reviewed use of statistical interference metrics by FCC**
  - **Discussed economic externalities of receiver standards**

Risk-informed interference assessment

- Case study analysis underway
  - "Strong-weak" adjacent band case
  - "Fixed / non-fixed" sub-scenario
  - Evaluation of worst case vs. probabilistic risk assessment
- Worst case analysis advantages
  - Concrete single values like maximum transmit power or exclusion distances are easier to grasp than percentiles
  - Provides baseline for sensitivity analysis
  - Interference parameters take a range of values, reasonable "worst case" is a safe choice
  - Provides maximum protection for incumbents

Risk-informed interference assessment

- **Worst case analysis disadvantages**
  - **Does not portray likelihood of risk: multiple independent variables are almost never all maximized simultaneously**
  - **Likely to lead to overall sub-optimal solutions**
  - **Doesn't lend itself to sensitivity analysis**

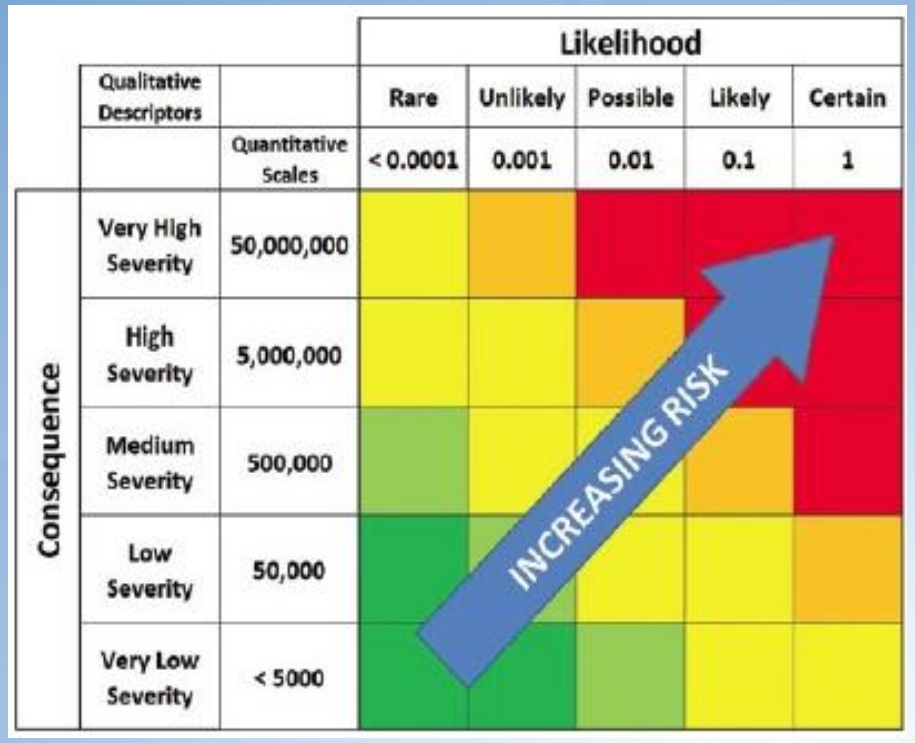
- **Advantages of probabilistic risk analysis**
  - **More realistic representation than worst case**
  - **Probabilistic analysis offers a "currency" for comparing scenarios**
  - **Quantification of uncertainty creates a better picture of what the community of experts knows or does not know**
  - **Highlights areas where the record is insufficient**

Risk-informed interference assessment

Risk assessment

1. What can go wrong?
2. How likely is it ?
3. What are the consequences?

Risk analysis should cover multiple scenarios ; whereas worst case focuses on a single scenario with greatest magnitude



Source : http://reliabilityweb.com/index.php/print/understanding_and_comparing_risk

Risk-informed interference assessment

- **Topics being considered for actionable recommendations**
  - **Develop know-how in the Commission**
  - **Apply statistical method to a low profile, low risk / impact proceeding**
  - **Offer the option of using probabilistic analysis as alternative to worst case in submissions**
  - **For now, leave aside interference scenarios that involve life safety**
  - **Identify simple metrics as proxies for risk that unify different failure modes / hazards**
  - **Assess risk potential against current baseline outage**
  - **When framing risk probabilistically, assess relative and absolute changes; also assess probability of being unaffected**

Interference resolution and enforcement

- **Work accomplished so far:**
  - **Released White Paper "Introduction to Interference Resolution, Enforcement and Radio Noise"**
  - **Held weekly conference calls to develop new strategies for interference resolution and enforcement in a rapidly changing spectrum environment**
  - **Initiated informal coordination with CSMAC in the development of enforcement strategies for a dynamic federal – non-federal shared spectrum environment**
  - **Discussed ex-ante and ex-post methods for interference detection, identification/classification, location and mitigation, and discussed issues of channel use security**

Interference resolution and enforcement

- **Continuing work:**
  - **Analyze the new shared spectrum environment involving the interactions between and among**
    - **Data-base/geo-location based Spectrum Access Systems ("SAS")**
    - **Commission's interference resolution and enforcement equipment and processes**
    - **Spectrum monitoring/measurement systems operated by incumbent federal government agencies to protect their communications**
    - **Other monitoring and measurement systems**
  - **As part of the coordination with CSMAC, develop a very preliminary version of a Straw-man Enforcement Proposal**
  - **Investigate the use of call-signs and equivalents (e.g., MAC addresses) and their utility in the new environment**

Interference resolution and enforcement

- **Further technology topics for consideration:**
  - **Continued study of identifiers and equivalents and information that can be linked to the identifier for enforcement purposes**
  - **Refinement of the Straw-man Enforcement Proposal in coordination with the CSMAC**
  - **Study of the usefulness of I/Q signal recordings from various platforms for forensic detection and analysis of interference incidents**
  - **Noise floor measurements / modeling**
  - **Methods to ensure channel / spectrum availability and security**

Channel Use Compliance – Multi-tier Band Sharing

- **Channel Use Compliance:**
  - **Assured compliance with authorized channel parameters**

- **Previous licensed regimes were strictly controlled:**
  - **Central network control**

- **Previous unlicensed regimes were not strictly controlled:**
  - **Distributed network control**
  - **Local autonomous firmware control of tuning**
  - **Interference was to other ‘un-protected’ status devices**
  - **Local firmware control is vulnerable to tampering, allowing unauthorized frequency use**

Channel Use Compliance – Multi-tier Band Sharing

- **New band sharing paradigm 'mixes' different tiers of uses:**
  - **Different interference, control & security expectations & capabilities**
  - **SAS manager will allocate channels to different tiers**
  - **How can SAS manager 'enforce' assignments in real time if lower tier access points are autonomously controlled?**
  - **Very large number of lower tier users would make ex post enforcement difficult and fleeting**
- **Need: Channel Use Compliance (e.g. channel tuning control at access point)**
  - **Fail safe SAS control of access point tuning (e.g. encrypted tuning words from SAS to synthesizer ASIC)**

4Q'14 Deliverables

- Make recommendations for using risk-informed interference analysis
- Report on analysis of a generic type of interference scenario between at least two classes or types of radio services
- Report on relevant statistical factors affecting regulatory policy
- Report and recommendations for an enforcement strategy for a shared spectrum environment (development and refinement of Straw-man Enforcement Proposal)
- Report on technology enablers (e.g., automatic identifiers/classifiers and collection of I/Q information for forensic analysis) for interference resolution and enforcement

THANK YOU

Technological Advisory Council

Advanced Sharing and EWT WG

September 23, 2014

Charter

- Establish an advanced sharing framework to enhance spectrum efficiency while protecting incumbent services, including both Federal and non-Federal services
- Identify and evaluate enabling technologies to enhance sharing efficiency, develop requirements for protection of incumbent services, and encourage co-existence of Federal and non-Federal systems
- Provide recommendations to the Commission regarding the establishment and objectives of “RF Model City” where the proposed advanced sharing framework and enabling technologies can be tested and evaluated

WG Participants

- Co-Chairs:
  - Sanyogita Shamsunder, Verizon
  - Brian Daly, AT&T
- FCC Liaisons:
  - Michael Ha
  - Chris Helzer
  - Kamran Etemad
- Participants/Guest Speakers:
  - Mark Bayliss, Visual Link
  - Lynn Claudy, NAB
  - Marty Cooper, Dyna LLC
  - Adam Drobot, OpenTechWorks
  - Kumar Balachandran/Mark Racek, Ericsson
  - Kevin Kahn, Intel
  - Milo Medin, Google
  - Dean Brenner/Luis Lopes/Etieen Chaponniere/Yongbin Wei, Qualcomm
  - Kevin Sparks/Milind Buddhikot/Harish Viswanathan, ALU
  - David Gurney/Bruce Mueller, Motorola
  - Prakash Moorut, Nokia Networks
  - Patrck Welsh/Arda Aksu, Verizon
  - Maqbool Aliani, Lightsquared
  - Neeti Tandon, ATT
  - Steve Sharkey, T-Mobile
  - Michael Fitz, TrellisWare

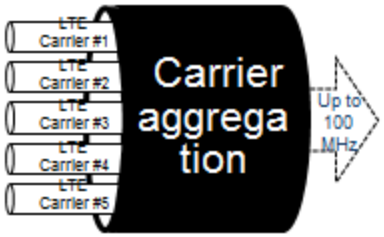
Enabling Technologies Sub-WG: Discussion Summary

- The sub-group has had presentations on a number of subjects relating to technologies/techniques that can be used to enable spectrum sharing
  - The evolution of LTE-- LTE-Advanced and interference cancellation technology
  - Co-existence testing between LTE small cells and radars conducted by NTIA
  - Identification of candidate spectrum bands to be targeted for sharing
  - In building propagation analysis for possible sharing of spectrum with outdoor incumbents
  - The aim of the sub-WG is to create a menu of technology options to enable spectrum sharing to the greatest extent possible

LTE Advanced brings different dimensions of improvements

Leverage wider bandwidth

Carrier aggregation across multiple carriers, multiple bands, and across licensed and unlicensed spectrum



Higher data rates
(bps)

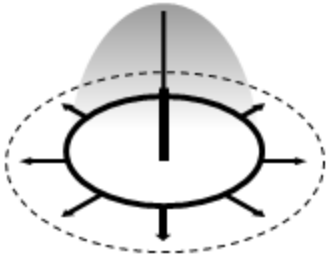
Leverage more antennas

Downlink MIMO up to 8x8, enhanced Multi User MIMO and uplink MIMO up to 4x4

Higher spectral efficiency
(bps/Hz)

Leverage HetNets

With advanced interference management (FeICIC/IC)

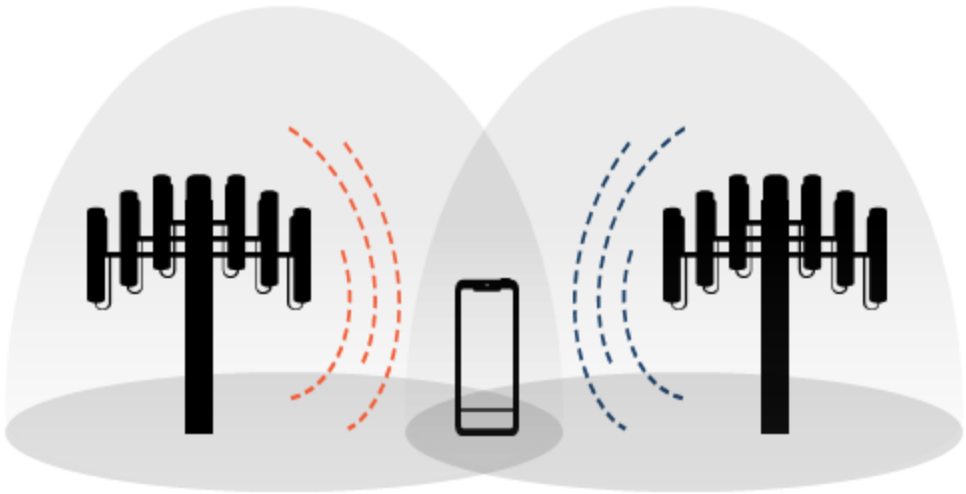


Small Cell Range Expansion

Higher spectral efficiency per coverage area
(bps/Hz/km^2)

Enhanced receivers offer better user experience & more capacity

Interference Cancellation



Interference Cancellation	Rel. 10/11	Re. 12
Sync ref. signal	✓	✓
Common ref. signal	✓	✓
Primary broadcast channel	✓	✓
Data channel		✓

- Higher data rates especially at cell-edges
- More network capacity
- Even more beneficial in managing interference in small cell deployments

Examples of LTE Features for Sharing

Example of LTE Feature	Enabler for	Comments / findings
Immediate Shutdown	Spectrum Clearing	Effective but calls drop.
Graceful Shutdown	Spectrum Clearing	Effective but TX dynamic range issue (Hardware & deployment dependency)
Cell Barring	Spectrum Clearing	Desired UE behavior depends on UE state. Use with other features.
UL pMax Control	Interference Management	Exclusion zone reduction benefit depends on RF conditions / path loss to UE.

- Current LTE standards and commercial equipment support enablers that serve as a foundation for a spectrum sharing solution
- Future LTE releases and products enable additional capability through such as features as carrier aggregation, load balancing and others

Key Learning: Interference Cancellation/Suppression of LTE Advanced

- Interference cancellation/suppression is a very important aspect of LTE and LTE-Advanced: Today, it's used to improve data rates, especially at cell edge and add network capacity.
- When an interference signal's waveform properties are know at the victim, interference cancellation can be used. When the victim does not have the knowledge of the waveform's property, interference suppression can still be used
  - An LTE UE has at least 2 RX antennas, and eNB can have 2, 4 or 8 RX antennas. Spatial filtering is a powerful tool for interference suppression
- As small cells are deployed, and hetnets become operational, interference cancellation is even more important because interference cancellation allows the hetnet operator to achieve the greatest possible gains from the small cells.
- Recent testing conducted by NTIA of LTE small cell/radar co-existence verified that LTE is quite robust vis-à-vis other radios (i.e., radars), even when the interference is very high. However, further study is needed for modern radars with higher duty cycle
- Using an appropriate SAS and lower power LTE small cells will enable co-existence with radars with relatively small exclusion zones.

In-building Only Sharing

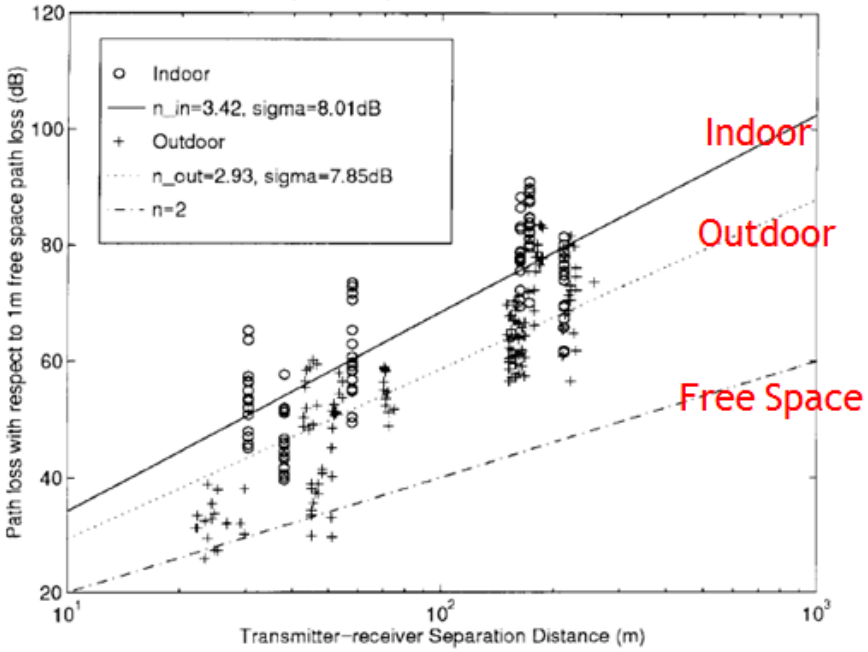
- In-building only sharing could be an option if outdoor sharing creates too much interference
- Enabling Technology Sub-WG has reviewed the additional propagation loss of various types of building material
- It also discussed a recent study on satellite-to-indoor measurement
- Given the demand of in-building services, this could be a sharing option to consider

Penetration Loss at 5.85GHz

SUMMARY OF ALL ATTENUATION VALUES (LOSS IN EXCESS OF FREE SPACE) AT 5.85 GHZ WITH OUTDOOR TRANSMITTERS AT 5.5 m HEIGHT ABOVE GROUND.

	Partition	Loss (dB)	σ (dB)	$\Delta\sigma$ (dB)
	Home exteriors			
Paper insulation	Brick†	12.5		
	Rappaport Home, 30m TX	10.2	2.6	3.1
	Rappaport Home, 150m TX	14.8	2.1	4.5
Foil insulation	Brick*	16.4		
	Tranter Home, 48m TX	16.1	3.4	3.9
	Tranter Home, 160m TX	16.6	3.2	4.5
Paper insulation	Wood Siding†	8.8	3.5	0.9
	Cinderblock wall	22	3.5	6.4
	Subterranean basement	31		
	Tranter Home, 48m TX	34	3.4	3.7
	Tranter Home, 160m TX	29	3.2	2.7
	Home Interior			
	Plaster walls	4.7		
	Rappaport Home, 30m TX	4.7	2.6	1.1
	Rappaport Home, 150m TX	4.6	2.1	0.8
	Plasterboard walls	4.6		
	Tranter Home, 48m TX	3.6	3.4	1.9
	Woerner Home, 30m TX	5.6	3.5	1.2

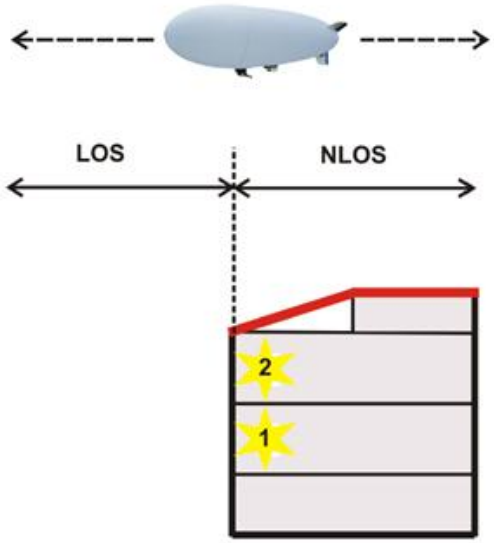
Source: Durgin, G.; Rappaport, T.S.; Hao Xu, "Measurements and models for radio path loss and penetration loss in and around homes and trees at 5.85 GHz," *IEEE Transactions on Communications*, vol.46, Nov 1998



Alcatel·Lucent

Satellite To Indoor Measurement Campaign

SOURCE: Kvicera, M.; Horak, P.; Korinek, T.; Zela, J.; Simunek, M.; Pechac, P., "Building penetration loss measurements for satellite-to-indoor systems: Preliminary results,", *2010 Proceedings of the Fourth European Conference on Antennas and Propagation (EuCAP)*, April 2010

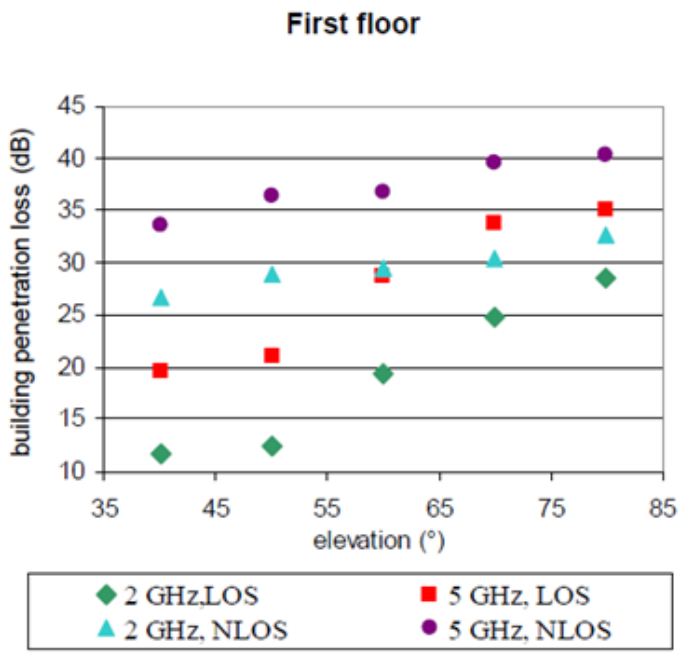


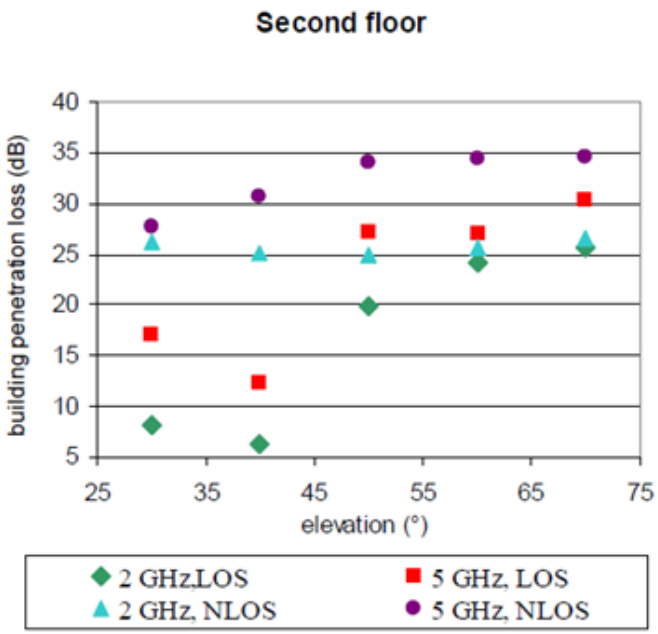
- Wide range of elevation angles to the transmitter
- Surrounding buildings are of the same height
- LOS: Front wall of the building where measurement is illuminated by TX
- NLOS: Back wall or roof of the building or surrounding buildings are directly illuminated
- Measurements made at 5 different buildings

COPYRIGHT © 2013 ALCATEL-LUCENT. ALL RIGHTS RESERVED.

Alcatel·Lucent

Satellite To Indoor Measurement Results





- Loss to first floor is higher
- Higher Loss at higher frequencies
- NLOS loss is higher

COPYRIGHT ©2013 ALCATEL-LUCENT. ALL RIGHTS RESERVED.

Alcatel·Lucent

Approach To Shared Spectrum

- Preferred candidate bands
  - NTIA lists of candidate bands
  - ITU-R candidate bands for IMT from JTG4-5-6-7.
    - Possibly restricted in the US
- < 3 GHz
  - Advantageous for coverage
  - Fewer incumbents and smaller exclusion zones are desired
  - Certain applications may require smaller bandwidth than wireless broadband services
- > 3 GHz
  - Suitable for capacity enhancement
  - May be able to handle varying degrees of incumbent use
  - Outdoor service offers more flexibility and in-building-only service may offer additional interference protection mechanism
  - Expected spectrum yield should be more than 100 MHz per band
- Consider both licensed and unlicensed applications in all bands

Candidate Bands List (1/4)

ITU-R/IMT (MHz)	NTIA (MHz)	Federal incumbent	Commercial/Global Use	Comments
1350-1400	1300-1370	Long range ground-based ATC radar		Candidate for sharing studies by FCC TAC
	1370-1390	Long Range ground-based ATC radar; DoD: mobile telemetry, GPS relay, point-to-point and ship-to-ship communications, nucear burst detection, RAS		
1427-1452		1427-1429.5: DoD fixed point-to-point and ground-to-air 1429.5-1432: DoD limited use voice and data communications in training ranges; federal medical data collection	1435-1525: Commercial AMT for flight testing	Aerospace and Flight test Radio Coordinating Council is the non-Govt. coordinator for frequency assignments in 1435-1525 MHz
1452-1492 1492-1518 1518-1525		1435-1525: AMT for testing, range safety, chase aircraft, weather data	Broadcasting Satelilite LTE Band 21 uplink (1447.9-1462.9 MHz	1427-1525 Possible band for sharing studies by FCC TAC
2700-2900	2700-2900	Air Traffic Control (ATC), Airport Surveillence Radar (ASR), weather radar including NEXRAD operated by the NWS, FAA and DoD.		NTIA identification for exclusive or shared use.

Candidate Bands List (2/4)

ITU-R/IMT (MHz)	NTIA (MHz)	Federal incumbent	Commercial/Global Use	Comments
	3100-3550	DoD: Ground and Airborne radar systems, usually fixed frequency for airborne	ITU-R: Radio Location systems	NTIA list shows 3100-3550 MHz for shared use
3300-3400		Ship-based, land-based and airborne radar systems; ship-based radar for littoral waters	ÌTU-R: Radio Location Service	
3400-3600		Coastal radar	ITU-R: Radio Location Service	
3700-3800		Federal and civilian use of 3700-4200: for satellite earth stations in support of voice, data, and video transmissions used in conjunction with commercial geostationary satellites for space-to-earth in conjunction with 5925-6425 MHz	ITU-R: Fixed Satellite Services and fixed services, common carrier fixed microwave	Commercial C-band downlink. Possible Candidate for FCC TAC consideration for shared use outdoor/indoors/small cells.
3800-4200				

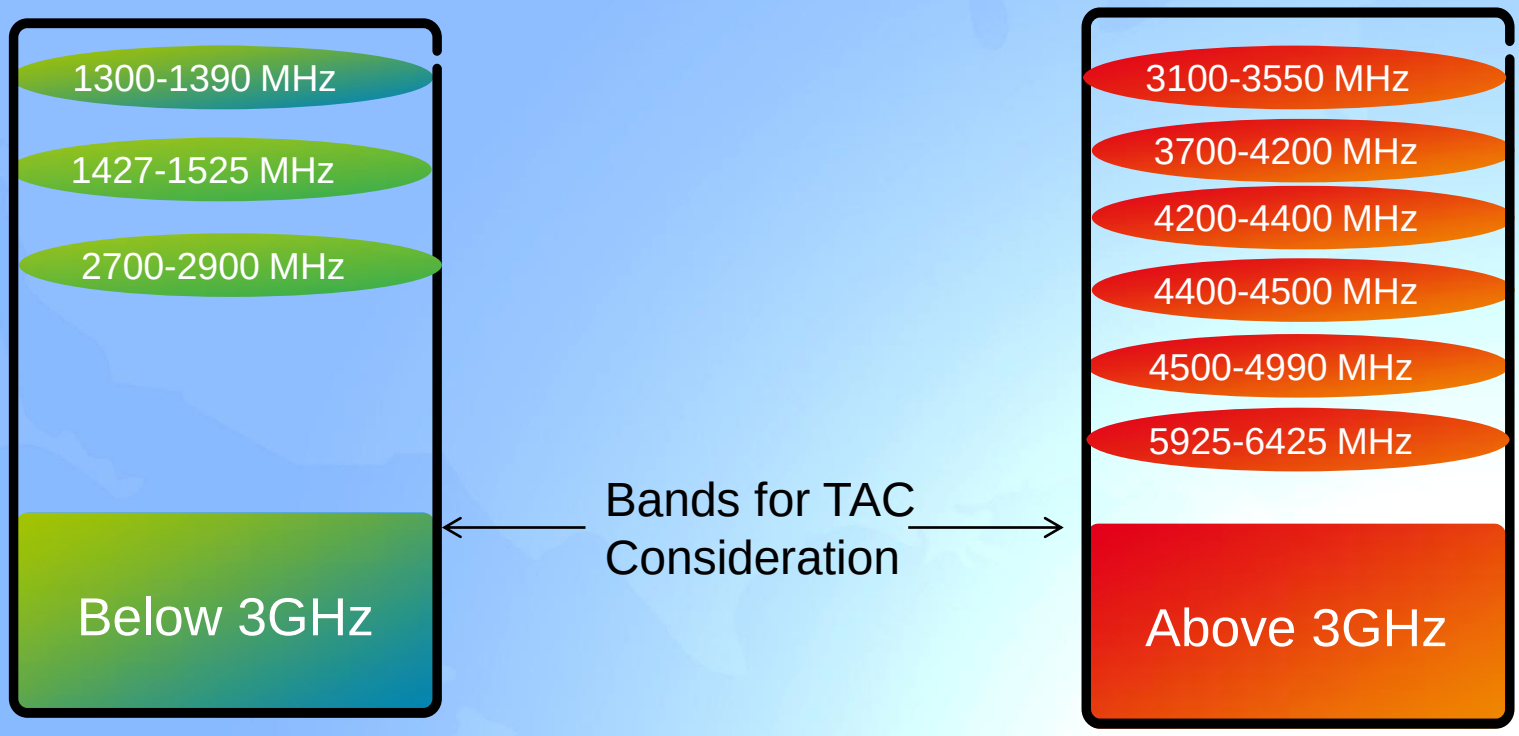
Candidate Bands List (3/4)

ITU-R/IMT (MHz)	NTIA (MHz)	Federal incumbent	Commercial/Global Use	Comments
	4200-4400	Radio Altimeters and Aeronautical Mobile Telemetry	Radio Altimeters and Aeronautical Mobile Telemetry	NTIA shared use identification; Possible candidate for TAC consideration for outdoor/indoor/ small cell use
4400-4500		Federal Government fixed and mobile services; military for training; supports fixed Line of Sight (LOS) and transportable-fixed point-to-point microwave systems, drone vehicle control and telemetry systems; Civilian federal agency use for the band for nuclear emergencies and law enforcement activities		
4500-4800		DoD: Line-of-sight and trans-horizon radio communications; air-to-ground operations for command and control, telemetry to relay data, and various range systems. Federal: video, law enforcement, drug interdiction missions and nuclear emergency response	ITU-R: Fixed Satellite Space-to-Earth	

Candidate Bands List (4/4)

ITU-R/IMT (MHz)	NTIA (MHz)	Federal incumbent	Commercial/Global Use	Comments
4800-4990 MHz		4800-4940 tuning range: military use at test ranges and naval ports; also, federal use for law enforcement, and drug Interdiction; RAS authorized		
		4940-4990	4940-4990: US: exclusively for non-Federal fixed and mobile; Space Research and EESS (passive, secondary); point-to-point data links; research and testing; land mobile; and air-to-ground operations. There are also limited uses of this band for flight telemetry and ship-to-shore operations; band transferred to non-Govt use in 1999	
5925-6425		N/A		US and ITU-R: Geostationary C-band satellite uplink, fixed service lower band

Sharing Recommendations



- Advanced Sharing WG recommends the Commission to consider these bands for future sharing
  - Specific sharing model would depend on the incumbent types and available tools to manage interference among various systems

Spectrum Database (SDB) Sub-WG

- A wide range of solutions may be involved to enable dynamic spectrum sharing and should be considered in Spectrum DataBase (SDB) frameworks .

Unlicensed	Local Sensing	Sensing Networks	Time Specific Exclusion	Fixed Exclusion
Limits in Power Adequate	Strong, detectable signals (e.g. DFS)	More Complex Detection, and better siting	Database Driven (e.g. SAS)	If Undetectable, or constantly on

Fixed Rules in Devices

Adjustable Rules in Database System

Spectrum DataBase (SDB): Protection Zones

- Dynamic Spectrum sharing between incumbent and secondary user taking advantage of spatial and temporal patterns of incumbent use would allow more efficient spectrum utilization.
- Protection zones may be used when incumbent use is present. In cases where incumbent use is static and/or cannot be shared, directly or indirectly, with secondary users static protection zones may be used
  - Static Zones: Never change whether primary present or not
  - Dynamic Zones: Reflects presence or absence of primary Via Primary assistance or passive, collaborative monitoring
- It is preferred that Protection Zones be defined based on incumbent protection criteria rather than fixed geographical areas.
  - Challenge is realistic propagation and interference modeling
  - A hybrid of fixed but reduced exclusion zone and a signal based protection zone may be used

SDB: Passive and Active Spectrum Management

- **Passive may use Channel ranking:**
  - DB aggregates measurements from Authorized User (AU) networks to assess quality and rank channels and provides to AUs a ranked list instead of static list
  - Similar to but enhanced variation of TVWS.
- **Active Secondary Channel management:**
  - Allocate channels to AUs to minimize aggregate interference to primary and maximize secondary capacity.
  - Channel reallocations should be minimized to protected networks
- Active Management may be more efficient but requires coordination if multiple SDB's are involved.
- Passive Management is simpler and may still be viable in some bands.

SDB: Key Learning and Other Issues to be Discussed

- Boundaries and allocations between systems being shared should be based on interference protection criteria, and not on fixed geographic boundaries like exclusion zones
- SDB's should be given flexibility to manage specific frequency assignments to maximize overall capacity of the band
- Enforcement and Security are two key issues to be addressed by multi-stake holder organization, standard bodies and regulators.
- Strict and clear requirements need to be defined and used in certification.

RF Model City

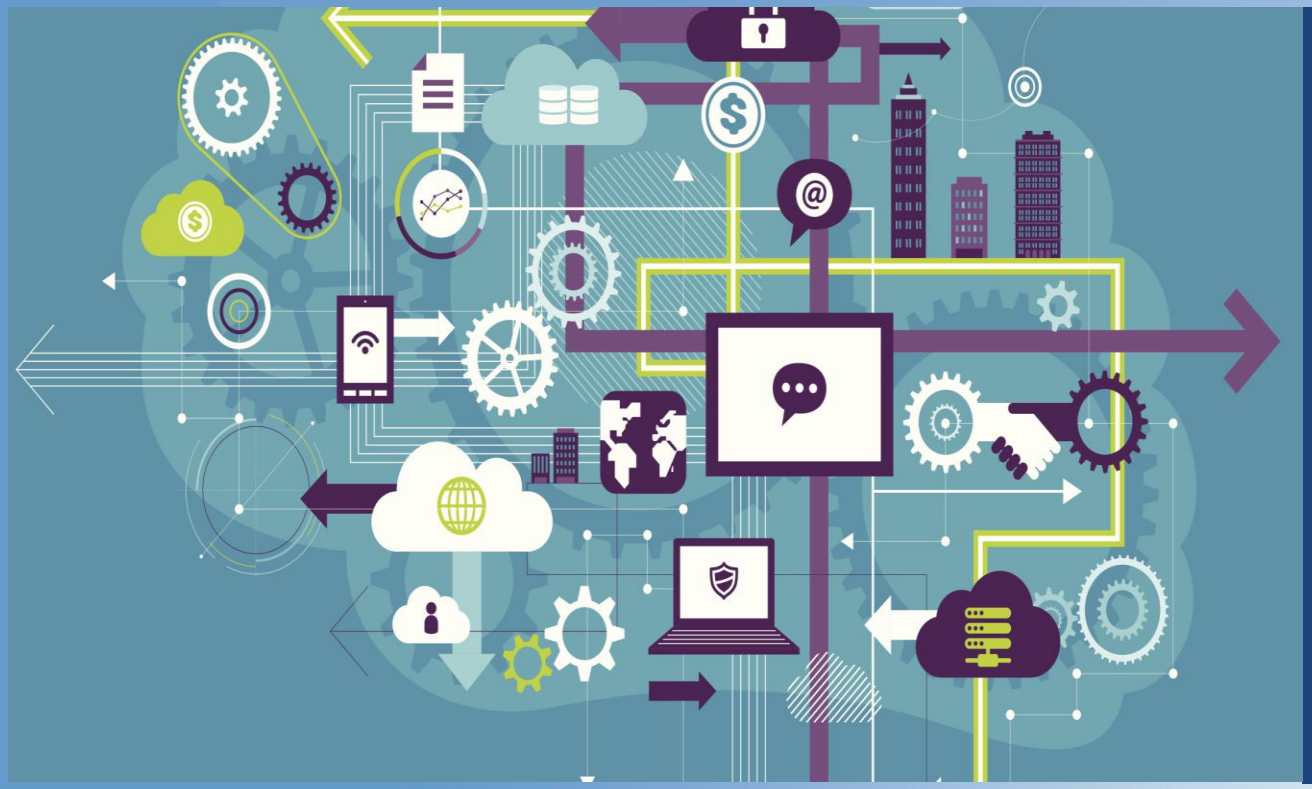
- Total of 13 responses: OEM, Small Business, Carriers, Associations, Cities
  - Pegasus Holdings, District of Columbia, City of Chicago, DC Digital Drive, ATT, CTIA, Dynamic Spectrum Alliance, TIA, City of Cincinnati and Cincinnati Bell, ARRL, NSN, Wireless Innovation Forum, Federated Wireless
- Generally supports the RF Model City concept and some demonstrated high interest in moving forward
- Several bands (1755, 3.5, 1370-1390, 2200-2290, 2700-2900, 4200-4400MHz) have been suggested with various applications servicing commercial, federal and public safety interests
- Mixed suggestions on exclusive use and dynamic sharing
- Suggested new flexible experimentation rules, FCC/NTIA to deliver governance and support stakeholders to develop, plan, test and report transparently
- Funding suggestions ranged from entirely private funding to public-private mix. Usage fees and funding models similar to European Union programs were also suggested
- NSN's comments on propagation measurement is an area of interest for the Advanced Sharing WG

Next Steps

- Continue discussions on candidate bands and enabling technologies
- Enabling Technologies Sub-WG will continue examining a range of technologies to create a menu of options to enable sharing in a variety of circumstances
- Per NSN's comment on the RF Model City, develop a framework for propagation model for future sharing simulations
  - Propagation model has the greatest sensitivity on determining the size of protection/coordination zones
  - WG will collaborate other streams of similar efforts and provide recommendations in December meeting
- Advance SDB discussions into actionable recommendations

CAPTION

FCC TAC: IoT- Sept 23, 2014



How will IoT impact *communications* networks in the next

10 years?

20 years?

CAPTION

IoT WG

Sept 23, 2014

- Russ Gyurek- (Co-Chair), Cisco
- David Tennenhouse- (Co-Chair), VMware
- Walter Johnston (FCC)
- Shahid Ahmed, Accenture
- John Barnhill, Genband
- Mark Bayliss, Visuallink
- Kevin Cage, NAB
- Greg Chang, Yume
- Marty Cooper, Dyna
- Kevin Kahn, Intel
- Mark Gorenberg, Zetta Ventures
- Stephen Hayes, Ericsson
- Anoop Gupta, Microsoft
- Joe Salvo, GE
- Adam Drobot, OpenTechWorks
- Amit Jain, Verizon
- Ranato Delatorre, Verizon
- DeWayne Sennett, ATT
- Brian Markwalter, CEA
- Lynn Merrill, Monte R. Lee
- Jack Nasielski, Qualcomm
- Ramani Pandurangan, XO Comm
- Deven Parekh, Insight Partners
- Marvin Sirbu, CMU
- Kevin Sparks, ALU
- Glen Tindal, Independent
- John Brzozowski, Comcast
- David Gurney, Motorola
- Hans Juergen Schmidtke, Juniper

CAPTION

Charter

- Identify key areas in the evolving Internet that should drive the work of the Commission or areas where the Commission should seek key information
- What new demands will the Internet of Things (including M2M) place on the network?
- What technology policy challenges exist in the evolution towards an Internet of Things?
- Explore how the FCC can foster IoT innovation and leverage federally funded R&D in this area

CAPTION

Focus & Actions

- Created a detailed Taxonomy of IOT by vertical segment
  - Used to filter from broad IoT market to relevant FCC focus, and “sizing”
- Several Position statements
  - Safe Harbor
  - Privacy
  - End-of-Life (EoL)
  - Co-existence (Etiquette)
- Demos: Consumer (2), Industrial (1), Technology- 6LoWPAN (1)
- IoT Sizing: Forecasts trends, scenarios,
  - Narrowing the focus: does video as a sensor disrupt the network as we know it?
- Security: What is FCC role, what is the line between edge/things vs cybersecurity
- Removing barriers and providing incentives

CAPTION

Safe Harbor Statement

- Many classes of IoT devices operate over a limited range and are expected to have a long life (8 year or greater life expectancy).
- To avoid spectrum support issues over this long period, it is recommended that such devices, and the networks to support them, utilize unlicensed operations where practical.
- This recommendation is critical whenever a safe harbor from wireless technology evolution is desired.

CAPTION

IoT Privacy Statement

The ubiquity of information exchange in the Internet of Things is creating privacy challenges for our society.

Recommendations:

1. Working with industry, develop an understanding of current approaches that support the reliable acquisition, transport, use and exchange of information across different vertical service/market groups.
2. Work with appropriate agencies and industry that define norms applicable to Internet of Things.
3. Understand public concerns and the impact of data breaches in relation to IoT on the consumer.

The TAC does not foresee the FCC playing the <u>lead</u> role on IOT privacy, however the FCC must be well-informed and a party to the discussions

CAPTION

IoT E0L Statement

Technology, whether for application, transmission capacity, or device, has an expected viable lifetime and IoT capable products will be no different. However, EoL issues associated with IoT can be especially challenging given the intersection of the very low cost and long expected life nature of many IoT devices.

- *End Of Life / End of Service Announcements be made publicly available sufficiently in advance allowing parties to manage the impact of EoL actions (e.g., download any relevant documentation, install final patches, etc..)*
- *End Of Life / End of Service Announcements should consider - and where possible highlight - critical exposures that the End Of Life action might create (eg., increased security issues)*

CAPTION

Unlicensed Etiquette Statement

In unlicensed bands, FCC rules provide that unlicensed users must accept interference (and may not cause harmful interference).

Although this regimen has worked well; now may be the right time for the FCC to investigate potential next steps in the evolution of the "digital etiquette".

Recommendations

- *SDO's should continue to coordinate with each other to facilitate co-existence.*
- *Non-standard wireless solutions should strive to protect the commons in ways that allow the operation of other technologies.*
- *As new frequency bands are allocated there may be significant value in re-examining co-existence techniques for unlicensed spectrum. …. the FCC should be open to future policy supporting ultra-efficient spectral technologies which may require that some newly allocated bands be restricted to use of specific technologies and or control protocols*
- *The IPv6 network protocol offers several advantages over IPv4 … and should be used where feasible.*

CAPTION

IoT Sizing

Millions of Apps, Billions of Connected Devices, Billions of Sensors

- Projections Vary Wildly
  - Project 50B Devices by 2020, Others Project Over 1 Trillion in 20 years
  - Reports assess GDP impact – Range 20T USD to 73T USD
  - Growth acceleration attributable to Microcontroller Price/ Performance, Sensor Advancements, Ubiquitous access, Sensor Advancements, Cloud infrastructure, and apps
- Note: Estimates based on Analyst forecasts based on current and announced service sets:
  - Factors not addressed:
    - New apps/ radical changes in data variety may significantly impact data volume (e.g. Video as a sensor)
    - Migration of data from private to public networks

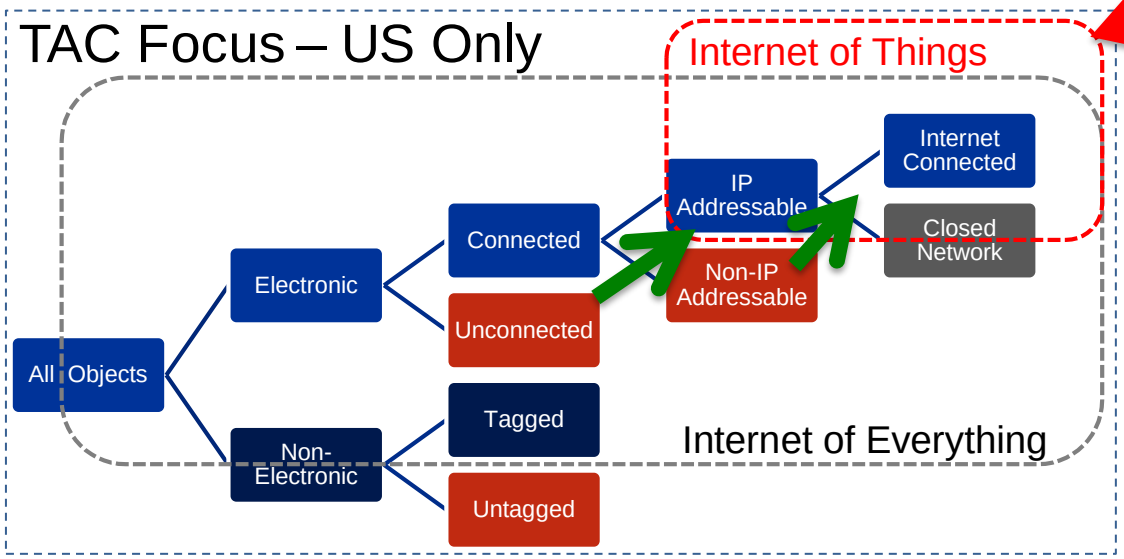
Device Activations: Today = 80 per Second. 2020 = 250 per second

CAPTION

Narrowing the Scope – Connected Devices

Global Reports

Source Courtesy of Bill Morelli, IHS



Potential Growth items to Consider:

- Disruptive Business Models (OTT's and more)
- Low cost of cloud computing promotes connectivity
- Desire to capture previously "transient" data for analytics
- Video enabled devices
- Forward looking projections based on current apps. New apps could accelerate #'s

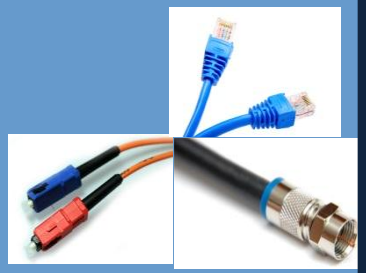
CAPTION

IoT Connectivity Technologies

Source: Courtesy Bill Morelli, IHS Technologies

Wired

- Ethernet, Coax, Fiber, etc. considered as a single category



WPAN

- ANT+
- Bluetooth – Classic & Smart Ready
- Bluetooth Smart

WLAN

- ZigBee PRO
- ZigBee RF4CE
- ZigBee Multi-Protocol
- EnOcean
- ISA100.11a
- WirelessHART
- Z-Wave
- Other 802.15.4

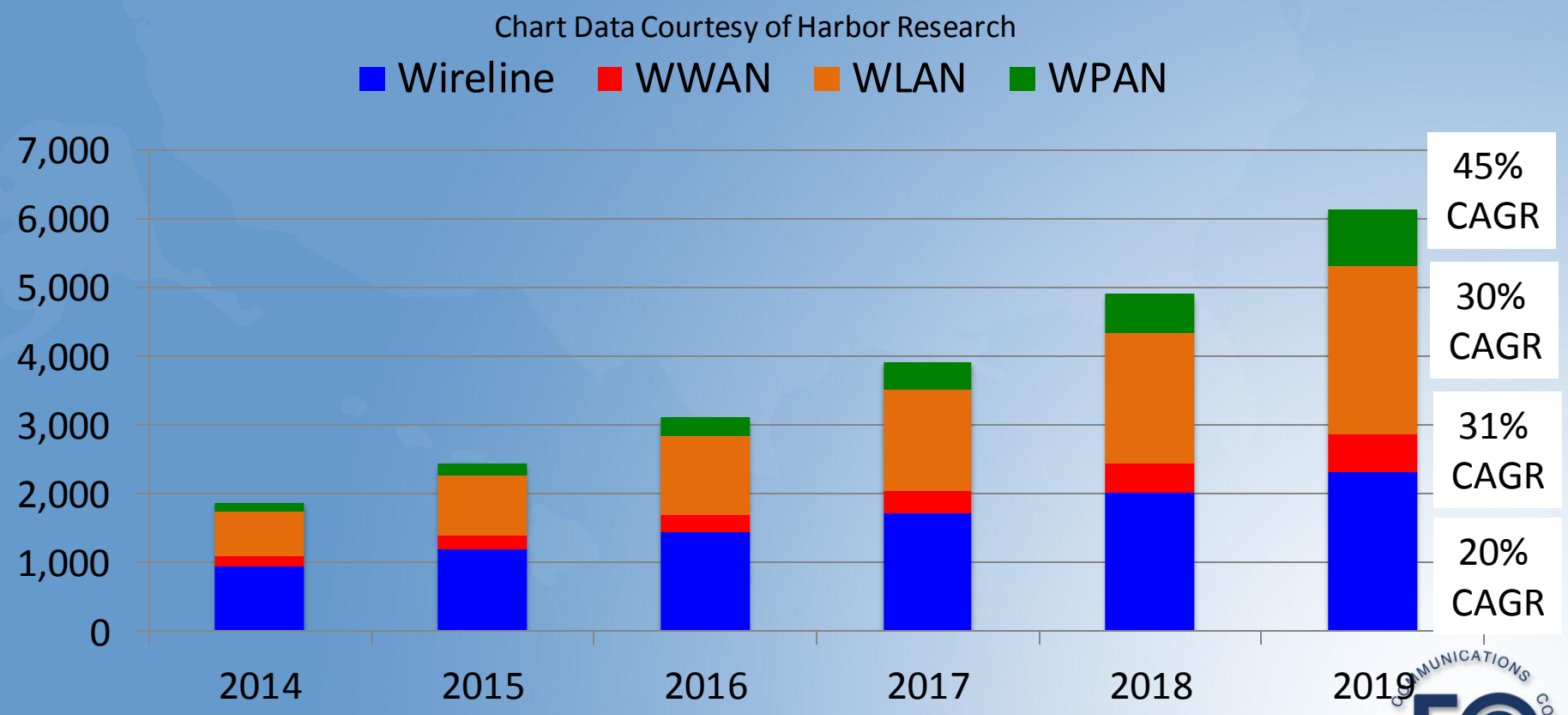
- 802.11a/b/g
- 802.11n
- 802.11ac
- 802.11ad
- Other 802.11
- DECT ULE
- Other 2.4GHz
- Other Sub-GHz

WWAN

- 2G Cellular
- 3G Cellular
- 4G Cellular

CAPTION

USA* Device Growth (M)



* Based on 85% of North American Growth as projected by Harbor Research Market Sizing Information

CAPTION

Sizing: Initial Observations & Next Steps

Volume vs Quantity

- IoT Traffic Patterns
  - Our work to date has considered the number of things.
  - A key next step is to construct scenarios related to the traffic intensity/patterns those things may generate and consider their implications for the network, especially the access network.
- Downstream vs Upstream Traffic
  - The "last mile" of wired and cellular broadband networks has been architected for asymmetric, downstream-intensive, traffic patterns
  - Future IoT traffic may be more upstream-intensive. If so, this could have significant implications for access networks
  - Is DropCam® a canary in the coal mine?

CAPTION

IoT Security Context

IoT WG Security Considerations – *not with a regulatory intent*:

- Large wave of new devices are going to enter the market
- Vast number of these devices will push content to the cloud
- Few of these devices are focused on or capable of addressing security exposures
- A growing volume of personal and geo-location data will cross the network to the cloud
- Net security exposure includes: identity theft, snooping, spoofing, botnet attacks, etc

IoT broadens the attack surface & creates new attack vectors

CAPTION

IoT Security: Initial Observations

- The IoT market is still nascent; IoT security is the role of multiple organizations, SDO's and government agencies
  - SDO and Consortiums are creating best practices
  - SP are creating best practices
  - The industry has recently demonstrated it will act quickly to address significant issues
- The FCC needs to clearly define what its role is within the IoT Security landscape
  - That role is likely focused on the protection of the network and avoidance of widespread disruption
  - It probably does <u>not</u> include security of the things themselves and/or of their cloud-based services
  - Somewhere in the network, IoT security becomes a cybersecurity issue of the sort dealt with today
    - *That somewhere is unclear*
- Three main focus areas for the TAC to explore:
  - Data transport / network security
  - Application Security
  - User security

CAPTION

IoT WG Next Steps

- Security
- IoT Sizing / Traffic Patterns
  - and their implications for the network
- Explore ways to stimulate innovation / investment
- Finalize recommendations

CAPTION

QUESTIONS, COMMENTS, INPUT

Cybersecurity Working Group

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

23-September-2014

Mission Statement

New security vulnerabilities in software and hardware continue to emerge, imposing even greater externalities and societal costs on users. Security software is widely available, but most security solutions aim to protect software and hardware after systems have been built and deployed. Software and hardware security are too frequently seen as an afterthought or a potential hindrance to businesses, routinely addressed after a product is released into the marketplace. Improving security and reducing the aftermarket and social costs of security failures requires building security into software and hardware at the initial stages of the design and development process.

- What collaborative activities within or between industry and government organizations focus on building security into software and hardware, and how can these or other collaborative activities be strengthened, modified, or initiated to more effectively address security problems? How can the FCC act to promote the effectiveness of these activities?
- How can the FCC collaborate with academic institutions to bridge the gap between current computer sciences curriculums, which lack focus on security as a core tenet, and the need for secure coding as an integral piece of computer sciences degrees?

Mission Statement Key Objectives

- How do threats appear in the supply chain paradigm, and how can supply chain resiliency be improved to address these issues?
- What are the most important considerations that should be addressed in determining how software and hardware are designed and developed to reduce the number of security patches that are needed post-deployment?
- Who are the important stakeholders, and how can new or smaller manufacturers and vendors be included in the process?
- What processes are needed to allow for the open sharing of software and hardware security threats and solutions, while providing adequate safeguards for confidential information?
- Where can new or modified procedures highlight and address software and hardware security concerns in the design and development process?
- What technical measures can manufacturers and vendors take, as part of the design and development process, to reduce the risk their products will have security issues post deployment?
- How can training be improved to help manufacturers and vendors build security into software and hardware?
- What roles, if any, do testing and auditing have to play in building security into software and hardware, and how can they be used more effectively?

Working Group Members

- WG Chair: Paul Steinberg, Motorola Solutions
- Vice Chair: Ramani Pandurangan, XO Communications
- FCC Liaisons: Jeffery Goldthorp, Lauren Kravetz

- Members:
  - Ernie Bio, incNetworks
  - Brian Daly, AT&T
  - Renato Delatorre, Verizon Wireless
  - Martin Dolly, AT&T
  - Adam Drobot, Open Tech Works
  - Jeff Foerster, Intel
  - Russ Gyurek, Cisco
  - Mike McNamara TWTelecom
  - Lynn Merrill, Monte R. Lee
  - Jack Nasielski, Qualcomm
  - Anand Palanigounder, Qualcomm
  - Deven Parekh, Insight Partners
  - George Popovich, Motorola Solutions
  - Jesse Russell, incNetworks
  - Harold Teets, TWTelecom
  - S Rao Vasireddy, Alcatel Lucent
  - Jack Waters, Level 3 Communications

Our progress since the June 10th meeting (1 of 2)

- Initial focus was around 1) **insider threats** and 2) **security metrics**, with reports due by the end of July
  - **Insider threats** (Led by Mike McNamara of TWTelecom)
    - **STATUS**: Collaboration led by Mike McNamara resulted in a report summarizing industry status best practices, and recommendations for the FCC **(Attachment 1)**
  - Security Metrics evolved away from reporting on metrics to **cyber security processes and functions** (Led by Renato Delatorre (Verizon Wireless) and Martin Dolly (AT&T)
    - **STATUS**: Collaboration led by Renato Delatorre (Verzion Wireless) and Martin Dolley (AT&T) resulted in report summarizing best practices published **(Attachment 2)**
  - Adam Drobot is driving a forward leaning effort assessing the current industry landscape around **insider threat mitigation technologies**
    - **STATUS**: Progress temporarily delayed to consider other topics (see later detail) – activity resumed with a report planned by end of year.

Our progress since the June 10th meeting (2 of 2)

- Projects Requested by the FCC
  - Further work on Insider Threat - Security Accountability
    - Define mechanisms / methods to track/assess actions of key Cyber Security practitioners (Analogous to a Cyber Logbook)
  - Security Practices for Core Network Equipment
    - Cyber Rating/Certification for Equipment (Analogous to a Cyber UL Rating)
  - Mobile Device Consumer Interface for Privacy & Security
    - Enhance & Automate FCC Security Checker in a User-friendly way (CAC/TAC Collaboration)

Insider Threat Mitigation Technologies

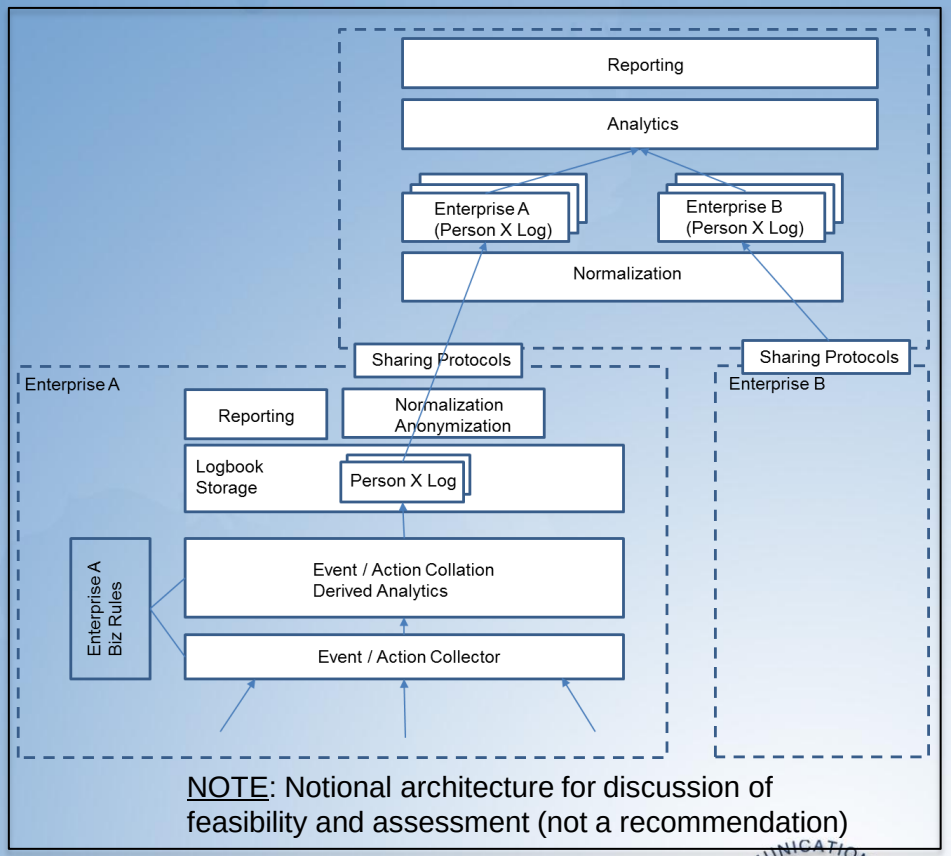
- **Background**
  - Assess and recommend future technologies for cyber security that the FCC could promote/advance
- **Cyber TAC WG action items**
  - Create an awareness of the vulnerabilities, the subsequent impacts, and the frequency (probability) with which a specific vulnerability pathway will lead to an incident.
  - Within the context of the NIST Cyber Security Framework, we will further examine enabling technologies.
- **Workplan**
  - For each of the five NIST Framework elements (Identify, Protect, Detect, Respond, Recover), we will look to data collection and analytics to further the current thinking on how these mechanisms can help mitigate the growing insider threat problem.
  - For example, we plan to leverage protection technologies and methods such as:
    - Security layering to increase monitoring and detection methods/tools
    - Trusted computing techniques to protect storage, logs, and control plane assets
    - Greater use of encryption to protect data
    - Examination of all connected devices for malware
    - Access control and monitoring, including moving beyond passwords for user authentication
  - Target timeline: Recommendations for the December TAC meeting

Insider Threat – Security Accountability Mechanisms

- **Background**
  - Automate collection of cyber activities/actions for key professionals/roles
  - Create a cyber personal record that lives with the professional across roles within an Enterprise or across Enterprises
  - Analogous to a Pilots 'log book' that contains a record of their career activities and actions
- **Cyber TAC WG action items**
  - Assess the merits and tradeoffs of such an appraoch
  - Identify an architecture or approach to enable automated collection and storage of records
  - Identify technical barriers or problems that would have to be addressed
  - Suggest the types of roles and responsibilities that should be accountable in this manner

Insider Threat – Security Accountability Mechanisms

- **Status**
  - Rough Feasibility and Architecture Assessment Conducted – no 'technical barriers' were identified
  - Issue: Concerns over balancing personal privacy / legality of such an approach. Member companies were not comfortable associating with recommendations.
  - Issue: Many in industry already do this well via personnel vetting, training / certification, internal audits, etc. and do not want practices imposed that could undermine
  - Issue: Concern over imposition of additional regulations and requirements
- **Workplan**
  - The group felt that there were too many non-technical questions/issues that it could not overcome within our charter/representation
  - No further work planned



NOTE: Notional architecture for discussion of feasibility and assessment (not a recommendation)

Security Practices for Core Network Equipment

- **Background**
  - Original question was - can we develop a tiered certification (analogous to UL) for security of core network equipment that could afford a means for equipment procurers to assess and tradeoff cybersecurity capabilities of equipment
- **Status**
  - Discussions in the WG about certification resulted in the scope to develop "Security practices to be designed-in for core network equipment (network backbone, operations & management, cloud / data centers, BGP, DNS, etc.) and tiered compliance checklist"
  - This could be a starting point for eventual tiered certification for vendors, voluntarily progressing at their own pace to attain increasingly higher levels
- **Work Plan**
  - Industry landscape - consult industry / organizations and Inventory current industry efforts (e.g. 3GPP / GSMA, CTIA)
  - Leverage recommendations already developed / progressing in industry consortia and by Service Providers
  - Requirements for the different tiers of compliance checklist
  - If potential gaps are identified, develop recommendations how these gaps can be addressed
  - Target timeline: Recommendations to the December TAC meeting

Mobile Device Consumer Interface for Privacy & Security

- **Background**
  - The Public Safety and Homeland Security Bureau and the Consumer and Government Affairs Bureau are working on a consumer-facing cyber security and privacy project
  - The long-term goal is to enable consumers the ability to configure security/privacy decisions in a simple, consistent manner that automatically triggers the appropriate settings on any platform
  - The FCC is exploring the development of a consumer education app focused on mobile security
- **Cyber TAC WG action items**
  - Enabling the development of a consumer education smartphone app focused on mobile security:
    - The App would present device owners questions regarding their security & privacy
    - The questions would remain constant, but the underpinnings would change as platforms evolve
  - Developing the plan for how platforms and providers would ensure their products and services can interface with the consumers' answers to the questions
  - Ensuring that the existing FCC Smartphone Security Checker is updated from a technical perspective, including developing "plain English" consumer content and a platform for delivery of that content
  - Initial recommendations are being requested for the outset of National Cybersecurity Month (October)

Mobile Device Consumer Interface for Privacy & Security

- **Status**
  - We have begun to educate ourselves on the state of the industry
  - We have learned that are vendors in this space which address various aspects of the request (e.g. Lookout, Quick Heal, Avast, Trend Micro, NQ Mobile)
  - Some WG members feel industry associations (e.g. CTIA) have already addressed this problem space
  - Examples of known CTIA work in this space:
    - Smartphone Anti-Theft Voluntary Commitment (e.g. a free, baseline anti-theft tool)
    - Best Practices and Guidelines for Location Based Services, including privacy considerations
    - CTIA's 11 simple tips using "cybersafety" as an acronym – to help consumers protect themselves
    - Consumer education videos such as password locking of devices and protecting against malware
- **Work Plan**
  - Complete the industry scan and document the findings
  - Seek out participation by key mobile OS vendors (e.g. Microsoft, Google, Apple, BlackBerry Limited)
  - Identify the remaining gaps between the above findings and the initial problem statement
  - Provide actionable recommendations on how to close any remaining gaps toward the goal of enabling the development of a consumer friendly smartphone app

Backup reference slide if desired:

Mobile Device Consumer Interface for Privacy & Security

FCC's current smartphone security checker
http://www.fcc.gov/smartphone-security

- **10 actions for Android, Apple iOS, BlackBerry, and Windows phone users:**
  1. Set PINs and passwords
  2. Do not modify your smartphone's security settings
  3. Backup and secure your data
  4. Only install apps from trusted sources
  5. Understand app permissions before accepting them
  6. Install security apps that enable remote location and wiping
     - For Windows phones, this is called *Set up "Find My Phone"*
  7. Accept updates and patches to your smartphone's software
  8. Be smart on open Wi-Fi networks
  9. Wipe data on your old phone before you donate, resell, or recycle it
  10. Report a stolen smartphone

Summary of Activities for the Remainder of 2014

- Pursue Insider Threat Mitigation Technologies Investigation
  - Output: Recommendations of forward technologies that have promise to help thwart insider threat issues
- Pursue Security Practices for Core Network Equipment
  - Output: Assessment of industry activities and practices , identification of gaps, recommendations to the FCC for addressing gaps in creation of a tiered certification mechanism
- Pursue Mobile Device Interface for Privacy & Security
  - Joint activity with CAC
  - Output: Provide actionable recommendations on how to close any remaining gaps toward the goal of enabling the development of a consumer friendly smartphone configuration interface

Attachment 1

Technology Advisory Council
Cybersecurity Working Group
Insider Threat Risk Reduction Report

25 July 2014

2014 Sub-Team Mission

- **The working group will make recommendations to identify tools and best practices that mitigate the growing risk of insider threats to critical infrastructure owners and operators**
- **The best practices will be identified using the core function taxonomy in the NIST Cybersecurity Framework**

Increased Warning Signs of Growing Concern

- **FBI Theft of Trade Secrets cases are up 39% since 2010**
- **FBI Economic Espionage cases have more than doubled in the last 18 months**
- **50% of employees leaving a company admit to taking proprietary information with them per the FBI**
- ***"Since 2008, our economic espionage arrests have doubled; indictments have increased five-fold; and convictions have risen eight-fold."*** – FBI Executive Assistant Director Richard McFeely, 2013
- ***"Emerging trends indicate that the pace of economic espionage and trade secret theft against U.S. corporations is accelerating. Trade secret theft threatens American businesses, undermines national security, and places the security of the U.S. economy in jeopardy."*** – Administration Strategy on Mitigating the Theft of US Trade Secrets, 2013

Courtesy www.FBI.gov

There is a broad set of Actors who contribute to actions that induce Insider Threats.

The way we use technology to store, process, and move information in ICT systems allows a savvy individual to do more damage than ever before. A first step for any organization is to build an awareness of what the vulnerabilities could be, the subsequent impacts, and the frequency (probability) with which a specific vulnerability pathway will in fact lead to an incident. A number of organizations have developed "Risk Based" approaches for investing in prevention and mitigation of Insider Threats.

Actors	Impacts
State Actors	Destroy Systems and Assets
Organized Cause Groups	Halt Operations
Criminal Enterprises	Impair or Impede Performance
Gangs	Steal Information and Data
Individual Hackers	Create Disruption
Disgruntled Employees	Impact Reputation

Top 4 Reasons Why Insider Threats are more difficult to detect:

- **Growing Volume of Network Activity**
  - **More data being exchanged which means more data transactions to monitor**
- **Growing Use of Outsourcing and Cloud Computing**
  - **Off site / Off-Shore activity and moving data storage / IT responsibilities to lower cost Cloud provider entities**
- **More users have network access – employees, contractors, business partners**
  - **By nature, the Insider Threat is typically from users that have AUTHORIZED ACCESS to the computer system. Tracking 'right' and 'wrong' behavior is much more difficult than tracking/stopping "brute force" attacks**
- **More IT assets on the network**
  - **Makes security more difficult (including Off-Site data; e.g. Cloud) where it is not under the company's direct control. Increase in mobility access & BYOD is also making security & the control of data more difficult**

The Insider Threat

- There is not a single solution for addressing / mitigating the Insider Threat
  - Technology alone may not be the most effective way to prevent and/or detect an incident perpetrated by a trusted insider
- There is an increase in threat potential as aging 'Gen X' transitions to 'Gen Y' workforce with greater knowledge and adoption of "constant connectedness" – including social networking and the belief of "everything should be shared"
- No standard exists on what type of indicators should be watched / monitored when it comes to certain detection of the issue nor a universal language for normalizing information gathered through tracking for exchange

Behavior Monitoring

- Likely the Number 1 thing that can and should be done to help detect and mitigate damage that could be caused by Insider Threat activity
- Identifies indicators of persons at risk and potentially malicious activity by analyzing existing corporate data for behavioral patterns
- Recommendations from Industry show where Behavioral Monitoring Systems that can be customized to monitor not only use of electronic information systems but also behavior throughout an employees tenure at the company can greatly reduce threats against the corporation
  - Periodic / recurring security background checks
  - Periodic criminal and financial checks
  - Ability to input world events to detect possible malicious activities by foreign-nationals
  - Other Primary Risk Indicators that track abnormal behavior & 'motivation' for potential threats at the INDIVIDUAL level

Behavior Monitoring - continued

- **Keys to a successful program:**
- **Approval from the C-Suite of the Program – everyone will be watched!**
- **Alignment of Human Resources & Regulatory departments to ensure no violation of privacy / human rights**
- **Transparency to the Workforce**
  - **Communicate what's being watched and why**
  - **Define & Communicate Policy, Awareness, and Consequences**
- **Create a culture of employee engagement**
  - **Not a culture of "snitches"**
  - **Program adoption and understanding that security is everyone's job**
- **Tools available – such as Wisdom from Lockheed Martin – are available for monitoring but *do need to be customized* to fit each company's specific requirements**

Tools to Aid in Protection Against the Insider Threat

- **Following NIST Cybersecurity Framework taxonomy…**
- **Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, & capabilities**
  - **Governance / Policy / Risk Mgmt: Archer, CA, MetricsStream, SAP, Protiviti**
  - **Data Classification: Varonis, Titus, Symantec**
  - **Risk Assessment: Nessus, Core Impact, Nexpose, Qualys**
  - **Governance: Agiliance, Modulo, RSA Archer, Symantec, MetricStream**

Area	Function	Technology Building Blocks
Asset Management	Understand and track assets	Inventory management
Governance	Policy and Guidance	GRC tools to synchronize governance, risk and compliance.
Risk Assessment	Identify Asset Vulnerability	Vulnerability tools to understand known exposures.

- **Protect – Develop & implement the appropriate safeguards to endure delivery of critical infrastructure services**
  - **Data Loss Prevention (DLP) At Rest & In Motion: McAfee, RSA, Verdasys, Symantec, CA, WebSense**
  - **Encryption: Symantec, FireEye, Cypherix**
  - **Mobile Device Management (MDM): MobileIron, Good, Zscaler, Citrix**

Area	Function	Technology Building Blocks
Access Control – Personnel	Identify and Authorize	Multifactor Identity Systems, Biometrics, etc
Access Control – Devices	Identify, Authorize, and Scan	Software coverage tools, packet inspection, etc
Resource and system protection	Limit access resources and limit impacts	Trusted Computing
Data and Information protection	Encryption	Encryption methods, Key distribution

- **Detect (Anomaly Based) – Develop & implement the appropriate activities to identify the occurrence of a cybersecurity event**
  - **Network: Arbor, Lancope, Radware, Palo Alto, WebSense**
  - **Security Intelligence with Matrixed Log Correlation: Splunk, LogRhythm**
  - **Endpoint: Encase, Mandiant**
  - **Application Behavior: Vericept, Digital Reasoning**

Area	Function	Technology Building Blocks
Data Collection and Monitoring	Log files, access data, personnel files, social data, web data, intelligence, etc	Distributed file systems, crawlers, etc
Data Mash-up or Data Fusion	Merging the information and base-lining risk parameters	Accessing and querying heterogeneous and unstructured data
Analytics	Detection of probable threats	Algorithms for detection– adaptive thresholds, cumulative sums, projection, change point identification. Social Network analysis - behavior characterization
Visualization	Reporting and display of information	Multidimensional data, social network and associativity graphs

- **Respond – Develop & implement the appropriate activities to take action regarding a detected cybersecurity event**

Area	Function	Technology Building Blocks
Detect	Identify unauthorized use or unauthorized changes to system parameters	Collection and base-lining of system behavior. Categorization of system states Anomaly Detection
Secure System	Cut-off unauthorized access and attack vectors and prevent additional damage	Traffic diversion.
Find Root Cause	Understand method of unauthorized attack	Real time analysis techniques with machine learning and other AI methods
Mitigate	Prevent future attack and reinitiate system	Access control, traffic diversion, intense data monitoring, honeypots, etc

Best Practices for Insider Threat Mitigation

Consider threats from insiders and business partners in enterprise-wide risk assessments.	Institutionalize system change controls.
Clearly document and consistently enforce policies and controls	Use a log correlation engine or security information and even management (SIEM) system to log, monitor and audit employee actions.
Incorporate insider threat awareness into periodic security training for all employees.	Monitor and control remote access from all end points, including mobile devices.
Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	Develop a comprehensive employee termination procedure.
Anticipate and manage negative issues in the work environment.	Implement secure backup and recovery processes.
Know your assets.	Develop a formalized insider threat program.
Implement strict password and account management policies and practices.	Establish a baseline of normal network device behavior.
Enforce separation of duties and least privilege.	Be especially vigilant regarding social media.
Devine explicit security agreements for any cloud services, especially access to restrictions and monitoring capabilities.	Close the doors to unauthorized data exfiltration.
Institute stringent access controls and monitoring policies on privileged users.	

SCOPE

- The Insider Threat is a rapidly growing area of risk for both the US Government as well as Industry as it is primarily linked to human behavior – never constant / always changing
- Fear by owners/operators that “sharing of incidents & issues” regarding breaches will have negative impacts on their company regardless of positive impacts from other industry learnings thus inhibiting wide adoption or practice
- High degree of difficulty in developing proactive tools within the industry as the human behavior, mobility & BYOD options, supply chain, and outsourcing possibilities continue to grow in size and scope
- Our work focused only on the technology issues – not policy issues surrounding privacy & other legal / regulatory concerns

TAC Recommendations for the FCC

- **Endorse & promote internal processes including background checks, and use of internal & Commercial Offerings (see Appendix slides) to identify & protect against Insider Threats**
- **The FCC should promote the use of information technologies such as STIX and TAXII as communication frameworks for sharing threat information between willing parties**
- **Encourage the sharing of threat information via DHS at the NCCIC. Facilitate legislation is in place that would help increase the sharing of threat information. Continued use of the CSRIC WG for sharing information on learnings and best practices**
- **Potentially align with CSRIC WG4 to determine if the tools listed within this deliverable aid in their efforts around further adaptation and adoption of technology in the NIST CyberSecurity Framework**

APPENDIX

Commercial offerings for Insider Threat: a very crowded and competitive marketplace

AlureSecurity	HP	CTC
Lancope	CyberArk	Verdasys
Palantir	Mtsi-VA	T-Sciences
Splunk	GuardTime	Deloitte
AdvatageSCI	SpiceWorks	Logos-Technologies
Cataphora	Tape-LLC	Wave
Cisco	GTBTechnologies	Aveksa

Commercial offerings for Insider Threat: a very crowded and competitive marketplace

ACRG-LLC	TSCAdvantage	Proficio
Vormetric	LogRythm	ESG-Global
CentraTechnologies	ManageEngine	Mandiant
McAfee	Reliaquest	Encase
CA	InsiderSpyder	Vericept
KinneyGroup	Tenable	Symantec
Securonix	Pol-Psych	Archer

Research and Operations Organizations Concentrating on various aspects of the Insider Threat

www.rand.org	www.cryptome.org	www.sans.org
www.parc.com	www.thei3p.org	www.gtri.gatech.edu
www.nsi.org	www.csrc.nist.gov	www.mitre.org
www.innovateuk.org	www.cert.org/insider-threat	www.globalecco.org

List of References for the Insider Threat Sub-Team:

- **Douglas D. Thomas: Director, Counterintelligence Operations & Corporate Investigations, Lockheed Martin Corp; 6 June 2014**
- **Randall Trzeciak: Director, CERT Insider Threat Center, Carnegie Mellon University; 27 June 2014**
- **National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat , U.S. Dept of Homeland Security; December 2013**
- **http://enterprise-encryption.vormetric.com/rs/vormetric/images/Global-Insider-Threat-WEB.pdf**

Attachment 2

Technology Advisory Council
Cybersecurity Working Group
Processes and Functions Report

25 July 2014

Sub Team Scope

Cybersecurity is increasingly becoming something that needs to be discussed in the Executive Suite. As such senior management should consider the processes and functions needed to maintain a Cybersecurity Program within an enterprise. These processes and functions should address the needs of the specific environment that the enterprise operates in and the risks that enterprise faces in running the nations critical infrastructure. Management needs to understand that an effective Cybersecurity program is more than just deploying technology, you have to have the right process, functions and the right people.

The Sub Team will identify those processes and functions that should be part of an Cybersecurity program for enterprises.

Sub Group Members

- Renato Delatorre, Verizon Wireless
- Martin Dolly, AT&T
- George Popovich, Motorola Solutions
- S Rao Vasireddy, Alcatel Lucent
- Ramani Pandurangan, XO Communications

Process and Functions

- Defining a Cybersecurity Program
  - Identify internal stakeholders – Who will operationalize the cyber program
  - Establish communication channels
  - Training
  - Detection and Mitigation Tools needed
  - Identify/Detect Threat/Attack
  - Develop mitigation strategies
  - Post Threat/Attack Analysis
  - Create a feedback loop into the process to continually improve the overall program
- Reference previous CSRIC and industry best practices as a starting point

Elements of a Security Program

- Risk Management that is integrated into the enterprise Service Delivery Lifecycle (SDLC)
  - Internal and External Reviews and Audits
  - Security interdependencies of process, functions and people should be a part of the risk management. Best practices, standards and multiple sources of data from SDLC should be comprehensively analyzed for an effective risk management strategy.
- Security Monitoring and Response
  - Event aggregation and correlation
  - Intrusion Detection Systems /Intrusion Prevention Systems
  - Security Incident Reporting and Incident Management
  - Yearly tabletop exercises
- Business Continuity Planning, Network Disaster Recovery & Crisis Management
- Compliance with Standards and Regulations
- Change Management
  - Ensure changes are documented and consistent with expected results
- Personnel Security
- Security Awareness and Education for employees
- Security Training and Certifications for security practitioners
- Security Compliance Reviews
- Security Advisory Program
- Privacy Committee
  - Privacy Compliance

Elements of a Security Program

- Security Executive Briefings and Roundtables
- Strategy for continuous Improvement
- Access Controls
  - Physical Access Control
  - Logical Access Control Measures
    - Multi-factor Authentication
  - Network Element Access Controls
  - Access Authorization Control
  - Single digital identity
- Network Perimeter Protection
  - Firewalls
  - Edge Routers
  - Boarder Routers
- Public-facing Website Protection
  - DNS protection/Secure DNS
  - DDoS Mitigation
  - DMZ
  - Host based IDS and checksum validation
- Workstation Security Management
  - Antivirus and endpoint security
- Security Status Checking and Vulnerability Management
  - Vulnerability Testing and Security Analysis
  - Security Status Reporting

TAC Recommendations for the FCC

- Endorse the concept that for an effective Cybersecurity program there needs to be focus on the process, functions and the need for Executive attention through CISRC and the NIST Cybersecurity Framework adoption

Technological Advisory Council

Supporting the Transition to IP

Working Group

23 September 2014

Working Group Members

- Mark Bregman and Tom McGarry (Neustar)
- Theresa Hennesy (Comcast)
- Kevin Kahn (Intel)
- Fred Kemmerer & John Barnhill (Genband)
- Steve Lanning (Viasat)
- Marvin Sirbu (SGE)
- Doug Jones & Tim Dwight (VZ)
- Kevin Sparks (ALU)
- Russ Gyurek (Cisco)
- Dale Hatfield (UCol)
- Harold Teets & Mike McNamara (TW Telecom)
- Lynn Merrill (NTCA & Monte R. Lee)
- Peter Bloom (General Atlantic)
- Dick Green (Liberty)
- Jack Nasielski (Qualcomm)
- Nomi Bergman, John Dickinson (Bright House)

Special thanks to the FCC members: Walter Johnston, Henning Schulzrinne, Kalpak Gude and William Layton for their contributions.

Today's Discussion

- Refresher: Review our original mission
- Share our approach: Survey; Architecture; Study Corner Cases; Identify opportunities
- Update on where we are:
  - Findings from surveys, what's left to complete
  - Early insights from Architecture work
  - Incorporate findings from prior TAC Working Groups (e.g., PSTN Transition, Resiliency) and organizations like ATIS
  - Further work on corner cases
- **Receive feedback from the rest of the TAC**

Review our Original Mission

- Examine opportunities for new communication technologies to better serve the needs of people with disabilities
- Identify potential opportunities for improvements in emergency alerting and information support during disasters enabled by an IP infrastructure and associated technology
- Identify opportunities for experiments or R&D that would support the understanding of the impact of tech transitions on the enduring values
- Analyze potential for new fiber technologies and wireless systems to better serve low population areas ensuring that rural communities are connected to the evolving broadband environment
- Identify opportunities and objectives for trials designed to support advanced communication capabilities to rural areas
- Support activities focused on improving acquisition of information on deployment of broadband technologies

Survey Work: Overall Approach

Summary of Past Surveys

- Small Rural Operator: Common Themes

Further Survey Work

- Midsize Rural Providers: Differ from Small Providers
- Satellite Providers: Common Themes
- Broadband Equipment Manufacturers: Common Themes

Next steps

- Further interviews to complement review of corner cases and to support reference architecture work

Small Rural Operator Survey: Common Themes

- Employees live in areas they serve and react quickly to customer needs and responses
- Middle-mile solutions represent a greater bottle-neck to providing broadband access services than last mile solutions
  - Installed larger fiber networks or joined a consortium to form statewide networks
  - Built redundant connection points over several years, for reliability
  - Due to long distances to internet gateways, companies use regional solutions to provide hosting and transit to mitigate high middle-mile transition costs.
- Varying stages of VoIP deployed.
- Aggressively adopted new and hybrid solutions which solved geographical challenges and fit investment profiles.
  - Deployment of FTTH in new build situations
  - Extended copper life by reaching customers with VDSL
  - Creative deployment of wireless solutions (LTE or WiMAX)

Further Survey Work

Midsize Rural Providers: Differ from Small Providers

- Provide service to rural geographical areas using a Central Design, Budget and Construction to ensure broadband investments are maximized
- Currently 11% FTTH with 4% added per year (Long-term to transition)
- Hard-to-Reach-Customers are covered by Resale of Satellite Data Service
- Softswitches are being used to serve both TDM and IP access
- Construction Techniques: Uses Sewer Lines for RR Crossings

Satellite Providers: Common Themes

- More Satellites are being launched to improve performance in all areas
- Expect up to 50Mbps in the future with newer satellites
- Mountainous areas have line of site issues
- Satellite has more subscribers closer to the cities that in the very rural areas.
- Majority of Capital not spent until customer signs up
- Dynamic Beam adjustment in future to reach areas of high demand

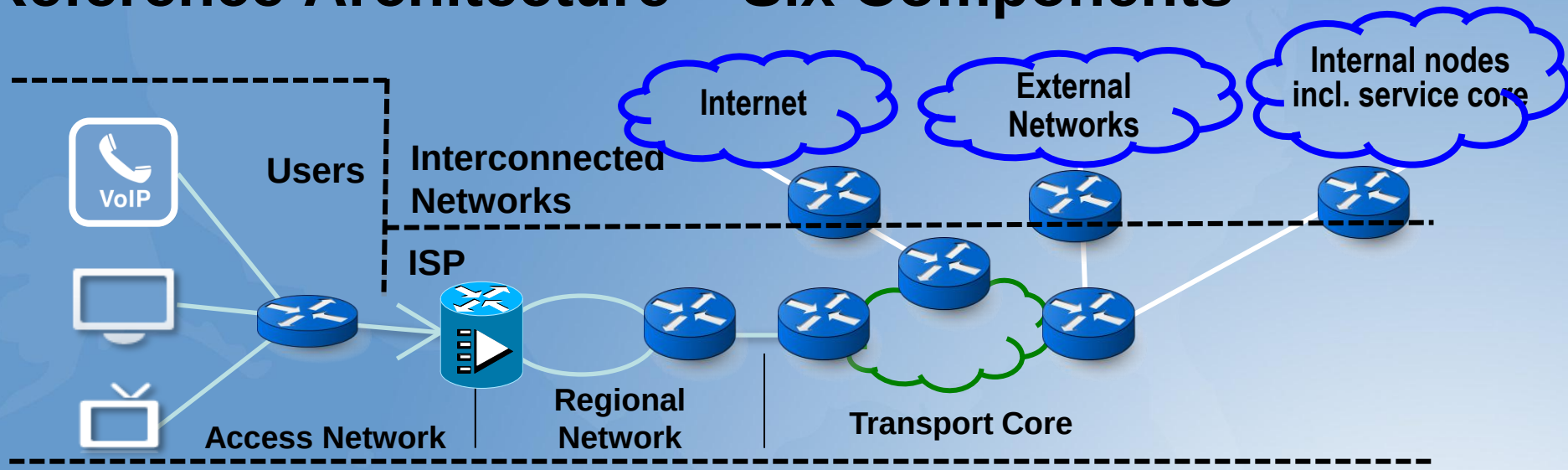
Broadband Eqpt Manufacturers: Common Themes

- Interviewed manufacturers of broadband and transport equipment, providing platforms serving large, medium and small providers in rural areas which handle PSTN voice, VoIP and Broadband services
- High degree of aggressiveness by the small provider makes for a suitable test bed for the manufacturers' products. Manufacturers attribute this to:
  - Small providers having local ties to the community
  - Small providers have small technical staff allowing for easy communication and quick responses to needed network changes
  - Small providers access to USF
  - Small providers can build with longer payouts when working with local economic development groups
- Larger Providers Implementation advantage:
  - Bulk Volume Purchase
  - Late adopter of products removes initial kinks, cuts cost for Lab Testing, Equipment and the provider receives historical benefits of customer usage of product

Reference Architecture Plan

- Develop a reference architecture to frame how we see the evolution of broadband access and backbone network technology solutions.
- Our specific mission: To describe existing architectures for the broadband network that provides users access to Internet and communication services. We hope to use this framework to share a technical view as to how solutions are evolving, and the opportunities and challenges they present.
- Marvin Sirbu is leading the access piece; Tom McGarry the backbone piece.
- Today, we will review technologies that provide broadband IP access:
  - Access network
  - In-home network
  - Physical characteristics
  - Logical characteristics

Reference Architecture – Six Components



- Access network – connects the user to the regional network
- Regional network – connects the access network to the transport core
- Transport core – connects the regional network to the Internet, the service core and other internal and external networks
- Internet – connections to other ISPs enabling users to access Internet services
- External networks – communications and video networks
- Internal nodes – other nodes within the network including the service core which enables communications and/or linear video service

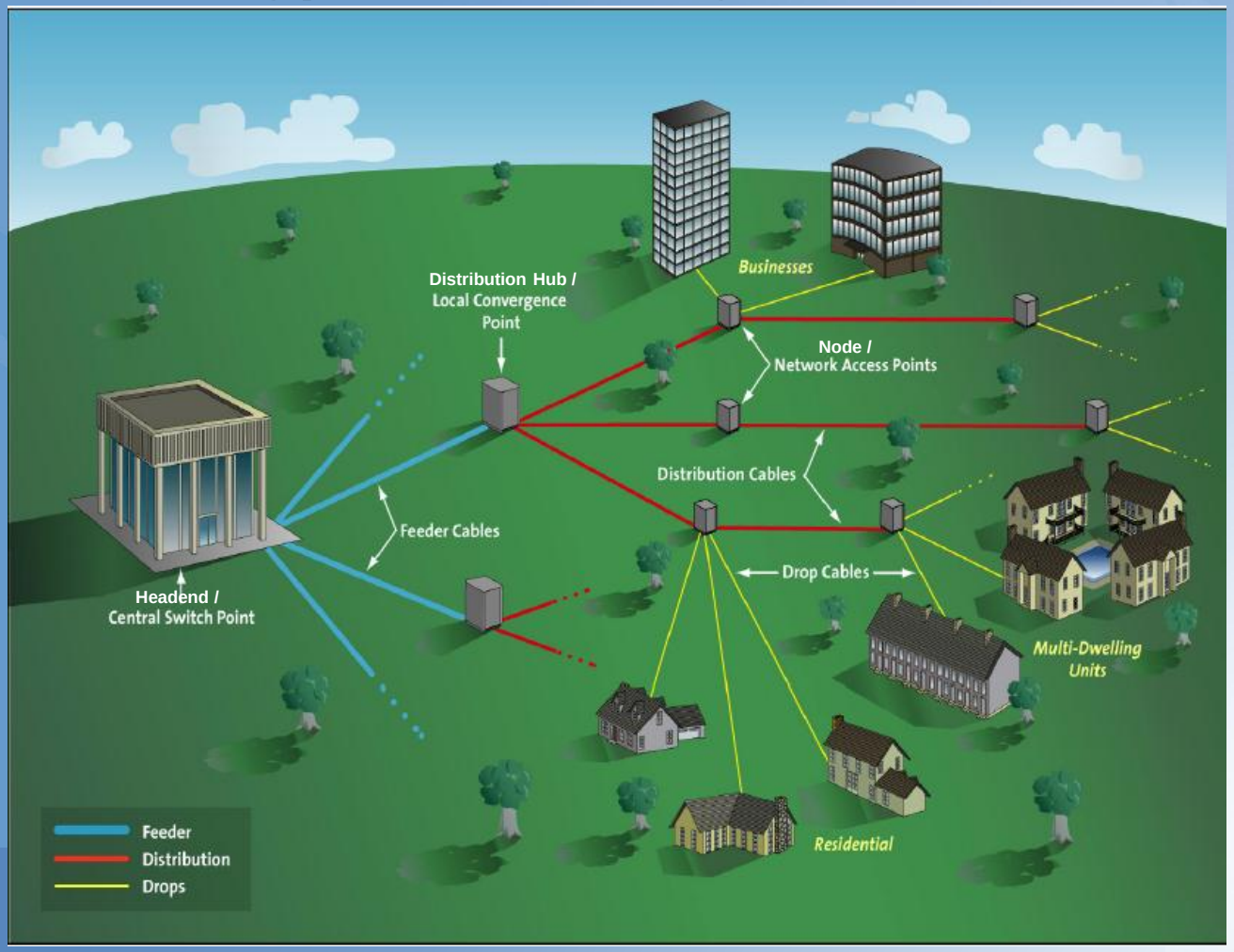
Technologies Described

- **Access Network**
  - Digital Subscriber Line(DSL) and hybrid Fiber/xDSL technologies (xDSL)
  - Fiber to the Premises (FTTP/FTTH)
  - Hybrid Fiber Coax (HFC)
  - LTE
  - Other wireless: WiFi, WiMAX
  - Satellite
- **In-Home Network**
  - WiFi
  - Multimedia over Cable Alliance (MoCA 2.0)
  - Power Line Networking: HomePlug AV, IEEE Std 1901-2010
  - Structured cabling (e.g. Ethernet)
  - Phone wiring: HomePNA ITU G.hn standard

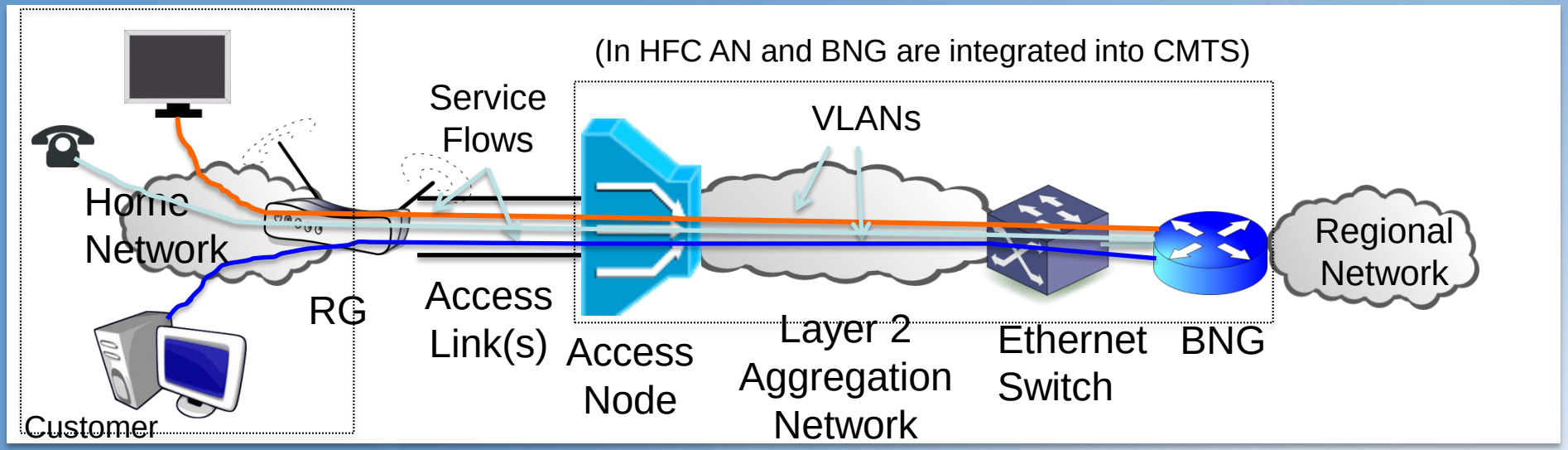
Physical versus Logical Architecture

- **Physical layer features include:**
  - Links (copper, fiber, coax, wireless), nodes (cross connect, splitter, DSLAM), layout, physical-layer features
- **Logical (layer 2)**
  - Each access architecture provides a means of separating traffic into distinct “flows” that can be given separate QoS treatment
  - In the extended materials, we describe how each architecture accomplishes this separation of traffic
- **Boundary of layer 2 network**:
  - Location of first layer 3 router
  - Divides access network from regional network

Elements in a Typical Wired Physical Architecture



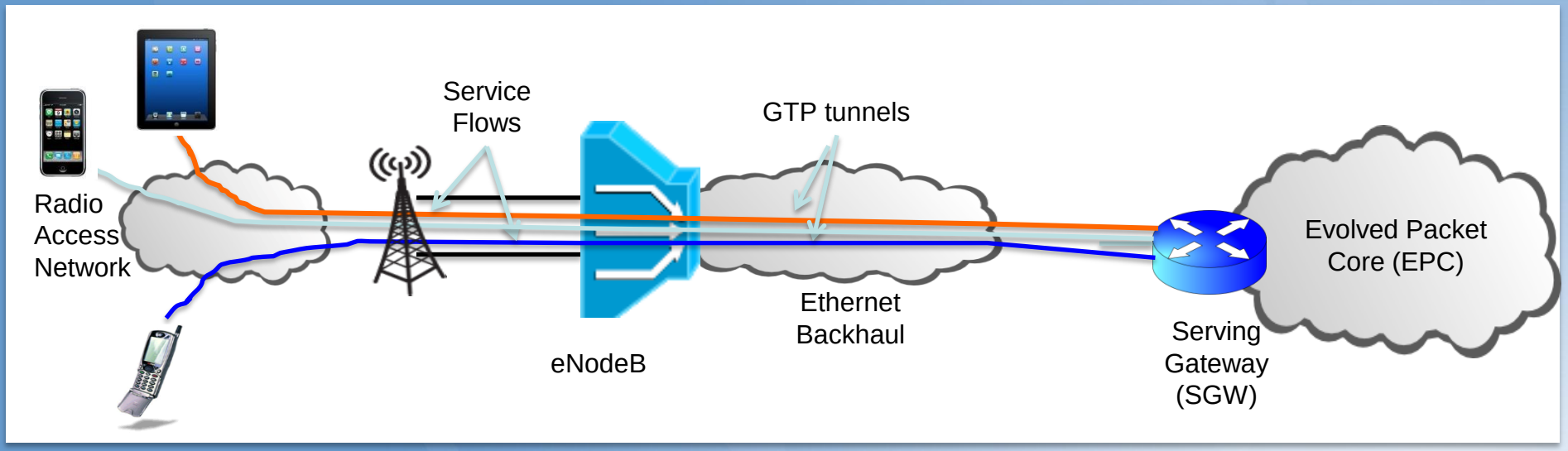
Logical Architecture – wired networks



- Access network extends from Residential GW (RG) to Broadband Network GW (BNG)
- Flow management between Access Node (AN) and RG depends upon the architecture
- Flow management in the Ethernet Aggregation Network similar across architectures (*i.e.* VLANs) but may differ from how flows are managed between the AN and the RG
  - In HFC AN and BNG are integrated. No aggregation network and thus no VLANs
- In Regional/Backbone Network flows are typically distinguished by layer 3 QoS tags and/or separate VPNs

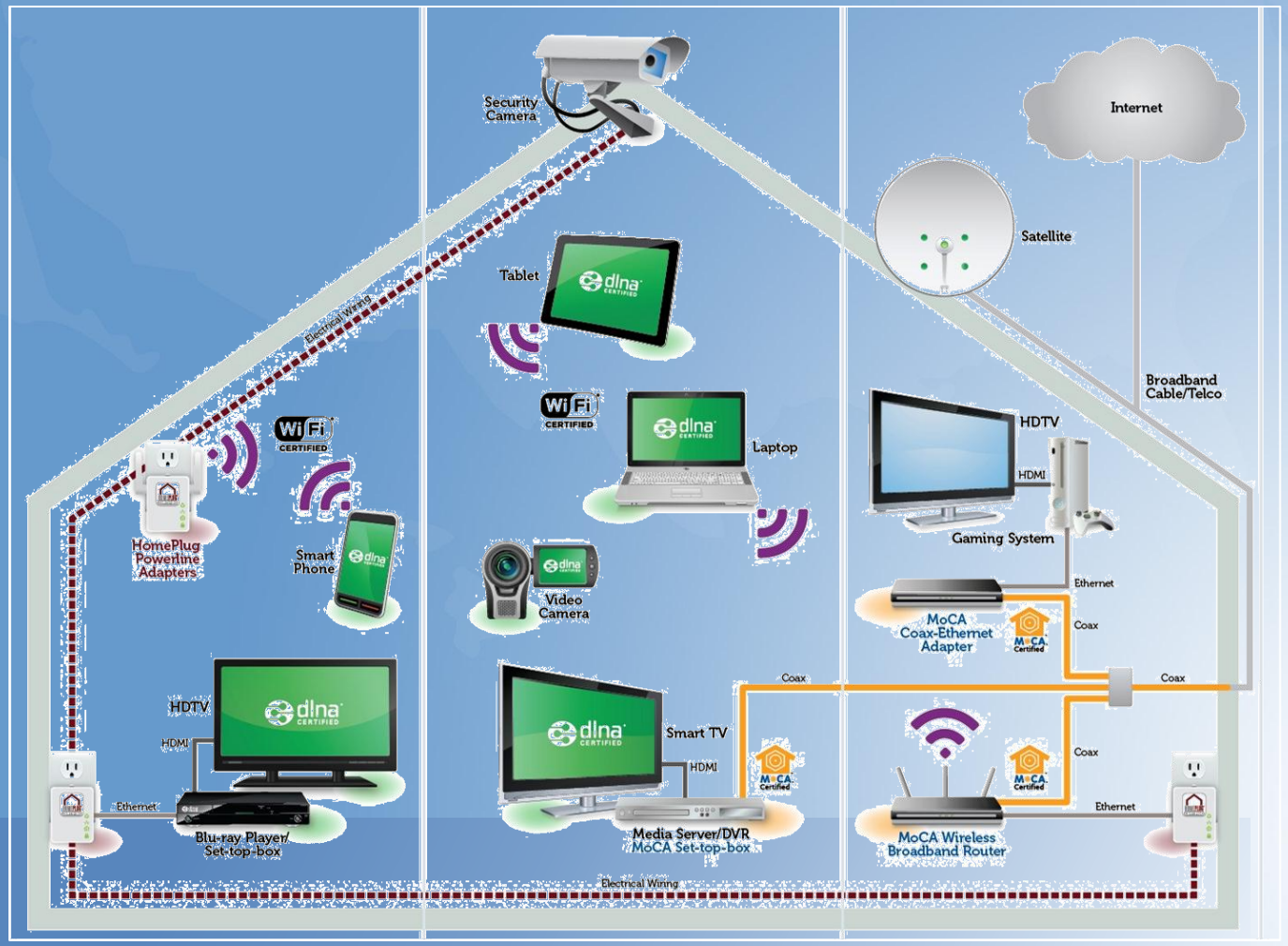
Adapted from http://www.broadband-forum.org/technical/download/TR-101_Issue-2.pdf

Logical Architecture: Mobile Wireless LTE Network



- Typically no residential gateway: transmission direct to end nodes
  - RG may be used with Fixed Wireless service
- GTP: General Packet Radio Service—GPRS—Tunneling Protocol
- Service flows are referred to as “bearers”

In-home broadband networks



Insights from Access Network Review

- IP broadband is a platform that supports both Internet access and specialized IP-based services (e.g. VoIP, video delivery)
  - These multiple logical networks differ with respect to:
    - QoS
    - Interconnection
    - Services available
  - Logical networks may be separated by:
    - Assignment to separate physical channels (e.g. separate wavelengths); or
    - A guaranteed share of link resources; or
    - Different priority levels
- Any of the access technologies can easily handle VoIP bitrates
  - Conversational video requires more
- OTT (nomadic) VoIP may behave differently than dedicated (fixed) VoIP
  - Do consumers need to be educated about these differences in order to understand how behaviors may differ?
    - *E.g.* location determination for E911 may be different for OTT and dedicated VoIP

Insights from Home Networking review

- Wired VoIP to the home today terminates at a Media Terminal Adaptor (MTA)
  - Most handsets are still analog (or cordless)
  - Limits the provision of ancillary IP-based services (e.g. SMS to the handset, HD voice, conversational video)
- Wired VoIP to the handset will change user expectations about phone behavior
  - The role of dialtone as an indicator of network operational status
  - Picking up an extension to join a call
  - Slow rate of evolution of the PSTN and fewer (and more accomodating) end office switch vendors allowed for well standardized interfaces between CPE and the network, and simpler integration testing. (e.g. Fax machines to CO line cards)
  - Greater variation in VoIP (codecs, MTAs) means greater likelihood of mismatch
    - E.g. Conventional fax doesn't work over compressed bitrate VoIP codecs.
- Residences shifting to mobile for voice service
  - Mobile supporting VoLTE or VoWiFi may become most common VoIP handset
- Phone numbers may no longer map 1:1 with the home (wired) or a device (mobile)
  - "follow-me" calling
  - Implications for number allocation

Issues for further study: Observed Transition Issues

- Critical Government Infrastructures are dependent on TDM. Dependencies and transition plans need to be identified across Federal and State Governments
  - The FAA National Airspace System is one example, which has some 22,000 TDM locations.
- Funding for replacing obsoleted devices is an issue. And manufacturers are discontinuing TDM equipment.
- Services are not being modernized as they become obsolete, or experience rapidly dwindling usage:
  - Technical solutions to migrate or replace exist, but performance and device spec compliance vary widely, extensive troubleshooting required
  - Some operator services solutions, party lines, etc.
  - Alarm industry may require battery monitoring
  - Elevators require analog line off IP system. If MTA required, deployment cost dwarfs hardware cost.
  - Spec exists for MTAs (TIA TR41.3) but no certification exists.

Next Steps for TAC 2014 Work

- Refine and publish high level reference architecture for the December meeting.
- Finish surveys: Interview Middle-Mile providers and fold in results to the Access and Backbone sub working groups. Will conduct follow up interviews as needed to complement WG's directive.
- Finish work to review and consider "corner cases" in aggregate.