Technology Advisory Council
Wireless Security & Privacy WG

Report to the TAC

Sept. 24, 2012

Charter & Members

- **Examine** security and privacy vulnerabilities of air interfaces used by commercial wireless networks, as well as the broader wireless ecosystem, **assess** how they are currently being addressed, and **recommend** what role, if any, the FCC should play
- Includes cellular and Wi-Fi wireless networks
  - Cellular and Wi-Fi
  - Networks and devices
  - Technical and operational/usage aspects
  - End user and network impacts

TAC Members

- Brian Daly – AT&T
- Kevin Kahn – Intel
- Randy Nicklas – XO Communications
- Dan Reed – Microsoft (formerly)*
- Kevin Sparks – Alcatel-Lucent (chair)
- Paul Steinberg – Motorola Solutions

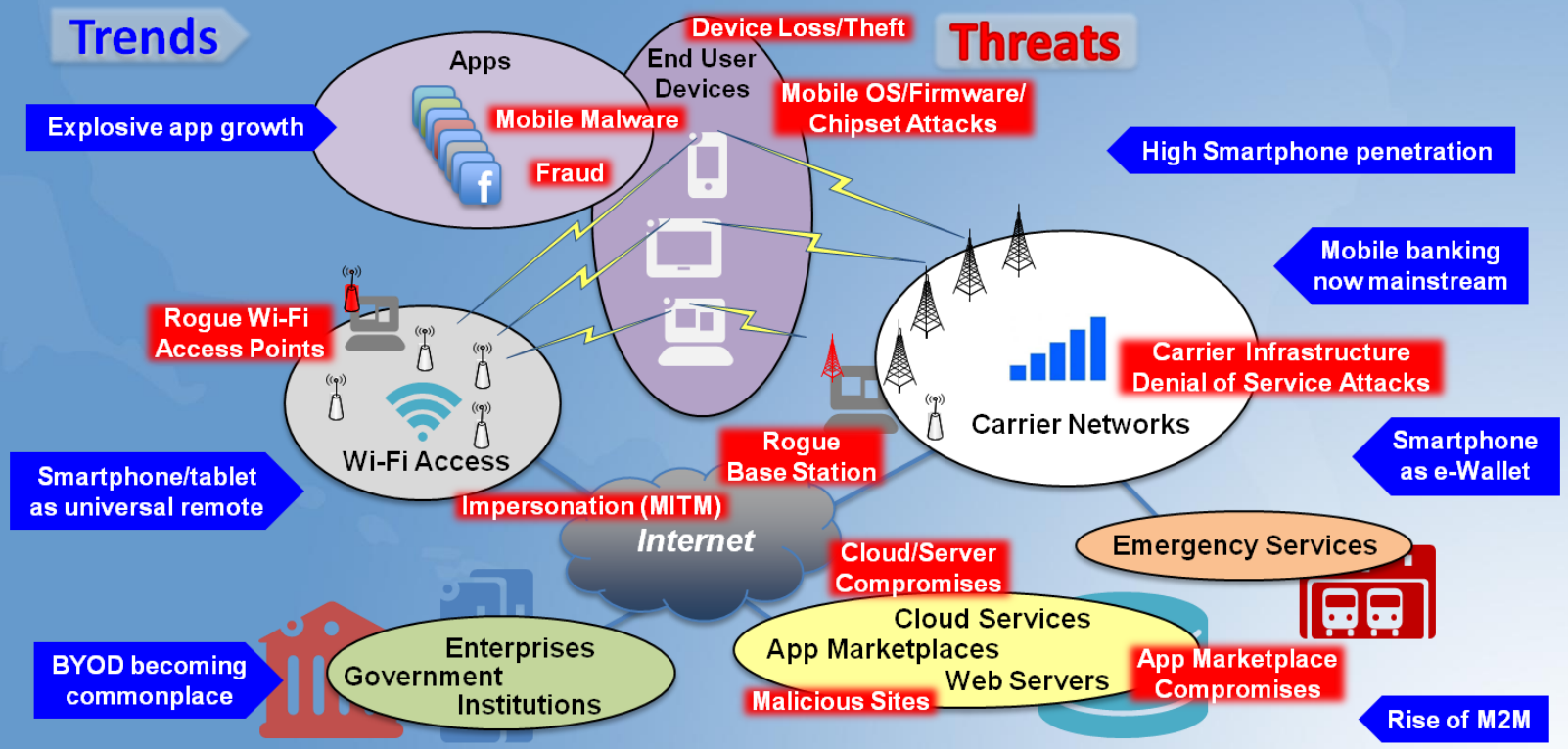
- FCC Liaison – Greg Intoccia, Ahmed Lahjouji

Additional WG members

- Bill Boni – T-Mobile USA
- Martin Dolly – AT&T
- Matthew Gast – Aerohive Networks
- Ali Khayrallah – Ericsson
- Simon Mizikovsky – Alcatel-Lucent

* no longer representing Microsoft

Mobile Security Landscape



Addressing the most critical mobile security/privacy threats requires a broad view of the complex mobile environment

Mobile Ecosystem Spans Distinct Cultures

Consumer Hardware/ Software Community
Highly diverse; Rapid cycles of innovation/iteration/obsolescence

Network Infrastructure Community
Large investments; Longer, more stable planning cycles & lifecycles; Aware of threats

Consumers
Limited view of risk, or patience with security annoyances; Drawn to convenience and "free"

Institutions, Government, Large Corporations
Typically aware of threats; Control own perimeters; Restrict employee use/access

Multi-faceted ecosystem, interplay across diverse communities increases and complicates mitigating security/privacy issues

Upfront Guiding Observations

- The threats are real, and they are growing very rapidly
- There are many strong efforts in many places to improve mobile security, but the diverse and distributed nature of the mobile ecosystem results in a fragmented, uneven, and vulnerable security and privacy environment
- There are no “silver bullet” solutions – mobile security requires a multi-faceted approach, multi-layered defenses, and continual improvement
- For successful adoption, solutions must take the culture/psychology of each community into account
- Collaborative, voluntary approaches are key to sustain the industry’s agility to respond to threats and innovate solutions quickly

Cellular Networks - End User Security/Privacy

Key Threats to End User Security

- **2G GSM weak authentication and widely broken encryption**
  - Readily available equipment to intercept, or create fake base station
  - Insecure network operating practices (e.g. reuse of authentication vectors)
  - 3G/4G → 2G bid-down attacks
  - 2G exposure diminishing, but remains for international and rural roaming
  - 2G also still widely used for M2M
- **Unprotected SMS**
  - Malicious emergency messaging
  - Mobile commerce fraud, potential barrier to market development
  - Despite alternatives, SMS remains popular due to ubiquity

Mitigation Approaches

- Too late in lifecycle to fully secure 2G GSM infrastructure and existing devices
- Better tools to manage/restrict 2G usage
- Educate end users on risks of 2G GSM roaming and SMS for sensitive information
- Network policy controls to restrict nefarious use of M2M subscriptions
- M2M ecosystem alignment on faster 2G to 3G/4G migration roadmap
- Application level authentication, integrity protection, and encryption for sensitive information (layered defense)

Recommendations - Cellular Security/Privacy

Seek collaborative ways to partner with industry and industry groups to limit exposure of **older less secure cellular technologies**

Recommended focus issues:

- End user education on security risks of 2G GSM usage (especially international roaming), and ways to reduce exposure
- Simple controls on smart mobile devices that allow users to enable/disable 2G GSM usage
- End user education on risks of unprotected SMS for transmission of sensitive information
- Roadmap for timely migration of M2M from 2G to 3G/4G, for security, address space (IPv6), and spectrum efficiency benefits

** WG still assessing priority items for practicality and partnership potential*

Preliminary*

Cellular Networks - Network Integrity

Key Threats to Network Integrity

- **Mobile Malware Denial of Service (DoS) Attacks**
  - Malware growing rapidly - in both instances and sophistication
  - Botnets can quickly and far-too-easily infect large numbers of mobile devices
  - Targets: critical/emergency services, any 3rd party, and/or the network itself
  - Volume SMS/data/voice attacks can overwhelm both systems and staff
  - Detection of malware is difficult; time to react is short once an attack begins
  - Insecure M2M endpoints can also be exploited for volume attacks

Mitigation Approaches

- Network-based and device-based malware detection and isolation
- Device management, including controlled remote wipe
- App Store application removal process
- Application certification (whitelisting)
- Server host based security filtering
- Mobile *ecosystem* alignment on mobile malware security best practices
  - Threats, tools, operating procedures
  - Joint policy/procedure for handling malware outbreaks
  - Frequent interaction and timely updates
- User education on malware risks, safeguards, tools
  - Point of sale, ongoing

Recommendations - Network Integrity

Seek collaborative ways to partner with industry and industry groups to reduce **malware attacks threats** against networks and vital services

Recommended focus issues:

- Voluntary sharing of security best practices among carriers on network and device-based malware detection & isolation
- Timely and effective communication of malware outbreaks among network operators
- App store support of application removal request process, accessible by network operators and other detection organizations

Other malware-related priority issues covered under "Devices & Apps" section

** WG still assessing priority items for practicality and partnership potential*

Preliminary*

Wi-Fi Access Security

Key Threats to End User Security

- **Widely varying levels of security**
  - Weak/no authentication & encryption common, even in managed hotspots
- **Tools for bad actors readily available**
  - Automated sniffing, session hijacking
  - "Evil twin" masquerading hotspots
- **Large magnitude of exposure**
  - Wi-Fi used widely to supplement licensed spectrum for localized capacity
  - Many large-flow apps require Wi-Fi
  - Usage-based cellular data plans encourage greater Wi-Fi use
- **Consumers especially vulnerable**
  - Risk awareness low, loses out to "instant gratification"
  - Minimal consumer VPN adoption

Mitigation Approaches

- Ecosystem alignment & adoption of strong Wi-Fi security best practices
  - Tiered (consumer/enterprise/govt. users) for acceptable levels of complexity and cost
  - Build on existing industry initiatives (Wi-Fi Alliance Passpoint, Protected Mgmt Frames)
  - Drive closure & adoption of Wi-Fi + cellular integrated security & roaming (WBA, 3GPP)
  - Seek ways to leverage managed Wi-Fi solutions for securing ad-hoc hotspots
- User education on "safe Wi-Fi"
  - Caution on usage of untrusted Wi-Fi
  - Awareness of secure Wi-Fi roaming indicator, and adapters for older equipment
  - Awareness of available VPN solutions
- Encourage defense in depth
  - Security software, VPN/Firewalls
  - Application level security

Recommendations – Wi-Fi Access Security

Seek collaborative ways to partner with industry and industry groups to reduce exposure from **unsecured Wi-Fi access**

Recommended focus issues:

- Greater use of mutual authentication and encryption for Wi-Fi
- Consider "secure Wi-Fi" branding to improve end user awareness, incent ecosystem
- Build upon existing industry secure Wi-Fi and Wi-Fi secure roaming initiatives (e.g. Wi-Fi Alliance Certified Passpoint, WBA, 3GPP)
- Educate end users on risks of unsecured Wi-Fi risks, and safeguards

** WG still assessing priority items for practicality and partnership potential*

Preliminary*

Mobile Devices & Apps

Key Threats to End User Security

- **Devices - huge targets of opportunity**
  - Hold a wealth of personal/private info
  - More exposure/vulnerabilities than PCs
  - Variety of under-protected ports (Bluetooth, USB, Wi-Fi, NFC)
  - Easily lost/stolen, often w/o passwords
- **Fertile malware environment**
  - Vast numbers of apps and developers
  - Evil clones of apps produced in volume
  - Varying levels of mobile OS API and permissions controls
  - Jail-breaking circumvents API controls
- **BYOD - mixing consumer & enterprise**
  - Mixed use devices open more attack paths, complicates security

Mitigation Approaches

- Ecosystem alignment & adoption of strong device/apps security best practices
  - Tiered (consumer/enterprise/govt) for acceptable levels of complexity and cost
  - Building upon existing industry initiatives
  - Secure mobile OS API controls
  - Enhanced app permissions models (visibility, granularity, automation)
  - App marketplace malware screening
  - App certification (whitelisting)
- User security awareness education
  - Maximize point of sale & online contacts to educate consumers on security basics, tools
  - Public service awareness campaigns
- Encourage mobile OS security market
  - Security software (local firewall, IDS)
  - Application level security

Recommendations - Mobile Devices & Apps

Seek collaborative ways to partner with industry and industry groups to limit end users' exposure to **mobile malware** and **device theft/loss**

Recommended focus issues:

- Effective techniques and business models for app certification (whitelisting) and malware screening
- More effective app permissions models (better visibility, granularity, and policy automation)
- Secure mobile OS API controls (restrict app usage of system APIs)
- Build upon existing government and industry initiatives (e.g. NIST, TCG)
- Leverage service/device/app touch points to educate end users on malware and loss/theft risks, safeguards, & tools

** WG still assessing priority items for practicality and partnership potential*

Preliminary*

Next Steps

Further consulting and assessment

- TAC feedback, consultations with other potential partnering industry groups
- Firm up views on which priority issues are practical to address through collaborative partnering, and ways they could be approached
- Further refinement of mitigation methods for corresponding priority issues

Finalize WG deliverables

- Refined and prioritized recommendations
- Consolidate the documentation of WG analysis and conclusions

Technology Advisory Council
PSTN Transition

The ‘A’ Team

September 24th, 2012

The ‘A’ Team Assignments	
PSTN A	
Copper (Retirement)	Finished
PSTN Users	Finished
Interconnection	
Database Transition	

PSTN Transition - Group A

(The “A Team”)

- Daniel Kirschner (FCC)
- Henning Schulzrinne (FCC)
- Nomi Bergman (Brighthouse)
- Russ Gyurek (Cisco)
- Anthony Melone (Verizon)
- Charlie Vogt (Genband)
- Joe Wetzel (Earthlink)
- Marvin Sirbu (CMU)
- Jack Waters (Level 3)
- Harold Teets (TW Telecom)
- John McHugh (OPASTCO)
- John Barnhill (Genband)

** With contributions from other technical experts **

Questions for Group A

- Database:
  - *What legacy databases will need to transition to a future all-IP environment?*
  - *How will databases that are essential to the operations of the PSTN need to evolve to operate in an IP-based network?*

Databases: Read-out

- Reviews of the relevant Databases (~18, 6 Next-Gen)
  - Creation of a database matrix
    - Function and type
    - Databases importance today, in transition, and post transition analysis
  - Coordination with Team B: What are needs for QoS, Numbering/Identifiers
  - Coordination with M2M team: what will be needed
    - Work in progress/requirements and needs to be defined
  - Developed VoIP interconnection scenarios to demonstrate OTT VoIP* interconnection.
- Actions for December TAC:
  - Finalize Matrix reference guide
  - Creation of a transition roadmap wrt to existing Databases and new databases
  - Deliver final recommendations to TAC

* ATIS slides included in the appendix

Databases: Industry Positions

The Good News:

- A limited number of databases to consider (external)
  - Very small group of vendors involved in DB, however, large number of SPs that use them
  - Greater potential in terms of service support and re-use in post-transition all IP environment
  - General agreement market will drive the needed updates, interoperation, and changes during and post transition
  - Need for standardization on a global basis as we move to all IP
  - Need to investigate the potential of a Location Database
- Several Next Gen databases are already in place

Critical DB's ID'd by TAC WG

DataBase	Description	Comments
LIDB	LIDBs are distributed database systems containing information on nearly all working telephone numbers in North America including listed, unlisted, Centrex/PBX, non-published, landline, wireless and VoIP. LIDB is not used for every call setup but it provides the data necessary for routing Single Number service and some operator-assisted calls. LIDB primarily supports fraud reduction, identity management, and communications services including: • Calling Name/Caller ID • Billing validation • Single Number Service • GetData • Number Portability billing settlements • Fraud Monitoring LIDB supports various TCP/IP interfaces, meets stringent availability and fault tolerance requirements, and offers flexibility to add new data elements as needed by new services.	No major technical hurdles are anticipated for LIDB to continue its role as a rich "data resource" in the future IP Network. LIDB owners have invested heavily in these platforms and may therefore find it economical to continue reusing the resource for new applications – as they are currently doing. The evolution of the product/platform is subject to business decisions by the different LIDB operators (carrier and non-carrier entities).
Toll-free Database	The 800 Service Management System (SMS/800) Functions Tariff FCC No 1 is administered by the Bell Operating Companies (BOCs) - Verizon Communications Inc.; AT&T Inc.; and Qwest (CenturyLink). SMS/800 services are provided to both Responsible Organizations (Resp Orgs) and Service Control Point Owner/Operators (SCP O/Os). Resp Orgs are organizations that use SMS/800 to perform number management functions for the Toll Free numbers for which they are responsible. A service provider may perform these functions directly or arrange to have them completed by another company. A toll-free number is a dialable number in the format 1-8XX-NXX-XXXX, where 8XX can currently be 800, 888, 877, 866 or 855. The Toll-Free Database Service subscribers uniquely define the eligible terminations and control destination/carrier selection associated with their particular toll-free numbers. With Toll-Free Database Service, the 10-digit number (8XX-NXX-XXXX) is analyzed by a LEC database to determine the proper carrier and optionally to provide a 10-digit translated address.	Some toll-free databases have already migrated to SIP-based platforms. However, toll-free service is reliant on the PSTN for initial call setup and number translation. SMS/800 is in the midst of a technology assessment and an evaluation of future technology and services in both the current environment and an IP environment.
ENUM	ENUM is a protocol defined by the IETF that enables circuit-switched and packet network convergence. ENUM translates an E.164 number into Internet domain names. Through the use of DNS resource records it finds SIP servers, email addresses, etc.	Telcordia built a Tier 0/1 ENUM solution for the CC1 ENUM LLC that is a standards DNS-based solution with both a query service and a DNS zone transfer download service to provision service provider Tier 2 servers. The LLC has suspended the CC1 ENUM effort as its members consider their path forward. There are several service provider ENUM solutions known today in the US, including but not limited to: CC1 ENUM, Cable Labs PeerConnect, Neustar Pathfinder and Syniverse Operator ENUM Service. Also, there are several ENUM peering federations, such as iBasis and others that are primarily enterprise solutions which tend to be limited to the members of the federation. In an IP network, a full scale deployment of compatible ENUM or ENUM-like interconnection solutions (not disparate federations) will be needed.
Location Validation Function (LVF)	The LVF is used to "validate" a location in an NG9-1-1 environment. That is, an LVF is queried with a location (in the form of a civic/street address) to determine whether that location can be used to route the emergency call and dispatch responders. The LVF data and interfaces are similar to those used by an ECRF representing the same geographic area(s). The query to the LVF contains a civic location, a service URN, and a validation flag. The response contains all the same information as an ECRF response, as well as an indication of which data elements were found within the LVF (i.e., which elements of the address are considered "valid").	

Potential Recommendations/Steps

- FCC to work with international regulators/partners on a transition plan that has least impact in terms of database work-arounds and requirements for backwards compatibility
- Emergency service Database's are a good example of NG work
- FCC establish milestones and schedule
- Joint session between Team A & Team B on DataBase impact to numbering/Identifiers
  - Further investigation on "location" needs
    - Spoofing concerns
    - Need for geo-location updates/DB
    - How is "Identity" determined

VoIP Interconnect

Questions for Group A

- Interconnection:
  - *What methods have evolved for the exchange of traffic in the hybrid IP-based/circuit-switched network? How will those methods transition as the network shifts to being wholly IP-based?*
  - *How might interconnection requirements and provisioning evolve as consumers adopt new communications technologies, such as HD voice or video?*
  - *Do technological interconnection issues exist at higher protocol levels, e.g., SIP?*
  - *What architectures might evolve to support VoIP interconnection and interconnection of advanced communications services? How would architectures function at different network layers (e.g., MPLS, IP, SIP)?*
  - *Develop a detailed matrix of technical issues that need to be worked out for an IP interconnection framework, the entities who would need to be involved in each aspect, and preliminary thoughts on possible technical solutions.*

VoIP Interconnection: Read-out

- Reviews of VoIP Interconnection issues and status
  - Continued to refine Matrix of Considerations with input from TAC Members
    - Met with XO, AT&T, L3, TWTC, VZ, Earthlink, Comcast
    - Worked with ATIS to review interconnection scenarios and receive input on broader industry initiatives*
  - Coordination with Team B: QoS, Identifiers, Public Safety and Database Committee
    - Hosted Presentations from Neustar, SIP Forum discussing databases and identifiers and their impact on interconnection
    - Developed VoIP interconnection scenarios to demonstrate OTT VoIP* interconnection. Particular Focus around QoS across networks.
  - Drafted Memo outlining areas of agreement/disagreement between industry participants
  - Began Process of Drafting recommendations for TAC
- Actions for December TAC:
  - Finalize Matrix of Considerations
  - Provide Final Answers to Work group questions.
  - Deliver final recommendations to TAC

* ATIS slides included in the appendix

Interconnection: Industry Positions

The Good News:

- Broad agreement on the end state for VoIP Interconnect
  - New public communications network will be an interconnected collection of managed IP networks accommodating real time communications.
  - IP to IP levels playing field
  - Most parties would *ideally* prefer free market solutions vs. regulation.
- Current state of Interconnect
  - The industry is moving forward, Interconnection is happening
    - Interconnection is moving forward based on private IP networks interconnecting
    - IP-to-IP Interconnection agreements for Internet traffic are market based today

VoIP Interconnection: Industry Positions

Unresolved Point ***(Not a technical issue)***

- Section 251/ 252 Applicability - Applying Telecom Act interconnect rules
  - ILECS: IP is an information service, not subject to 251/252 or good faith negotiations
  - Others*: Telecom Act is technology neutral and section 251 interconnection rights extend to managed VoIP with all safeguards including arbitration
    - Skeptical that commercial agreements will ensure competitive parity
  - Concerns:
    - Concerns about "dumping" and "3rd party transit traffic"

*Service Providers and Trade Groups (COMPTEL, NTCA, NCTA, OPATSCO), Wireless (excluding AT&T or Verizon) and State Commissions

Potential Recommendations

- TAC notes that the Commission needs to resolve the fundamental question around section 251 applicability.
- Regardless of 251 interpretation, the Commission should promote a technology-neutral position and allow for continuous innovation going forward
- Be aware of other country implementations
  - CRTC ruling for Canadian market sets interconnect triggers
    - Does Service Provider provide voice interconnection to an affiliate (or anyone else)?
    - Does Service Provider serve VoIP-enabled customers?
    - Do they provide VoIP Interconnection through a subsidiary?
    - In the event of a request, the service providers will have 6 Months to come to agreement.

THANK YOU

Questions & Comments

Supporting Material

Databases

Database Matrix 1 of 5

DataBase	Description	Comments	Network Type/Function Label	Type (call-Routing, management, other)	Maps to: number, name, billing, etc	Replacement? Is there one today?	Entity that runs database	PSTN specific?	Inter-Provider or Intra-Provider
LIDB	LIDBs are distributed database systems containing information on nearly all working telephone numbers in North America including listed, unlisted, Centrex/PBX, non-published, landline, wireless and VoIP. LIDB is not used for every call setup but it provides the data necessary for routing Single Number service and some operator-assisted calls. LIDB primarily supports fraud reduction, identity management, and communications services including: • Calling Name/Caller ID • Billing validation • Single Number Service • GetData • Number Portability billing settlements • Fraud Monitoring LIDB supports various TCP/IP interfaces, meets stringent availability and fault tolerance requirements, and offers flexibility to add new data elements as needed by new services.	No major technical hurdles are anticipated for LIDB to continue its role as a rich "data resource" in the future IP Network. LIDB owners have invested heavily in these platforms and may therefore find it economical to continue reusing the resource for new applications – as they are currently doing. The evolution of the product/platform is subject to business decisions by the different LIDB operators (carrier and non-carrier entities).	Call-completion, Billing, Fraud Mngt	Management (Note: not in signalling path, except for Single Number Service)	Name, Billing Address, Service Provider ID, household language, etc..	No. Expected to continue serving in all major SPs' networks	Major SPs and Alternate DB providers	No, Evolving to support post PSTN services	Inter
Listing Databases	Directory Assistance operators provide customer listing information (telephone numbers, address information, etc.) via a database accessible by the operator or, in some cases, directly accessible by the customer. *411 database*	Listing—type services will continue to be needed in Successor networks for users to obtain contact information. Forms and platforms offering such services may vary from today's 411 DA in an IP network.	Information	Information	Name, number, address, …	Yes, Info discovery	SP's, directory assistance companies	No	External
Operator Intercept Database	INDB stores elements to support Intercept Services related to Intercepted DNs. Intercept Service options include (but not limited to) regular and customized treatment. In a given record, the INDB stores fields such as DN, subscriber name, treatment code, time of day, effective and expiration dates, billed number and business/residence indicator. The treatment code has multiple values; e.g., not in service, call complete with or without announcement, customized announcement, etc. ATIS Packet Systems and Technologies Committee's subcommittee for Signaling, Architecture and Control (PTSC-SAC) is in the process of defining NGN Operator Regular Intercept Standard.	The need for this database will depend on the extent of intercept services deployment in the IP network as well as the evolution status this database (or a future version of it) reaches to properly perform those services in an IP environment.	Call-Completion, call treatment	Call-Routing, Management	n/a	?	SP	There is need for this capability	Intra

Database Matrix 2 of 5

DataBase	Description	Comments	Network Type/Function Label	Type (call-Routing, management, other)	Maps to: number, name, billing, etc	Replacement? Is there one today?	Entity that runs database	PSTN specific?	Inter-Provider or Intra-Provider
Traffic Routing Administration	The Routing Database System (RDBS) is a central database for the dissemination of static network routing and rating elements related to a particular NPA NXX or Thousand Block and service provider identification; e.g. this system performs mass updates needed for deploying new NPA-NXX codes, and NPA splits (new area codes). The system has been modified, enhanced and has evolved to meet changing industry needs for over 25 years. This information reflects the current network configuration and scheduled network changes for all entities originating or terminating within the NANP, and is not available in NPAC.	LERG/LARG/CSARG data will be required throughout the transition until such time as no PSTN networks exist. Having all of the static network routing and rating elements in one place throughout transition should provide ease and efficiency for the industry as they transition from PSTN to all IP If there is a need for similar network data based on numbering and service provider, new tables can be easily derived from the master data sources. If there is no need for a static set of network routing and rating elements based on numbering and service provider; then there may be no need for LERG in all IP network environment.	Database (Repository)	Call-Routing	Network Point Address	Yes, DNS and other IP databases	Vendor A Owns (Used by all major SPs)	n/a	n/a, or intra
	National LIDB Access Routing Guide (LARG), CLASS Services Access Routing Guide (CSARG), and NPA-NXX Activity Guide (NNAG) databases maintained by the (Vendor A) Traffic Routing Administration (TRA).		Database (Repository)	Call Completion and Query Routing	Numbers, Network Addresses, line attributes	required throughout TDM transition. No replacement	LARG, CSARG, TRA is (Vendor A), Each Carrier uses them	Yes	Both
Carrier Access Billing	Maintains orders not for individual lines (except in special instances), but for network facilities such as establishing a feature group; connecting or enhancing trunk groups, entrance facilities, or special access facilities (e.g., private line); and requesting tandem interconnection, database access, or interconnection to the LEC Common Channel Signaling (CCS) network.	Even in an all-IP environment, intercarrier settlements are expected to take place for asymmetrical traffic flow scenarios. “Bill-and-Keep” is not expected to apply to international traffic. However, it remains to be seen whether carriers will continue to use CABS for these settlements in the IP network or if they will establish different forms of billing settlements.	Intracarrier, but existing for the forseable future	Management / Billing System	Billing, Trunking	There are requirements today on the IP side for settlement free billing. More investigation as to the specific applicaton	Carrier Specific	today yes.	Intra Provider
HLR	HLR maintains the persistent service profile information for mobile subscribers, as well as information concerning their current location. Thus, each HLR provides a central repository of information concerning a particular set of subscribers. This information is made accessible to other network elements, as the subscriber roams to different serving areas.	Many HLRs and VLRs are housed in IP-capable MSCs today.	Intracarrier - multiple version exist per service provider	Call Routing/ Call Completion	User/ Location/ Network	Will need to migrate functionality beyond SS7 based capability	Each Carrier	Wireless	Intra Provider

Database Matrix 3 of 5

DataBase	Description	Comments	Network Type/Function Label	Type (call-Routing, management, other)	Maps to: number, name, billing, etc	Replacement? Is there one today?	Entity that runs database	PSTN specific?	Inter-Provider or Intra-Provider
GSMA IMEI	A global central database containing basic information on serial number (IMEI) ranges of millions of mobile devices (e.g. mobile phones, laptop data cards, etc.) that are in use across the world's mobile networks. The GSMA provides access ONLY to the IMEI DB to its members, the mobile network operators across the world, and to qualified industry parties (i.e. manufacturers of device management products), to determine what types of devices are being used by their customers, and what features they support. The IMEI DB also supports what is known as a "black list". The black list is a list of IMEIs that are associated with mobile devices that should be denied service on mobile networks because they have been reported as lost, stolen, faulty or otherwise unsuitable for use. The IMEI is a 15-digit number that is used to identify the device when it is used on a mobile phone network. The IMEI must be unique for each device, so there needs to be a way of managing allocations of IMEIs to handset manufacturers to ensure that no two devices use the same IMEI. The GSM Association performs this role, and records all of the IMEIs that are allocated to mobile device manufacturers in the IMEI DB.		Device registration	Management	Device capabilities	No, not needed	GSM association	No	n/a
ALI Database	The E9-1-1 tandem will forward a key with the 9-1-1 call to the PSAP. In many cases, the key will be the callback number. The PSAP will use this key when it queries the Automatic Line Identification (ALI) database. The ALI will return the information that is associated with the key, including such things as the callback number, the Police, Fire and Medical units responsible for that location. The ALI database will either need to be a shared database (i.e., containing all information related to wireline and wireless Emergency Calls), or be capable of coordinating with other ALI databases.		Multiple versions, geographically spread, Multiple Carriers provide	Emergency Call Services, Call Routing, Call Management	Number, name, location with specialized location information provided to PSAP	NG911 is working all issues related to emergency location and call completions	Multiple Carrier	the E911 tandem is a PSTN construct but the function is not.	Interprovider

Database Matrix 4 of 5

DataBase	Description	Comments	Network Type/Function Label	Type (call-Routing, management, other)	Maps to: number, name, billing, etc	Replacement? Is there one today?	Entity that runs database	PSTN specific?	Inter-Provider or Intra-Provider
Selective Routing Database	Selective Routing Database (SRDB) is used in legacy Emergency Services Networks to determine which PSAP to route a call to.		Emergency Calling	Call Routing	Name, number, address, …	ECRF (LOST protocol)	SP to the PSAP	Yes, today	Intra
	** In a NG9-1-1 Emergency Services IP Network there is an Emergency Call Routing Function (ECRF) that will provide the equivalent functionality, although with different inputs and outputs.			Call Routing					Intra
Toll-free Database	The 800 Service Management System (SMS/800) Functions Tariff FCC No 1 is administered by the Bell Operating Companies (BOCs) - Verizon Communications Inc.; AT&T Inc.; and Qwest (CenturyLink). SMS/800 services are provided to both Responsible Organizations (Resp Orgs) and Service Control Point Owner/Operators (SCP O/Os). Resp Orgs are organizations that use SMS/800 to perform number management functions for the Toll Free numbers for which they are responsible. A service provider may perform these functions directly or arrange to have them completed by another company. A toll-free number is a dialable number in the format 1-8XX-NXX-XXXX, where 8XX can currently be 800, 888, 877, 866 or 855. The Toll-Free Database Service subscribers uniquely define the eligible terminations and control destination/carrier selection associated with their particular toll-free numbers. With Toll-Free Database Service, the 10-digit number (8XX-NXX-XXXX) is analyzed by a LEC database to determine the proper carrier /optionally provide a 10-digit translated address.	Some toll-free databases have already migrated to SIP-based platforms. However, toll-free service is reliant on the PSTN for initial call setup and number translation. SMS/800 is in the midst of a technology assessment and an evaluation of future technology and services in both the current environment and an IP environment.	Intercarrier routing database	Routing	Number, billing, carrier code	No. There are IP capabilities but not replacements. Backwards compatibility will be needed. Some SPs have migrated their 8xx to an IP platform	The 800 Service Management System (SMS/800) Functions Tariff FCC No 1 is administered by the Bell Operating Companies (BOCs) - Verizon Communications Inc.; AT&T Inc.; and Qwest.	Yes	Inter
ENUM	ENUM is a protocol defined by the IETF that enables circuit-switched and packet network convergence. ENUM translates an E.164 number into Internet domain names. Through the use of DNS resource records it finds SIP servers, email addresses, etc.	(Vendor A) built a Tier 0/1 ENUM solution for the CC1 ENUM LLC that is a standards DNS-based solution with both a query service and a DNS zone transfer download service to provision service provider Tier 2 servers. The LLC has suspended the CC1 ENUM effort as its members consider their path forward. There are several service provider ENUM solutions known today in the US, including but not limited to: CC1 ENUM, Cable Labs PeerConnect, Neustar Pathfinder and Syniverse Operator ENUM Service. Also, there are several ENUM peering federations, such as iBasis and others that are primarily enterprise solutions which tend to be limited to the members of the federation. In an IP network, a full scale deployment of compatible ENUM or ENUM-like interconnection solutions (not disparate federations) will be needed.							

Database Matrix 5 of 5

DataBase	Description	Comments	Network Type/Function Label	Type (call-Routing, management, other)	Maps to: number, name, billing, etc	Replacement? Is there one today?	Entity that runs database	PSTN specific?	Inter-Provider or Intra-Provider
Number Portability Administration Center (NPAC) and Number Portability Databases	LNP allows end users to keep their telephone numbers when they change communications service providers. NPAC is the registry that enables LNP. NPAC is a Service Management System (SMS) governed, supported and shared by competing communications service providers. The data managed by this shared resource is used to route, rate and bill calls with respect to telephone numbers that are no longer assigned to the original carrier. The data is downloaded by individual carriers. NPAC is not queried for each call. Number Portability Databases (NPDB) contains all ported numbers within a ported domain as well as routing information necessary to support number portability. Its function is to provide the association between the called party and the carrier location routing number (LRN), identifying the switch to which the call should be routed.	IP network will still require mechanism to manage portability of telephone numbers between carriers. NPAC and LNP databases will need to evolve from SS7.							
CRIS	Customer Record Inventory System (CRIS) establishes and maintains end user accounts. Billing printing and remittance processing takes place through CRIS. Data in CRIS is updated through the service order process.	Customer account information and inventory will continue to be required in IP networks. However, each provider's choice of system will vary.							
Network Traffic Management (NTM)	Network Traffic Management Operating Systems continuously monitor and control a large variety of switching systems within their areas. They gather network data and perform calculations every 5 minutes; results of these calculations are matched against preset thresholds in the NTM database; e.g. switching system performance indicators, and trunk-group overflow conditions.	In an IP network, similar functionality is expected to be available for monitoring and maintaining quality of service.	Internal Carrier system						
Inventory databases	Used to run own business. Are these of interest to WG-A? LFACS, TIRKS, CLI, etc. These are SP internal databases		Internal	management	many	n/a	SP	Yes	n/a
Do Not Call Database	The National Do Not Call Registry is managed by the Federal Trade Commission (FTC), the nation's consumer protection agency. It is enforced by the FTC, the Federal Communications Commission (FCC), and state law enforcement officials. This Registry was created so that telemarketers and sellers covered by the FTC's rules can remove a consumer's phone number from their call lists. Telemarketers are required to search the registry every 31 days and delete from their call lists phone numbers that are in the registry.								
Critical infrastructure Databases	Homeland security Type?	No Data							

Database Matrix Next Gen

Emergency Call Routing Function (ECRF)	A functional element in an i3 Emergency Services IP Network (ESInet) which takes location information (in the form of a civic/street address or geo-coordinates) and a Service Uniform Resource Name (URN) that is associated with emergency services, and maps it to routing information in the form of a Uniform Resource Identifier (URI) which is used to route emergency calls toward the appropriate PSAP for the caller's location, or towards a responder agency.
Emergency Routing Database (ERDB)	The ERDB is a database in the NENA i2 architecture that contains routing information associated with each Emergency Service Zone (ESZ) in a serving area. It supports the boundary definitions for ESZs and the mapping of civic address or geo-spatial coordinate location information to a particular ESZ
Call Information Database (CIDB)	The CIDB is part of the NENA i3 architecture. Its role is to store Additional Call Data associated with an emergency call. Additional Call Data consists of non-location information such as Service Provider contact information and class of service information. A CIDB may also contain information about the device that call originated from. The data content and structure associated with Additional Call Data is being defined jointly between NENA and IETF
Additional Caller Data Repository (ACDR) (formerly referred to as the Subscriber Database [SDB])	An i3 database operated by a carrier or other service provider which supplies data which provides information about the person(s) associated with the device placing the call. The ACDR is queried with the caller's "From" address from the SIP signaling message and responds with: • An XML document containing the caller's Additional Caller Data (by value). • A URI that can be used to dereference the callers' Additional Caller Data. • A HTTP 303 response (Iterative Refer), instructing the client to direct an Additional Caller Data query to the resource specified in the response. • An indication that no data was found for the provided "From" URI
Location Validation Function (LVF)	The LVF is used to "validate" a location in an NG9-1-1 environment. That is, an LVF is queried with a location (in the form of a civic/street address) to determine whether that location can be used to route the emergency call and dispatch responders. The LVF data and interfaces are similar to those used by an ECRF representing the same geographic area(s). The query to the LVF contains a civic location, a service URN, and a validation flag. The response contains all the same information as an ECRF response, as well as an indication of which data elements were found within the LVF (i.e., which elements of the address are considered "valid").
Spatial Information Function	The SIF is a specialized form of a Geospatial Information System (GIS) database for use with NG9-1-1. Nearly all location related data is ultimately derived from the SIF. The SIF supplies data for the ECRF and LVF.

What legacy DBs will need to transition to a future all-IP environment?

- Geographic numbering
  - NANPA, PA, NPAC
- Non-geographic numbering
  - SMS/800
- Public safety
  - ALI

How will DBs that are essential to the operations of the PSTN need to evolve to operate in an IP-based environment?

- Geographic numbering
- May need to add IP addressing information to numbering assignments
- Non-geographic numbering
  - May need to add IP addressing information to numbering assignments
- Public Safety
  - VoIP providers are required to integrate customer addresses into the existing ALI infrastructure

1. http://ecfsdocs.fcc.gov/filings/2011/03/08/6016172420.html

What new DBs or DB architectures will be necessary or helpful in an all-IP environment? To what extent have these new DBs been developed, and by whom? What are the challenges?

- Telephone number authentication
- TN-IP Mapping
  - A method to map a TN to an Internet address, e.g., ENUM
  - Each carrier is expected to assess which other databases are “helpful” in conducting their business and whether some of the current databases will transform to serve IP needs
  - Many vendors have created different implementations of ENUM (see Appendix, Slide 29)
  - Most of these current implementations are associated with particular federations. Some are proprietary and may not be compatible with each other.

PSTN B Successor Networks Working Group

Co-Chairs:

Brian Daly, AT&T

John Barnhill, GENBAND

PSTN Successor Infrastructure Work Group

- The PSTN Successor Infrastructure Work Group will focus on identifying key elements essential to an IP-based communications infrastructure.
- As consumers and businesses turn to other networks to replace functionality previously provided by the PSTN, questions arise as to how those networks can replicate the best characteristics of the PSTN while taking advantage of their advanced technological underpinnings.
- Successor networks face new quality of service and robustness challenges. They may depend upon new databases and take advantage of new interconnection standards.
- The work group will look past the challenges of transitioning from the legacy PSTN, and focus on the technical characteristics and user experience of successor networks.
- The work group will make recommendations to the Commission to identify challenges to the effective performance of successor networks.

Work Group Progress

- Bi-weekly calls held by working group reviewing three major items
  - Quality of Service – David Clark
  - User/Service/App Identifiers – Mark Bayliss
  - Robustness and Public Safety – Brian Daly
- Worked with ATIS PSTN Transition Landscape Team to generate technical evaluations of WG questions
- Breakout sessions to address specific sub team focus areas

Quality of Service

David Clark

Quality of Service

- **Champion**: David Clark
  - **Participants**: Joe Wetzel, Kevin Kahn, Dan Reed, Jesse Russell, Tom Evslin, Harold Teets
- **Background:**
  - With the move of VoIP and other critical services to IP-based platforms, the quality of these services will be of increasing public concern.
  - A variety of different IP-based platforms will be used for these services, so the interconnection of these platforms, and the service quality of these interconnections, will be of concern.
- **Definitions:**
  - Managed IP network: An IP-based network offering services to the public, such as VoIP, not a part of the public Internet. Usually operated by facilities owner.
    - For example, the platform used by providers such as Comcast to offer telephone service.
  - Private IP network: An IP-based network operated by an enterprise or other private entity and providing service to that entity.
    - For example, the IP analog of a PBX for VoIP
  - The public Internet: The global, interconnected IP network.
    - Supports OTT VoIP products such as Vonage, Skype, etc.

QoS in Managed IP Networks

- The move to VoIP over managed IP networks is well underway.
  - Interconnection often based on use of PSTN or IP exchange points.
  - Some service quality issues may be arising due to technology or economic issues.
- Little opportunity to use advanced QoS tools to manage these networks.
  - If dominated by a single application class, only approach to QoS is adequate provisioning.
  - Addition of new services will change this situation.
- Little evidence that FCC should concern itself with technical details of managed IP networks.
  - Techniques for interconnection, etc. will evolve.
- Focus on defining minimal expected service quality.
  - Work with industry and standards bodies to define metrics of call quality.
  - Encourage industry to track quality impairments over time.
  - Encourage instrumentation of end-node VoIP software to detect and report quality impairments.
- Conversion from circuit to packet-based managed telephony does not change the level of concern the FCC should have with respect to service quality.

Service quality today

- Several sorts of possible service impairments.
  - Problems related to packet carriage (loss, delay).
    - Addressed using advanced QoS tools and provisioning.
  - Application-level problems (voice echo).
  - Failure of calls to complete.
- Issues are observed today with service quality of calls.
  - Example: call completion in rural areas.
    Problems may relate to hybrid calls (crossing multiple technologies).
  - FCC has reason to track call quality today.

Measurement

- Measurements taken inside network cannot always detect service impairments.
  - Problems may only be detected at end nodes and service points.
- Need a measurement/reporting architecture that allows end-node reporting.
- FCC should encourage open development of standards, tools and metrics to track quality.

Interconnecting VoIP Variants

- VoIP over managed IP networks, ISP VoIP over public Internet using QoS tools, private IP networks, mobile VoIP services, OTT VoIP.
  - Basic expectation: all of these must be able to interconnect in effective ways to provide interoperable service.
    - Problems with hybrid call completion today suggests there may be problems.
  - Different intrinsic service quality may compound issues of interconnection.
    - Different economic motivations of different providers are a further factor.
    - Isolation of service impairments across providers will be a difficult problem.
  - Proposed expectation: points of interconnection should not be limiting factor in quality.
  - Now: measurement and monitoring appropriate.

QoS on the Public Internet

- Internet today is “best effort”.
  - No guarantees of performance but current performance often adequate (e.g. Skype, Vonage).
- FCC has concerned itself with service quality of public Internet.
  - SamKnows tests measure jitter, latency, etc.
  - Proxy tests for classes of applications—video, VoIP.
  - No attention at this time to provision of advanced QoS on public Internet.
- Continued attention justified to track service quality over time.
  - Not a call for regulation.

Special QoS Considerations: Public Internet

- Citizen emergency access.
  - Mixing VoIP with other traffic on public Internet may lead to VoIP degradation in times of crisis.
    - Degraded capacity and functionality in network.
- VoIP equivalent of GETS or access priority.
  - Should we assume need for this service on public Internet?
- Universal service
  - Will OTT VoIP ever be the service of last resort?
  - If so, what service qualities will qualify?

General Principles

- Consumer choice in VoIP services
- Support range of options to satisfy universal service objectives for voice.
- Establish basic expectation that they will interconnect at reasonable quality.
- Remember that VoIP will not be the only service carried over managed IP networks.
  - May be interconnection/QoS issues for other services.

User/Service/App Identifiers

Mark Bayliss

User/Service/App Identifiers

- **Champion**: Mark Bayliss
  - **Participants**: KC Claffy, Kevin Kahn, Jesse Russell, Charlotte Field, Tom Evslin

- What changes might be expected in a numbering plan optimized for IP-based communications services? (For example, current numbering systems are tied to physical resources, such as lines, and are often service specific, e.g., SMS short codes.)What are the obstacles to assigning numbers to users, analogous to how domain names are assigned, rather than to service providers?
- Should number assignment need to retain a geographic component? For example, do numbers still need to be assigned to specific rate centers in an all-IP world?
- How can the receiver of a call validate that the caller is authorized to use the number or other identifier ("caller ID validation")?
- What role is ENUM going to play as a number mapping service as the numbering system evolves? Is there a need for additional or alternate solutions?
- How might technological changes drive signaling requirements and number translation capabilities?

Observations

- Likely to have three main types of identifiers going forward
  - **E.164** based identifiers will be a network requirement for a period of time
  - **OTT's** service providers and webRTC voice enablement are disruptors to the status quo, however:
    - SIP/ e.164 compatibility will be required for VoIP Interconnect with service providers.
    - Limited interop scope of OTT services with other IP services or PSTN will likely limit the interoperability of advanced capabilities across service providers.
  - **Email** address are an ideal source of Globally unique Identifiers, already used for multiple services but with security and portability limitations.
- The Commission has plenary authority over the number plan
  - Proprietary address schemes, email based identifiers etc fall outside the purview of the FCC (Should there be a plan for regulated/unregulated interop?)
- Historic Usage as Geographic/ Rate Center/ LATA Identifier
  - Becoming irrelevant (move to 10 digit dialing everywhere)
- VoIP Interconnect, NG911,Databases all have interdependencies on the addressing schemes adopted

Actions to Baseline Current Situation

- Several reviews of the future of numbers and identifiers have been held with working group and industry participants to baseline current activities
  - Neustar (Tom McGarry) on the future of numbers, portability
  - SIP Forum (Richard Shockey) on the near term requirement for ENUM and the continued need for completion to both e.164 and IP Uniform Resource Indicators
  - Google , Skype ,Sidecar and others rapidly expanding the concept of direct Peer to Peer communication addressing for services while continuing to support e.164 and SIP resource indicators for interoperability.
- Drafted Preliminary responses to work group questions, final on 12-10-2012
  - Some points of disagreement and scope are being worked on.
- Identified Multiple uses for Telephone numbers which we must consider as part of a PSTN transition plan.
  - Routing – PSTN uses to route to end devices
  - Personal Identification (includes affinity programs, ID verification etc.)
  - Application identification
  - Geographic Location Determination - Method to map name to address

Additional Factors To Be Considered

- Who owns the Identity?
  - Subscriber? Service Provider? The Commission?
  - Can we separate the service/device from the identifier?
- Who Assures Identity?
  - Web/ DNS
  - PSTN (caller ID, display name: CNAM database, based on caller ID)
  - How do you stop Caller ID Spoofing?
- How to address Machines (cars, appliances, home automation et al)?
  - explosion of M2M (view of 50B connected devices), e.164 not sufficient
- Should numbers be treated as names?
- Should numbers have a geographic component?
  - Create a plan to phase out rate centers and LATAs

Communication Identifiers Characteristics

Property	URL - owned	URL - provider	E.164	Service-specific
Example	alice@smith.name sip:alice@smith.name	alice@gmail.com sip:alice@ilec.com	+1 202 555 1010	www.facebook.com/alice.example
Protocol-independent	no	no	Yes*	yes
Multimedia	yes	yes	maybe (VRS)	maybe
Portable	yes	no	somewhat	no
Groups	yes	yes	bridge number	not generally
Trademark issues	yes	unlikely	unlikely	possible
Privacy	Depends on name chosen (pseudonym)	Depends on naming scheme	mostly	Depends on provider "real name" policy

* Limitations are that e.164 doesn't include mapping domain (Assumes PSTN)

Numbers vs. DNS & IP addresses

	Phone #	DNS	IP address
Role	identifier + locator	identifier	locator (+ identifier)
Country-specific	mostly	optional	no
# of devices / name	1 (except Google Voice)	any	1 (interface)
# names /device	1 for mobile	any	any
ownership	carrier, but portability unclear (800#)	property, with trademark restrictions	ISP
who can obtain?	geographically-constrained, carrier only	varies (e.g., .edu & .mil, vs. .de)	enterprise, carrier
porting	complex, often manual; wireline-to-wireless may not work	about one hour (DNS cache)	if entity owns addresses
delegation	companies (number range)	anybody	subnets
identity information	wireline, billing name only	WHOIS data (spotty)	RPKI, whois

No agreed mapping of E.164 to SIP/VoIP endpoints

- Currently based on bilateral exchange of data among operators (often by simple spreadsheet!)
- No agreement across Autonomous System [AS]/carrier boundaries.
  - Limits ability of enterprises to benefit from heavy investment into SIP-based systems and trunking services
  - Not scalable to 1200 licensed operators in the United States.
  - Need for new database(s) for E.164 phone number into IP URIs translation with associated metadata. Progress not currently tracked/measured
- Recommendation:
  - Propose timeline for industry to work out this problem

Shockey, Ex Parte, 4 September, 2012

Potential Commission Actions

"A clear national policy on the Future of Numbering is… an essential precondition for further progress on the National Broadband Plan, SIP/VoIP Interconnection and the inevitable transition to all IP networks." Shockey, Ex Parte, 9/4/2012

- Initiate rulemaking on the full range and scope of issues with numbers/identifiers
  - relationship of Numbering to SIP/VoIP Interconnection and the PSTN Transition
- Consider setting a schedule to implement nationwide 10 digit dialing
  - Align LATA's and rate center elimination with "Bill and Keep" implementation date
  - Fully decouple geography from number and Implement geographic number portability
- Sponsor multi-stakeholder forum to define requirements for E.164 real-time communications and for new databases that map E.164 to IP data.
- Sponsor a series of Technical Workshops involving network operations experts to address technical transition issues moving to an all IP network.
- Review approach with major IP to IP providers "Google, Skype, Sidecar and others" and work with ATIS, IETF and ARIN to stay aligned with Internet and industry initiatives.

Robustness and Public Safety

Brian Daly

Robustness and Public Safety

- **Champion**: Brian Daly
  - **Participants**: John Barnhill, Dale Hatfield, Mark Bayliss, Marvin Sirbu, David Tennenhouse, Tom Evslin
- How will the transition affect network robustness?
- What will robustness likely improve or degrade in the transition?
- What technologies can improve network survivability? How effective are these technologies likely to be compared to existing PSTN survivability?
- Wireless
  - Backup power at base station and handsets?
  - Capacity vs. footprint tradeoffs
- Wireline
  - Backup power for both the network and home or small business environments?
- What, if any, additional capabilities are needed from the underlying broadband network to enable 911 or other emergency services functionality that is at least equivalent to that offered by the existing system?
- **Next steps**: Finalize responses to WG Questions for December TAC

Robustness and Public Safety - Observations

- Technology is defined for NG 9-1-1
  - 10 Year plus history of work to define NG9-1-1
    - Multiple groups – NENA, ATIS, IETF, ITU, CSRIC et al
  - Defines IP-based interfaces into the PSAP
  - Expands 911 for new mediums (text, photos, videos, data)
- Slow migration to IP has the potential to limit TDM transition
- Highly Distributed Ownership is largest implementation hurdle
  - Federal, State, Community etc.
  - Multiple constituencies/ technologies
  - No central deployment funding or timetable

Emergency Communications

- Citizen-to-authority
  - Next Generation 9-1-1
  - Multimedia Emergency Services (MMES)
- Authority-to-citizen
  - CMAS
  - Next Generation Alerting
- Authority-to-authority
  - Next Generation Network Government Emergency Telecommunications Service (NGN GETS)
  - ESInet & PSBB, FirstNet

Constituencies

- End Users
  - Wireline, Wireless, VoIP, SMS, MMS, Video, Enterprise
- First Responders
  - FirstNet, GETS, WPS, etc
- PSAPs
  - NG911 – Survivability, Diverse Routes, Geographic Redundancy
- Law Enforcement
  - CALEA, GETS, WPS, PSBB
- Governments - Many

Slow, but Notable Deployment Progress

- February 2012 – Legislation to create FirstNet (with $7B in funding)
  - Nationwide broadband network, managed within NTIA
    - take “all actions necessary” to build, deploy, and operate the network…
- Public Safety Interoperable Communications (PSIC) Grant Program
  - Awarded nearly $1B (NTIA with the Dept. of Homeland Security)
- DoT’s National Highway Traffic Safety Admin. and NTIA awarded grants to improve 911 services and implement next-generation technologies.
  - $40M awarded to 30 states/territories, authorized in ENHANCE 911 Act
  - Additional $115 million in approved in 2012 legislation
- FEMA funding ($B) MULTIPLE grant programs to accelerate deployment
- USDA providing targeted loans for NG911 upgrades
- Trials in progress

Public Safety – Preliminary Recommendations

- Large number of recommendations by multiple agencies (Example on next slide)
  - TAC should defer to SME's in CSRIC, ATIS, IETF, NTIA, NENA, DOT, DoHS etal
- Create and promote goal for nationwide deployment
  - Ask Congress to Identify a coordinating authority to work with States on implementation
  - Set a target implementation dates with State driven milestones
  - Create PSA's to promote Advantages – Scale, Networking, Failover
- Promote standards development to support PSBB-ESInet interworking
  - Multimedia content from ESInet out to first responders via the PSBB LET network
- *General Conclusion:*
  - *Lack of mandate and funding will gate deployment.*
  - *Long period of interop between current and future will be the reality*
  - *Frustration by long-time advocates due to slow progress*

Funding Recommendations

911 Program Office (911.gov)

- "A National Plan for Migrating to IP-enabled 911 Systems" has identified several options for funding, governance and policy issues:
  - Ensure that IP-enabled 911 upgrades are considered a fiscal priority for States and local jurisdictions and Federal grant programs
  - Change outdated funding mechanisms to be more technology-neutral
  - Ensure that 911 funds are preserved for 911
  - Clarify jurisdictional frameworks and responsibilities and identify the coordination required at each level of government to make IP-enabled 911 possible
  - Consider developing model legislation that would address updating regulation, legislation and other policies to reflect modern communications and IP-enabled 911 system capabilities

http://www.911.gov/911-issues/funding.html

Backup Slides

FCC Dockets on 911

- CC Docket No. 94-102
  - Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems
- WC Docket No. 05-196
  - E911 Requirements for IP-Enabled Service Providers
- PS Docket No. 07-114
  - Wireless E911 Location Accuracy Requirements
- **PS Docket No. 10-255**
  - **Framework for Next Generation 911 Deployment**
- **PS Docket No. 11-153**
  - **Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications**

How will the transition affect network robustness?

- This addresses availability of the network after the transition.
- Some components of broadband and wireless access technologies are not necessarily engineered to the same level of reliability as central office switches.
- The existence of multiple access options (wireless and broadband) may provide greater overall availability since they are largely independent.
- Application, transport, and interconnect issues are also important in accessing end-to-end availability.
  - Transport availability may be similar since it may be mostly the same transport infrastructure as today.
  - End-user service availability is unknown, but may be driven by commercial factors and competition
  - Interconnect availability is evolving and is an area of active study in the industry

What will robustness likely improve or degrade in the transition?

- This addresses availability of the network during the transition.
- Access and transport availability will be based on the level of availability the system is engineered for.
- Interconnection in the IP environment is more flexible with many more commercial and technical possibilities.
  - More interconnect design choices
  - More media types and bandwidth requirements
- End-user service availability will likely be driven by commercial factors and competition.

What technologies can improve network survivability? How effective are these technologies likely to be compared to existing PSTN survivability?

- IP technology is inherently more survivable than circuit-switched
- Redundancy and geographic distribution can in many cases increase availability. Application of these methods depend on the engineering requirements.
- The above capabilities can be used to make accesses as available as (or more available than) the PSTN.
- Whether backup power is provided and the duration of provided backup power depends on the engineering decisions. This applies to both wireless and wireline.
- As users migrate to new technology (e.g. as with cordless phones, modems, and routers today), customer premise backup power will supplement network backup power.

What, if any, additional capabilities are needed from the underlying broadband network to enable 911 or other emergency services functionality that is at least equivalent to that offered by the existing system?

Emergency Services

Requirements for Successor Network

In this context, “Emergency Services” is defined as:

- **Citizen-to-authority**
  - Next Generation 9-1-1
  - Multimedia Emergency Services (MMES)
- **Authority-to-citizen**
  - Next Generation Alerting
- **Authority-to-authority**
  - Next Generation Network Government Emergency Telecommunications Service (NGN GETS)

Emergency Services
Requirements for Successor Network (cont.)

- Next Generation 9-1-1
  - Location accuracy for wireless handsets and VoIP clients
  - NENA Emergency Services (i3) interconnection and interoperability for 3GPP IMS based systems
  - 9-1-1 Availability – ensure 9-1-1 is available for voice, text, and multimedia communications from all communications methodologies supported by the PSTN successor network during times of emergencies
    - Methodologies used for day-to-day communications should support Next Generation 9-1-1 communications
    - Discussion of 9-1-1 call prioritization is being investigated by the FCC CSRIC Working Group 10 and recommendations on this issue should defer to CSRIC.
- Applicable Standards:
  - NENA Functional and Interface Standards for Next Generation 9-1-1 Version 1.0 (i3) defines system architecture for the evolution of Enhanced 9-1-1 to an all-IP-based emergency communications system
  - FCC Emergency Access Advisory Committee (EAAC) addressing texting and multimedia capabilities to emergency services which will benefit both the individuals with disabilities and the general public
  - FCC CSRIC III Working Group 3: E-9-1-1 Location Accuracy
  - ATIS ESIF Next Generation Emergency Services (NGES) subcommittee providing industry input on
    - Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination
    - Automating Location Acquisition for Non-Operator-Managed Over-the-Top VoIP Emergency Services Calls
  - 3GPP TS 23.167, IP Multimedia Subsystem (IMS) emergency sessions
  - FCC CSRIC III Working Group 10: 911 Prioritization

Emergency Services
Requirements for Successor Network (cont.)

Multimedia Emergency services (MMES)

- Extend emergency services to support all media types including
  - Voice
  - Real time video
  - Text
  - File transfer
  - Video clip sharing, picture sharing, audio clip sharing
- Standards
  - FCC Emergency Access Advisory Committee (EAAC) addressing texting and multimedia capabilities to emergency services which will benefit both the individuals with disabilities and the general public
  - 3GPP TS 22.101 Service aspects; Service principles contains requirements added for IMS Multimedia Emergency Sessions (MES)

Emergency Services
Requirements for Successor Network (cont.)

Next Generation Alerting

- Expansion of alert delivery media (e.g., video, audio, text, graphics, etc.) for most effective delivery of next generation alerts
- Common Alerting Protocol for generating, formatting, and distributing alerts
- Security to mitigate potential threats and attacks on the alerting systems
- Integration of social media into alerting systems
- Standards
  - FCC CSRIC III Working Group 2: Next Generation Alerting
  - Internet Engineering Task Force (IETF) Authority to the Citizen Alert (ATOCA) Working Group
  - 3GPP TS 22.268 Public Warning System (PWS) requirements

Emergency Services
Requirements for Successor Network (cont.)

Next Generation Network Government Emergency Telecommunications Service (NGN GETS)

- Evolution of legacy GETS and Wireless Priority Service (WPS) to achieve service continuity in an IP Successor network
- Expands GETS requirements for Session Initiated Protocol (SIP) based voice service and requirements for priority processing and signaling of NGN GETS calls
- Standards - Industry Requirements (IR)1 for Next Generation Network (NGN) GETS Voice service developed under the National Communications System (NCS)

Emergency Call Routing Function (ECRF)

- Next Generation 9-1-1 route database, part of NENA i3 standard
- Maps a location and a "Service URN" to a SIP URI using RFC5222 LoST protocol
- FCC is undertaking a 5 step effort to evaluate implementation of NG 9-1-12

Participant	Work Group Assignment
KC Claffy	**Participant on Identifiers**, Interconnection
David Clark	**Leader of QoS**
Brian Daly	**Co-Chair Team B, Leader of Robustness and Public Safety**
Russ Gyurek	Co-Chair Team A
David Tennenhouse	**Participant Robustness and Public Safety**
Charlie Vogt (John Barnhill)	***Co-Chair Team B*, Participant On Robustness and Public Safety**
Joe Wetzel (Chris Murray)	**Participant in QoS**
Mark Bayliss	**Leader of Identifiers, Participant Robustness and Public Safety**
Kevin Kahn	**Participant in QoS, Participant on Identifiers**
Tom Evslin	**Participant in QoS, Participant on Identifiers, Participant Robustness & Public Safety**
Dan Reed	**Participant in QoS**
Jesse Russell	**Participant in QoS, Participant on Identifiers**
Harold Teets	**Participant in QoS**, Co-Champion of Interconnect and Copper WG in PSTN-A
Charlotte Field	**Participant on Identifiers**
Marvin Sirbu	**Participant Robustness and Public Safety**
Henning Schulzrinne	Group B FCC Liaison
Daniel Kirchner	Group A FCC Liaison
Dale Hatfield	**Participant Robustness and Public Safety**
Dick Green	*(TBD – just joined the working group)*

Technological Advisory Council

Multiband Devices Working Group

24 September 2012

Charter and Working Group Members

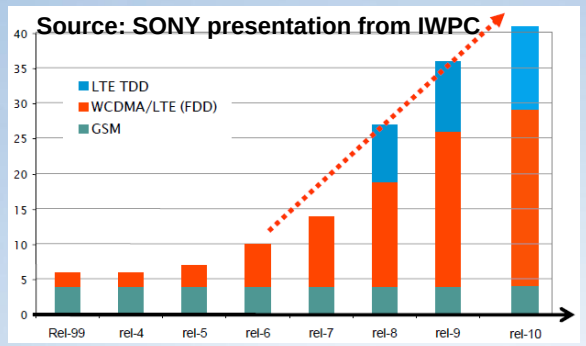
- The Multi-band Devices Working Group will study the challenges in developing subscriber equipment that is capable of operating over numerous frequency bands.

- WG Chair: Brian Markwalter
- FCC Liaisons: Michael Ha, Chris Helzer
- WG Members:
  - John Chapin
  - Lynn Claudy
  - Marty Cooper
  - Jack Nasielski
  - Mark Richer
  - Jesse Russell
  - Peter Gaal
  - William Mueller

Problem Statement

- Diverse and Complex Frequency Options
  - 22 FDD bands, 11 TDD bands defined in 3GPP R10.6, and counting
  - 4 types of positioning (GPS, Glonass, Galileo, Compass)
  - Multiple types of unlicensed bands: WiFi, BT, NFC, etc*
- Each carrier desires different combinations of band support
- International roaming further complicates the handset design
- Future spectrum allocation continues to be fragmented
- Spectrum Aggregation being standardized in 3GPP

- *What is the expected roadmap for receiver improvements?*
- *How does that roadmap inform policy and industry decisions?*



Number of Bands per 3GPP Releases

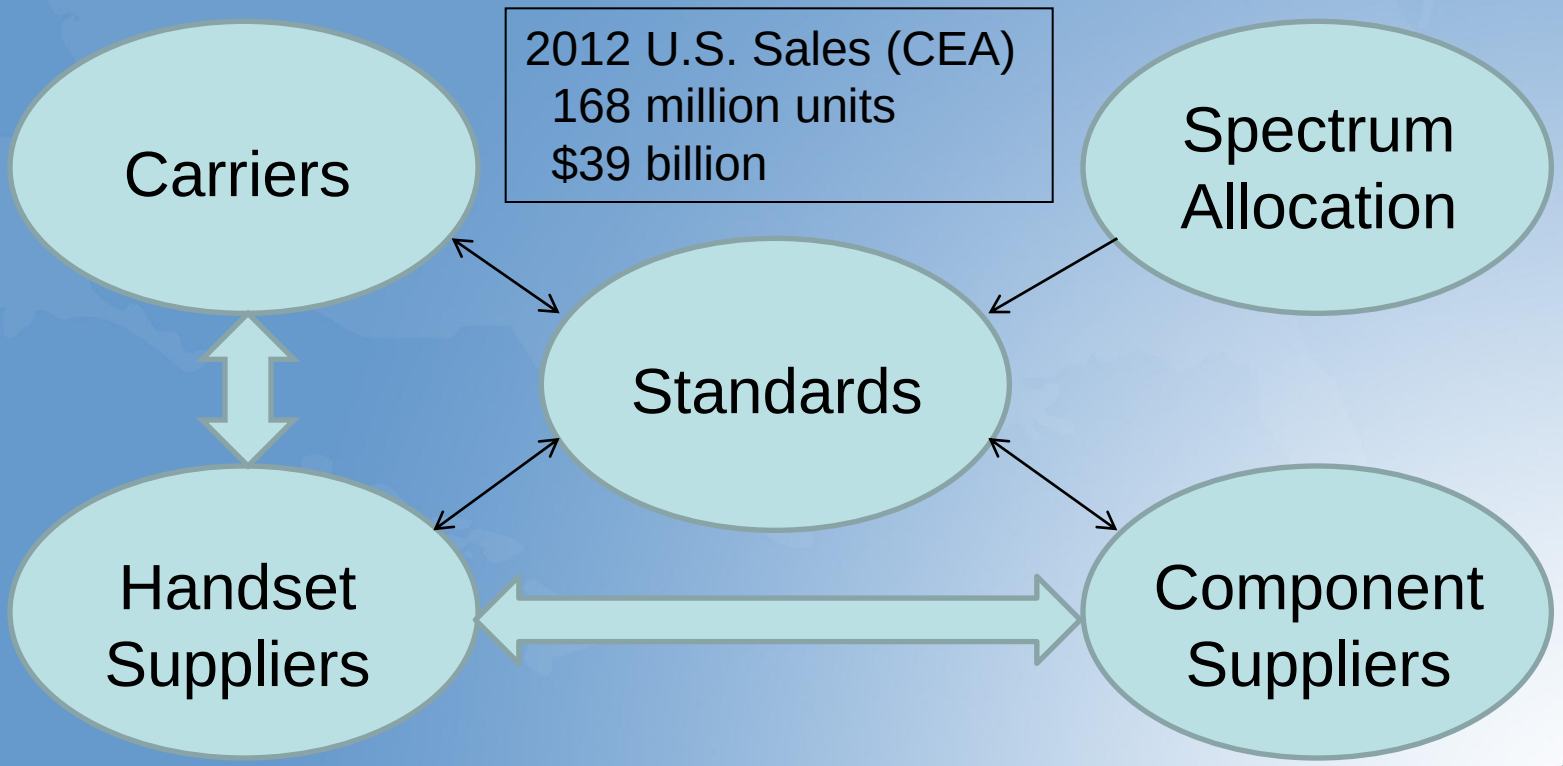
Second Quarter Review

- Advancements in processing power of Baseband Chipset and increased density of CMOS silicon for Transceiver IC have enabled multi-band/mode implementation in a cost-effective manner
- Due to power handling, temperature variation, and other operational requirements, RF Front End and antenna elements have become the limiting factor of multi-band radios
- Further study was reported for tunable elements

Third Quarter Focus

- Capitalize on FCC's Forum on Future Wireless Band Plans
- Drill down with experts on baseband, transceiver, RF front end and antenna
- Understand rate of change and system design/cost issues
- Consider roadmap contributions

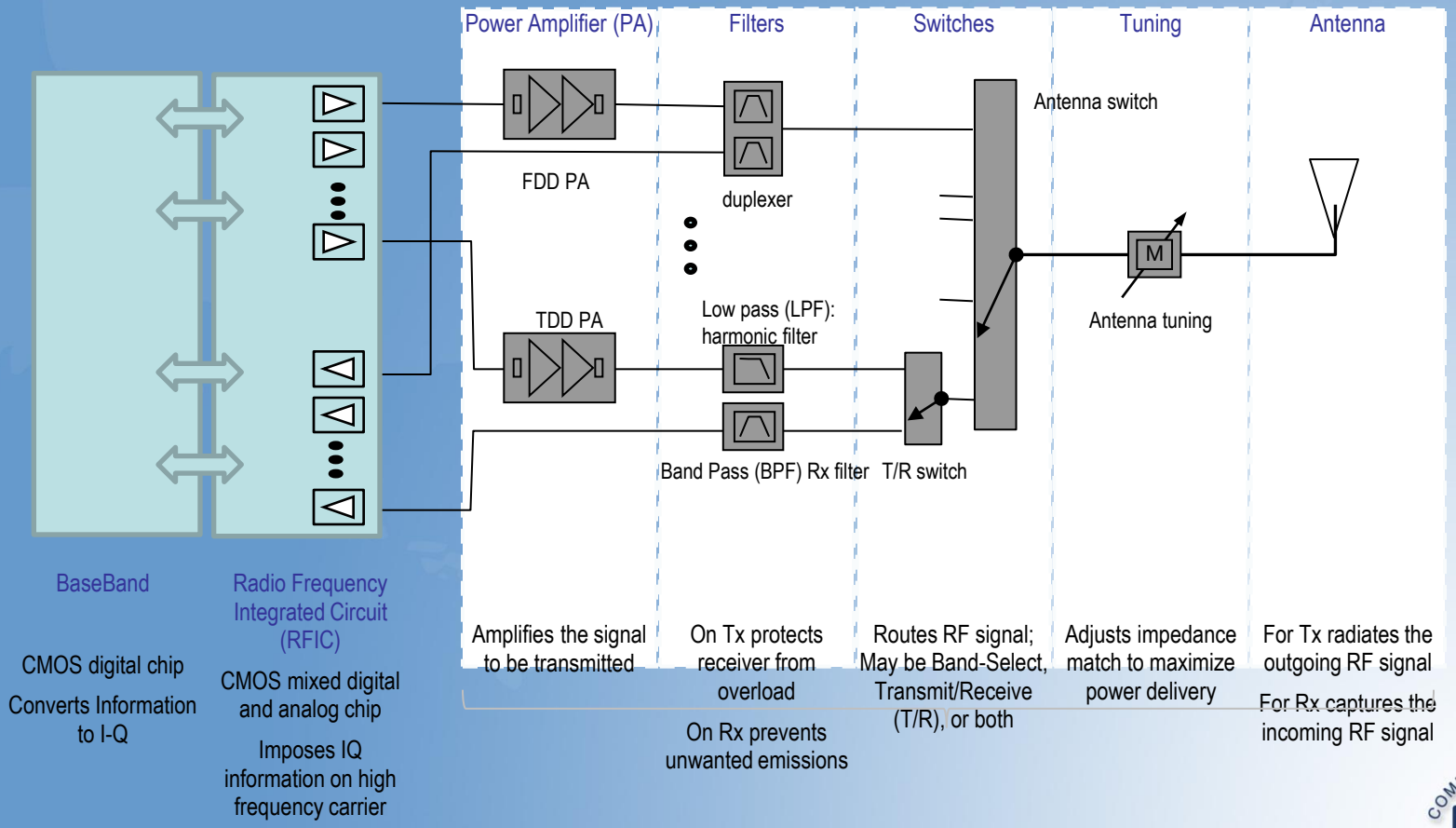
Handset Ecosystem– 1.8 billion units worldwide 2012 (IDC)



Giving Consumers What They Want

- Carriers, handset manufacturers and component suppliers work together to provide a continuous supply of new phones and features
- High volume drives optimized solutions and re-investment in R&D (development follows opportunity)
- Handset design balances multiband support, link budgets, numerous radios and GPS, OS/applications and battery life

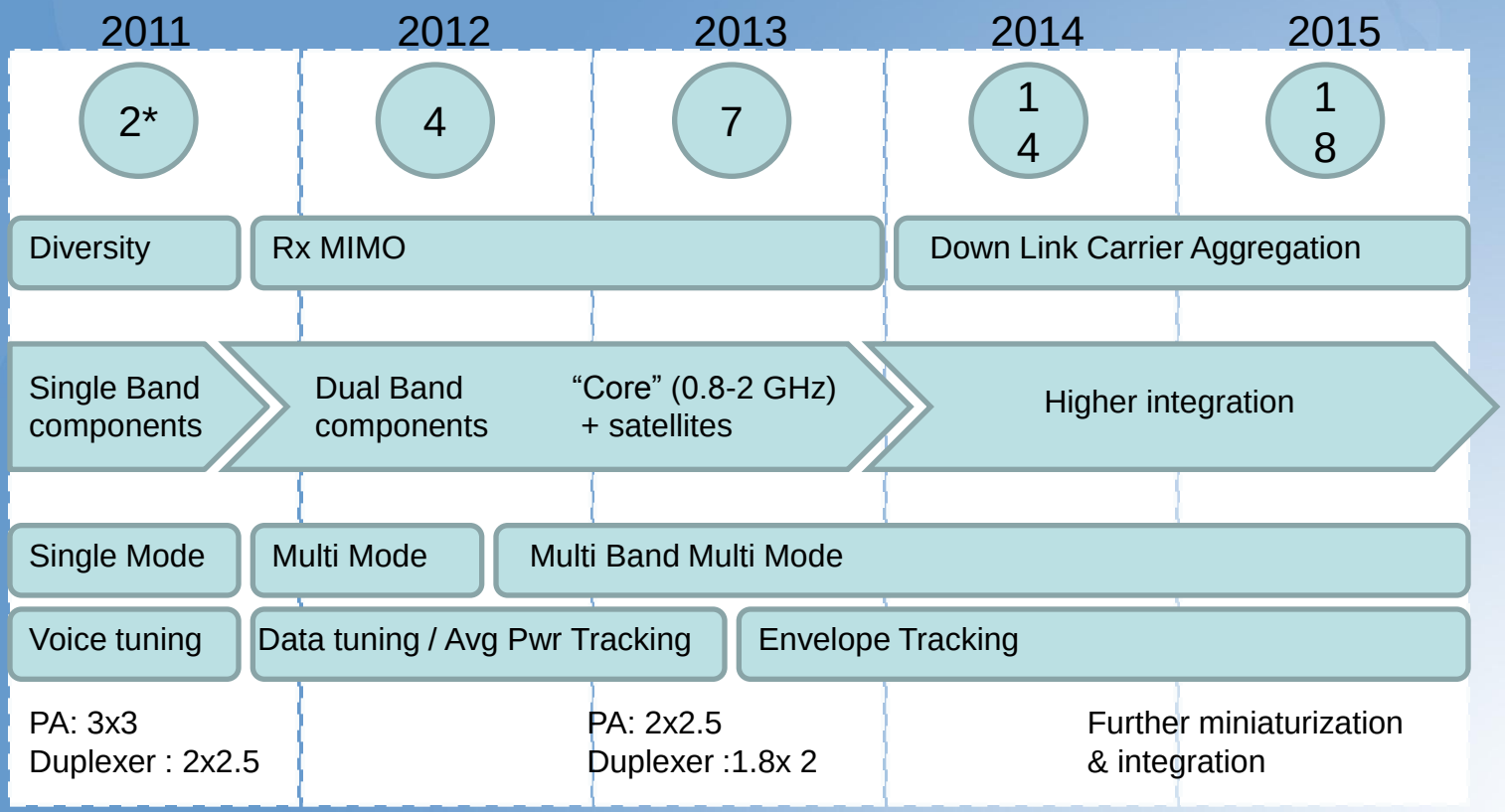
Simplified Block Diagram of the RF Front End



Discrete RF FE vs. Tunable RF FE

- Discrete RF FE continues to offer cost effective solution in mass market
- Tunable components have identified a few sweet spots in the RF FE
- More stringent RF requirements of new bands will impact the cost-performance effectiveness of Discrete/Tunable components
- Market forces promote innovation in both technologies which will benefit consumers

Handset RF Front End Component Roadmap

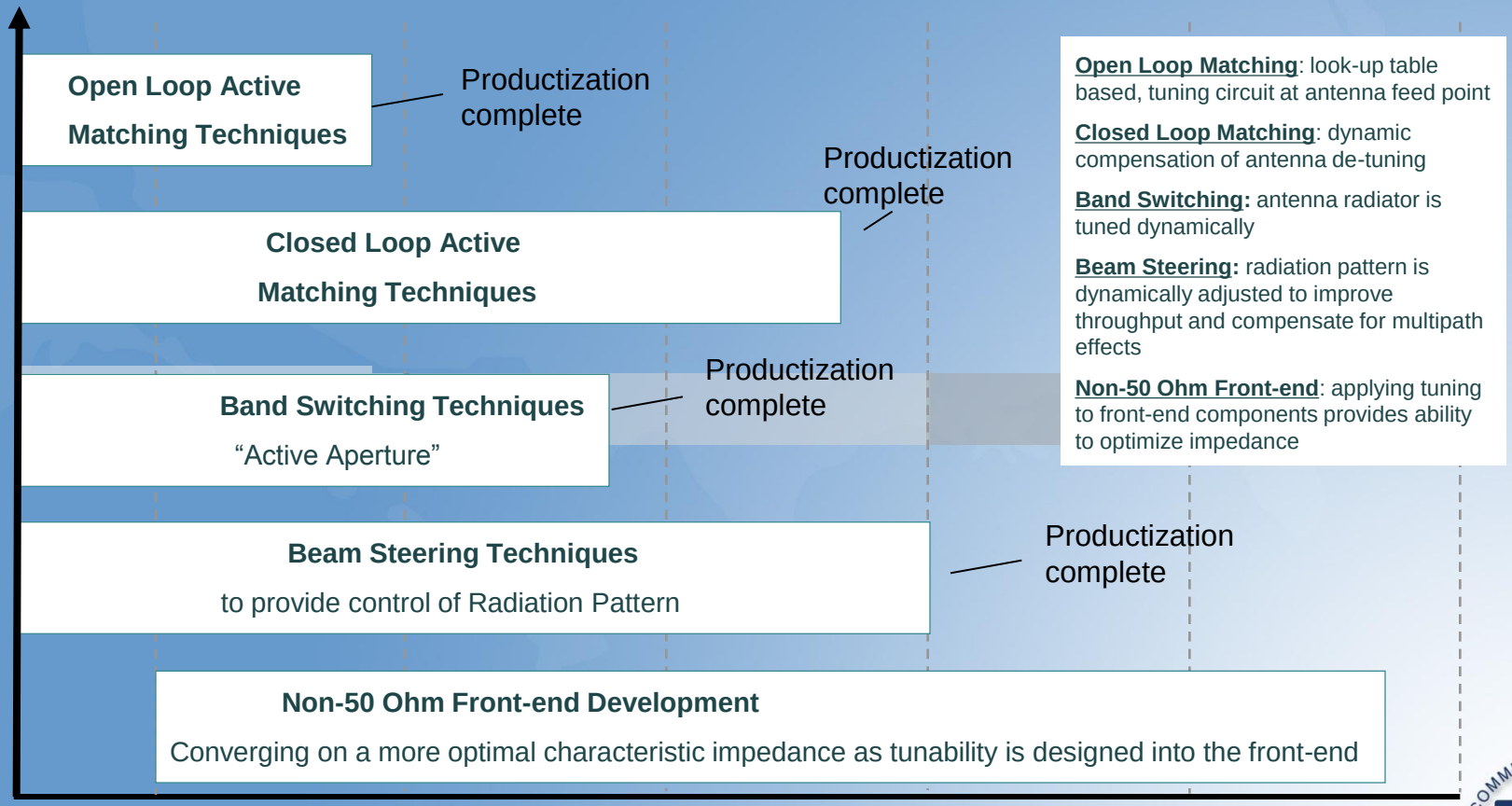


* Bands supportable per phone past QB GSM

Tunable Front End Roadmap

	2012	2013	2014	2015	2016
Tuning Areas	Antenna	Antenna(s) Notch Filter	Antennas Notch Filter LNA	Antennas Notch Filter LNA, PA	All
Building Blocks	Smaller Antennas Load Correct	CA and SVD filters	Fully tunable RX chain	Tunable RX + TX notches	Fully tunable RFFE
# bands (incl. QB)	7-10	10-13	15-18	20-25	As needed
Total Bandwidth supported by RFFE over all states (TX+RX)	1,2,3,4,5,7,8,13 ~ 750 MHz	1000 MHz	1250 MHz	1500 MHz	2000 MHz
Maximum instantaneous BW	20 MHz	40 MHz	40 MHz	40 MHz	80 MHz
# simultaneous bands (interband CA)	1	2DL	2DL	2RX+UL	2DL+UL 4DL
MIMO	2x1	2x1	2x1	2x2	4x2

Antenna Technology Roadmap for Mobile Devices



Open Loop Matching: look-up table based, tuning circuit at antenna feed point

Closed Loop Matching: dynamic compensation of antenna de-tuning

Band Switching: antenna radiator is tuned dynamically

Beam Steering: radiation pattern is dynamically adjusted to improve throughput and compensate for multipath effects

Non-50 Ohm Front-end: applying tuning to front-end components provides ability to optimize impedance

Recommendation #1 Spectrum Allocation

Recommendation:

- Allocate spectrum in block sizes that are multiples of 5 MHz where possible.
- Consider allocating unpaired spectrum for downlink only. This may include spectrum with geographic limitations or spectrum available part time to be used opportunistically.

Need:

- Trend is toward 5 MHz block sizes for mobile spectrum.
- Consistent and harmonized RF requirements reduce component counts and “special cases.”
- Current data usage is directionally asymmetric. Except in rare circumstances, downlink far exceeds uplink.
- Avoid harmonics in allocating downlink spectrum

Recommendation #1 Spectrum Allocation

Benefits:

Focused Design Investment– Consistent 5 MHz block size focuses the design roadmap.

Global Harmonization – Commonality in block sizes throughout the world increases opportunity for parts re-use and allows handsets to cover more bands.

Improved Spectrum Use – Opportunistic use of bands for downlink, even if not nationwide or always available provides better service for consumers and improves utilization of spectrum.

Next Steps

- Continue investigation of device testing process with respect to new innovations that are on the roadmap
- Develop actionable recommendations to result in a Handset Technology Roadmap
- Key characteristics of a technology roadmap
  - Timeline out to 10 years to inform spectrum allocation decisions
  - Impartial, technology agnostic assessment
  - Created and updated over time
  - Involve worldwide industry and academia
  - Spotlight improvements that yield greater spectrum efficiency
  - Express roadmap in terms meaningful to spectrum allocation

Technological Advisory Council

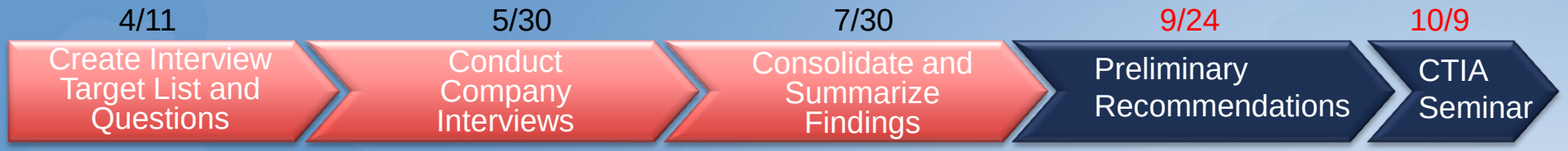
Machine to Machine Working Group

Table of contents

Draft

Friction Point Analysis Approach

Initiated survey of stakeholders in relevant sectors and targeted ~30 companies. To date the M2M TAC group has interviewed over a dozen companies and surveyed key issues impacting vertical opportunities: Regulator, Technical, Certification, Standards, Cost, and Others.



Participants

Company	Description	Vertical
Sprint	Network Operator	Multiple
verizon	Network Operator	Multiple
KORE	MVNO	Multiple
QUALCOMM	Devices and Platforms	Multiple
nest	Solution Provider	Home Automation
OnStar	Solution Provider	Telematics
EATON	Devices	Energy
SOUTHERN COMPANY	Utility	Energy
TELCARE	Solution Provider	Healthcare
* Sempra Energy	Utility	Energy
ERICSSON	HW and Platforms	Multiple
* Google	Solution Provider	Multiple
* at&t	Network Operator	Multiple

Questions Asked

1. How do you define M2M?
2. What do you believe are the key verticals?
3. What are some inhibitors to M2M growth?
   a. Regulatory (i.e. legacy regulations that inhibit M2M)
   b. Standards
   c. Technical
   d. Security
   e. Certification
   f. Other
4. What do you think the FCC should do that could help remove some of these inhibitors or create a catalyst for M2M growth?

Preliminary Recommendations

1. Allocate shared spectrum to M2M
2. Create M2M Service Registration Database
3. Create a numbering and addressing plan
4. Add a M2M Center of Excellence in the FCC's Wireless Bureau
5. Faster certification process for M2M devices
6. Create a 2G sunset roadmap for migration to 3G / 4G
7. Consider seeding the market to spur M2M innovation

CTIA (MobileCon)Seminar

Agenda

1. Introduction: Shahid Ahmed, M2M TAC Chair and Senior Executive at Accenture
2. Guest Speaker: Henning Schulzrinne, CTO, FCC
3. Panels
   - Panel 1: Standards, Technology and Certification:
   - Panel 2: Business and Policy:
4. Guest Speaker: Martin Cooper, Chairman, Dyna, LLC and Member of the FCC TAC

Preliminary Recommendation List

1. Allocate shared spectrum to M2M
2. Create M2M Service Registration Database
3. Create a numbering and addressing plan
4. Add a M2M Center of Excellence in the FCC's Wireless Bureau
5. Faster certification process for M2M devices
6. Implement 'Roadmap" for 2G sunset - migration to 3G / 4G
7. Seed the market to spur M2M innovation

Preliminary Recommendation 1: Allocate shared spectrum to M2M

- **Situation**
  - The 2.4 Ghz unlicensed band is over crowded and even 5 Ghz is experiencing noise interferrance.
  - New standards abandon this spectrum, e.g. 802.11ac/ad do not operate on 2.4 Ghz.
  - 60 Ghz is too short and 1.2-3.1 Ghz is just right for mobile.
- **Complication**
  - When new spectrum is opened for unlicensed devices, it eventually becomes crowed.
  - Radar Interference Avoidance Schemes such as DFS for Wi-Fi on 5 GHz had mixed results: it avoids interference but was not always enforced/implemented.
- **Recommendation**
  - Allow spectrum sharing with Commercial and Military Radar systems operating at frequencies from 1.2 – 1.4 Ghz and 2.7- 3.1 Ghz.
  - Creating special rules for M2M creates a bias against other unlicensed uses.
  - Require interference avoidance AND geo-location database registration. (higher cost)
  - Coordinate with the EU's effort to prevent competing recommendations.
- **Complexity to implement**
  - **Long Term**

Preliminary Recommendation 2: Create M2M Service Registration Database

- **Situation**
  - M2M is not measured adequately and there is little data available on what devices are in use. M2M devices are expected to grow exponentially with adoption of connected machines. There is also no easy way for M2M providers to use multiple networks or easily change networks.
- **Complication**
  - A registration database may increase the costs for implementation and perception of registration as a regulation may prevent cautious public/private investment.
  - Geo-location registration creates a bias towards devices that utilize infrastructure such as Cell Towers, GPS, or Wi-Fi.
- **Recommendation:**
  - Create a single secure nationwide (or regional) database administrator for M2M device registration similar to the local number portability (LNP) database administration.
  - The FCC will select a database administrator to provide an API. Companies can volunteer information without risking security of their networks.
- **Complexity to Implement**
  - **Short Term**

Preliminary Recommendation 3: Create a numbering and addressing plan

- **Situation**
  - Currently there are tens of millions of devices latched onto 2G networks with IPv4 addresses in place. As IPv4 approaches depletion, the M2M ecosystem will be looking for a solution for a new addressing schemes for the millions of additional devices scheduled to hit the market.
- **Complication**
  - A solution is required soon before Carriers decide on their own proprietary solution making it even more complicated for M2M devices to be introduced in the market and have broad acceptance across carriers.
- **Recommendation**
  - Develop an IPv6 migration path for the near, medium, and long term to meet requirements for M2M fixed and mobile applications (On-Net, Off-Net (i.e. Roaming).
- **Complexity to Implement**
  - **Medium Term**

Preliminary Recommendation 4: Add a M2M Center of Excellence in the FCC's Wireless Bureau

- **Situation**
  - M2M is not really represented at the FCC today as a separate industry.
  - The FCC has mentioned M2M but companies feel they have not provided enough input.
- **Complication**
  - A strong focus on M2M may create some fear in the industry that more regulations are coming for the M2M market and this might impact the growth of the M2M market.
- **Recommendation**
  - Organize a formal Center of Excellence within the FCC's Wireless Bureau to review this committees recommendations in more depth.
  - Return to the companies we interviewed with potential solutions in hand.
  - Use the definition of M2M provided by this group to help inform the public.
  - Form a long-term committee and forum for M2M companies to contact the FCC.
- **Complexity to Implement**
  - Short Term

Preliminary Recommendation 5: Faster certification process for M2M devices

- **Situation**
  - M2M device makers are challenged by varying regulations for regions and districts across the US and the rest of the world.
- **Complication**
  - The certification process is serial and companies cannot apply to FCC and FDA in parallel
  - Startups and device manufacturers lack the experience to develop radios & antennas that span multiple government organizations
- **Recommendation**
  - Create a Certification "Lite" process to reduce the cost and time to market a new device.
  - Allow carriers to deploy & test new devices on their network with Certification Lite.
  - Approve "Startup Districts" such as Silicon Valley & Austin to use Spectrum in a way to provide "Interference Tolerance" via registration.
  - Provide guidance tailored for M2M device manufacturers on the process for certifying a new device.
  - Request assistance from certification bodies, FDA, FAA, etc
- **Complexity to Implement**
  - **Short Term**

Preliminary Recommendation 6: Create a 2G sunset roadmap for migration to 3G / 4G

- **Situation**
  - National carriers have announced that they will be shutting down 2G existing wireless networks in the coming years. Some will be shut down as soon as 2016.
- **Complication**
  - Since there are tens of millions of 2G devices connected to these networks, existing devices will be forced to upgrade to 3G/4G modules. This will have a significant impact on the ROI for device manufactures who will be required to upgrade current device set. For many M2M players the 2G module prices have finally hit a point where they are seeing ROI (~$20.00 per module). The module prices for 3G/4G prices are double and quadruple (~$40.00 to ~$80.00) in some cases.
- **Recommendation**
  - Create a 2G roadmap for transitioning from 2G to 3G/4G. This will allow current M2M 2G device OEMs to plan accordingly .
  - FCC recommended window of time supporting legacy 2G infrastructure with migration guidance to LTE with IPv6 addressing. The desired result being to return spectrum while upgrading infrastructure, eliminating legacy.
- **Complexity to Implement**
  - **Medium Term**

Preliminary Recommendation 7: Consider seeding the market to spur M2M innovation

- **Situation**
  - Device OEMs report that moving to 3G/4G modules on a broad scale is a costly effort and believe with time and R&D the cost could come down. Carriers reported that the module cost is not coming down fast enough and this is having an impact on the market growth
- **Complication**
  - If nothing is done to help bring down the cost for the module set, this will have a direct impact on the ROI for Carriers who offer M2M services to their end users and who ultimately purchase the devices from the OEMs.
- **Recommendation**
  - Create a financial structure to entice software and hardware vendors to produce M2M modules at a low cost. Furthermore, providing new start ups/small businesses with financial incentives to create M2M modules at lower costs would aid in the effort to fuel the growth to the M2M market
- **Complexity to Implement**
  - **Medium Term**

Summary: Recommendations for Consideration

Recommendations	Benefits	Complexity
1. Allocate Shared Spectrum to M2M	• Reliability, Security, Ecosystem expansion • Increased QoS	High cost. Regulatory complexity. Long term.
2. Create an M2M Service Registration Database	• Interoperability, Roaming • Service Management	Maintaining database will be complex Standards
3. Create a Numbering and Addressing Plan	Standardized national solution to accommodate M2M growth	Will need coordination with carriers Standards
4. Add an M2M CoE in the FCC's Wireless Bureau	Sustained focus on M2M	Low complexity. Funding and right skillset needed
5. Certification "Lite" for M2M devices	• Reduce certification complexity and speed to market • Ensures "Safe network"	Coordination with carriers to define app and HW certification across various network types
6. Create a 2G Sunset Roadmap	• Clear roadmap investment decisions • Alignment with other TAC workstreams	Coordination with carrier roadmaps
7. Seed the Market to Spur M2M Innovation	• Innovation in strategic areas	Agreement on strategic areas to be funded


"Quick Win"
"Strategic Consideration"
Highest
Benefit
5 Certification Lite
6 2 G Sunset Map
Numbering and Addressing Plan 3
M2M Service Registration Database 2
7 Seed the Market
Allocate Shared Spectrum 1
4 M2M CoE at FCC
"Nice to Have"
"Not Worth the Effort"
Lowest
Less
Effort/Complexity
More

Preliminary - Implementation Timeline for Recommendations

Short Term: (6 to 12 months)

- #2 - Create M2M Service Registration Database
- #4 - Add a M2M Center of Excellence in the FCC's Wireless Bureau
- #5 - Faster certification process for M2M devices
- #7 (start) - Consider seeding the market to spur M2M innovation

Medium Term: (12 to 18 months)

- #3 - Create a numbering and addressing plan
- #6 – Create a 2G sunset roadmap for migration to 3G / 4G
- #7 (Implement) - Consider seeding the market to spur M2M innovation

Long Term (1): (18+ months)

- #1 - Allocate shared spectrum to M2M

Next Steps

1. Finalize recommendations - pick 2-3 quick-wins.
2. Develop an implementation plan with more detail around timing, dependencies, and level of effort
3. Present final set of recommendations to the broader industry

Appendix

TAC Wireless Apps and Services (M2M) Working Group

Name	Company	
Shahid Ahmed	Accenture	Workgroup Chair
Kevin Sparks	Alcatel-Lucent	
Bud Tribble	Apple	
Tom Evslin	Evslin Consulting	
Peter Bloom	General Atlantic	
Milo Mendin	Google	
Robert Zitter	HBO	
Deven Parekh	Insight Venture Partners	
Glen Tindal	Juniper	
Dave Tennenhouse	New Venture Partners	
Wesley Clark	Wesley K. Clark and Associates	
Greg Chang	Yume	
Walter Johnston	FCC Laison	

Draft

M2M Working Group Mission Statement

The TAC Machine to Machine (M2M) Working Group's mission is to accelerate the growth of the M2M market through education, policy development, and the reduction of barriers to entry for new entrants.

Objectives:

1. Identify legacy regulation that impedes growth in the new M2M paradigm
2. Provide guidance and recommendations for industry groups on standardization, privacy and security
3. Identify economic enablers that will act as catalysts for growth and job creation
4. Identify specific industry vertical issues and challenges
5. Identify metrics to gauge how the M2M market and traffic is growing and the impact it will have on wireless networks
6. Recommend actions to the FCC Technological Advisory Council
7. Facilitate the conversation with the M2M industry and community

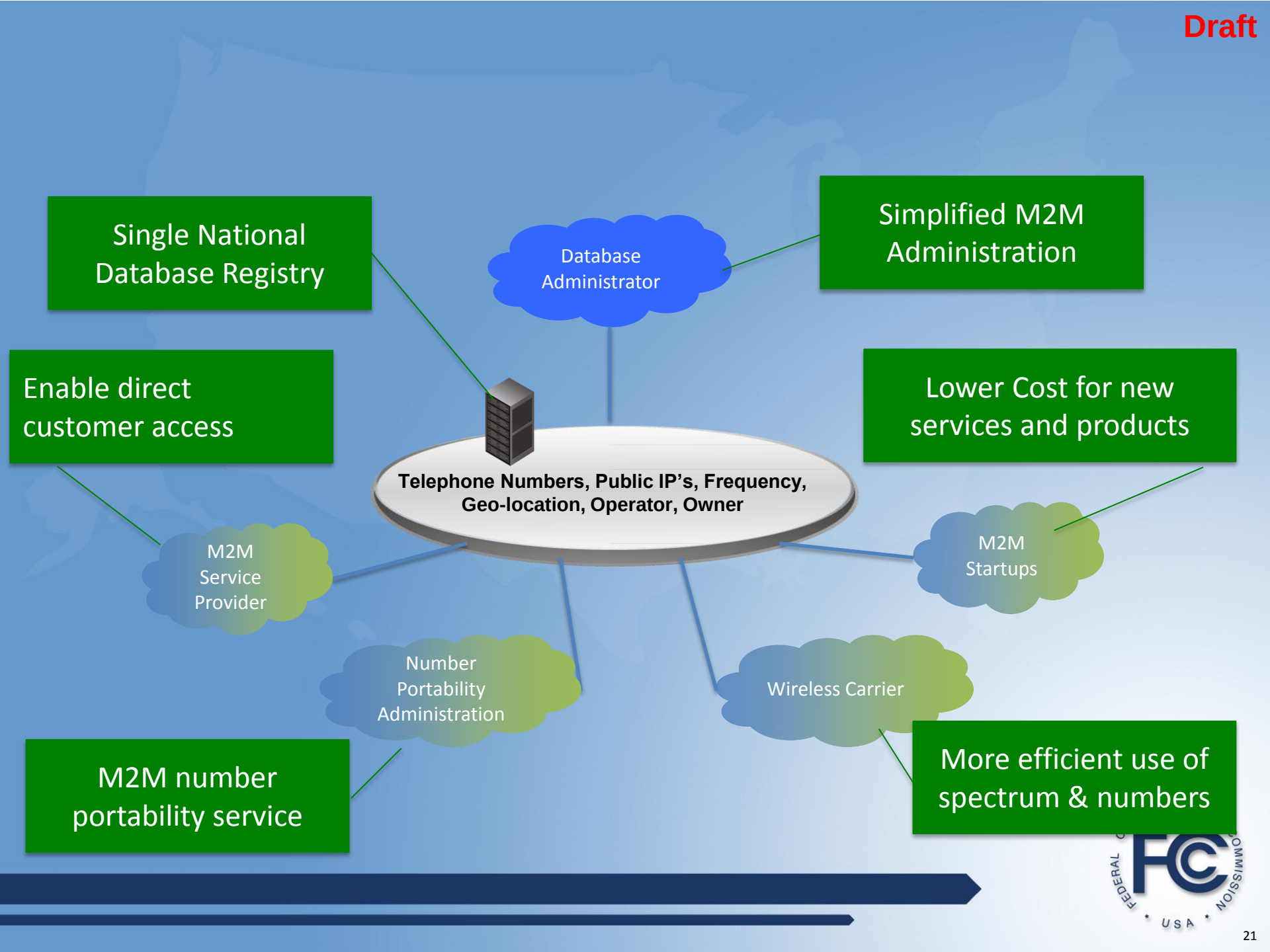
Initial Observations: Ideas Summary

1. Create a Certification Lite “Safe Network” to lower the cost for bringing solutions (devices and applications) to market.
2. Work as an industry to show technology roadmaps (e.g. 2G sunset) and pricepoints to guide application vendors
3. Provide a guidance on what defines “well behaved” applications
4. Provide exceptions for access to spectrum for critical infrastructure providers
5. For 2G sunset, consolidate into one network
6. Investigate feasibility of Spectrum set aside. Look at leveraging TV White Space
7. FCC to work with peers around the world to enable globalization
8. Rethink including M2M in the Universal Service Fund tax structure (FNPRM)
9. Consider seeding the market:
   - Incentives for Mobile Health, Wireless, or M2M in Phase 3 of the HHS-ONC’s meaningful use program.
   - Push funding for engineering and science education in K-12 and Higher Ed to make US more competitive in engineering and sciences

Recommendation #1

Frequency range		Bandwidth	Center frequency	Availability
6.765 MHz	6.795 MHz	30 KHz	6.780 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	14 KHz	13.560 MHz	
26.957 MHz	27.283 MHz	326 KHz	27.120 MHz	
40.660 MHz	40.700 MHz	40 KHz	40.680 MHz	
433.050 MHz	434.790 MHz	1.84 MHz	433.920 MHz	Region 1 only and subject to local acceptance
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz	Region 2 only
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz	
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz	
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz	
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz	Subject to local acceptance
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz	Subject to local acceptance
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz	Subject to local acceptance

Draft


Single National Database Registry
Database Administrator
Simplified M2M Administration
Enable direct customer access
Telephone Numbers, Public IP's, Frequency, Geo-location, Operator, Owner
Lower Cost for new services and products
M2M Service Provider
M2M Startups
Number Portability Administration
Wireless Carrier
M2M number portability service
More efficient use of spectrum & numbers

Technological Advisory Council

Receivers and Spectrum Working Group

24 September 2012

Working Group Members

- Lynn Claudy
- Richard Currier
- Dick Green
- Mark Gorenberg
- Dale Hatfield
- Greg Lapin
- Brian Markwalter
- Geoffrey Mendenhall
- Pierre de Vries
- Bob Pavlak
- Julius Knapp
- Dennis Roberson

Introduction

- Charter: The *Receivers and Spectrum* Work Group will tackle the issue of the role of receivers in ensuring efficient use of the spectrum and how to avoid potential obstacles to making spectrum available for new services

THEREFORE:

- Need to maximize the value of spectrum that comes from closer band packing, increased access, new services, device innovation…
- But increased density requires more care in optimizing the whole system, particularly transmitter vs. receiver trade-offs across band boundaries
- Goal to increase service density, reduce regulatory risk and encourage investment
  - By clarifying, up-front, who will bear the cost of mitigating harmful interference in specific situations – Interference Limits Policy and Receiver Standards Database
  - By applying new receiver technology to provide more flexibility to future spectrum allocations and more efficient spectrum utilization

Case Studies*

- Understanding selected spectral areas where receiver issues may be pronounced and / or where there is considerable interest in re-farming or sharing spectrum
- Areas of Focus for Working Group
  - Digital Television Bands
  - 2.4 GHz Unlicensed / Broadband Radio Service (BRS)/ Educational Broadband Service (EBS) / Terrestrial Mobile Satellite Service (MSS)
  - 3550 – 3650 MHz military radar and non-federal FSS earth stations
  - 2700 – 2900 MHz federal radars

*The 1755-1850 MHz band is also of interest but is being covered extensively by other groups at this time, especially CSMAC.

FCC Web Accessible Standards Repository

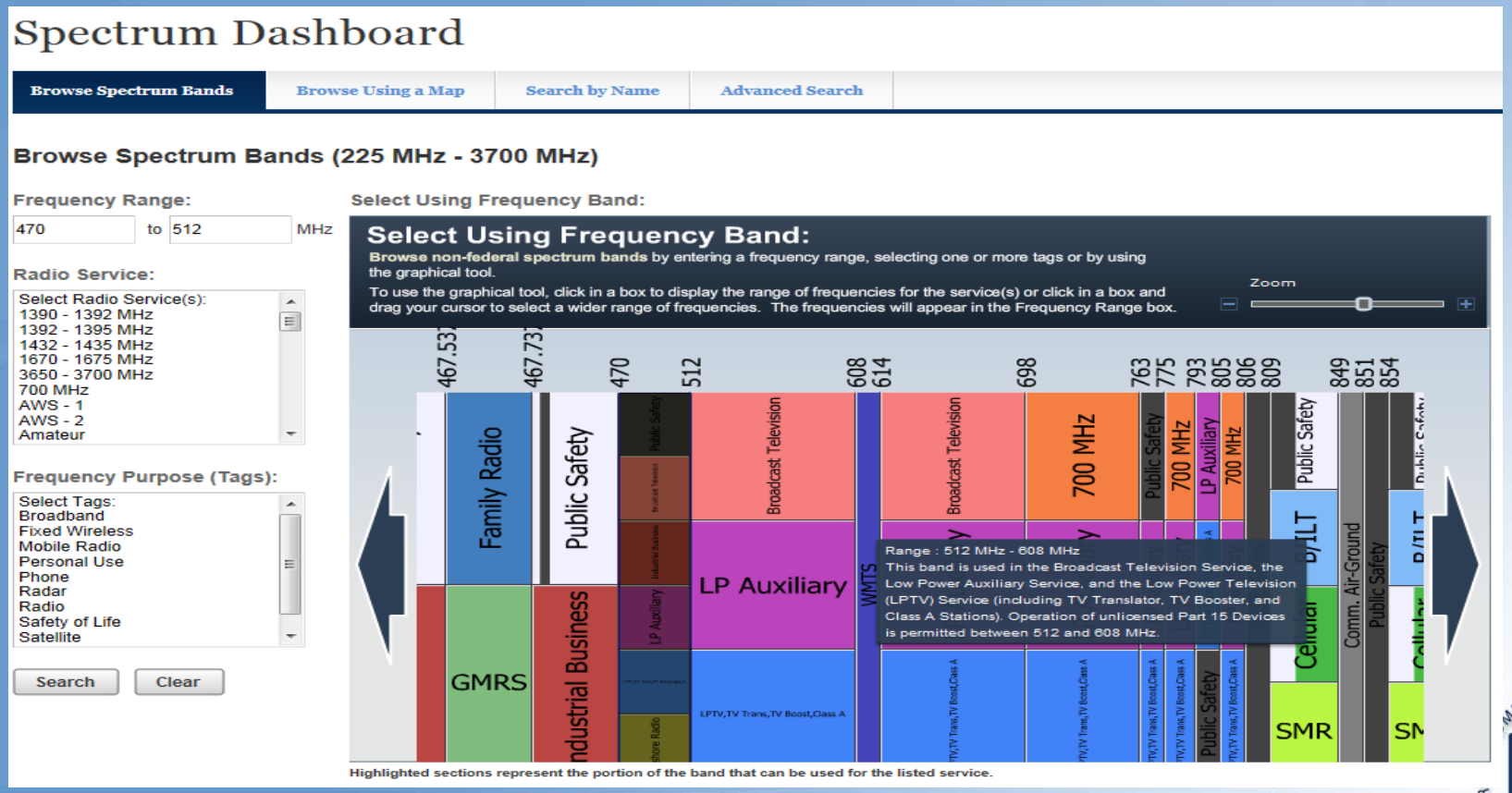
Motivation

- More efficient use of spectrum is leading to closer spectral juxtaposition of services by different users/industries necessitating known specifications for receiver immunity to interfering signals
- Industry and/or government receiver standards and recommended practices may exist (e.g. NTIA 2003 report on receiver spectrum standards) but are often unknown to spectrum suppliers and users operating in adjacent bands
- FCC website could serve as central information source for standards/recommended practices on receiver interference immunity characteristics for different services as a service planning tool

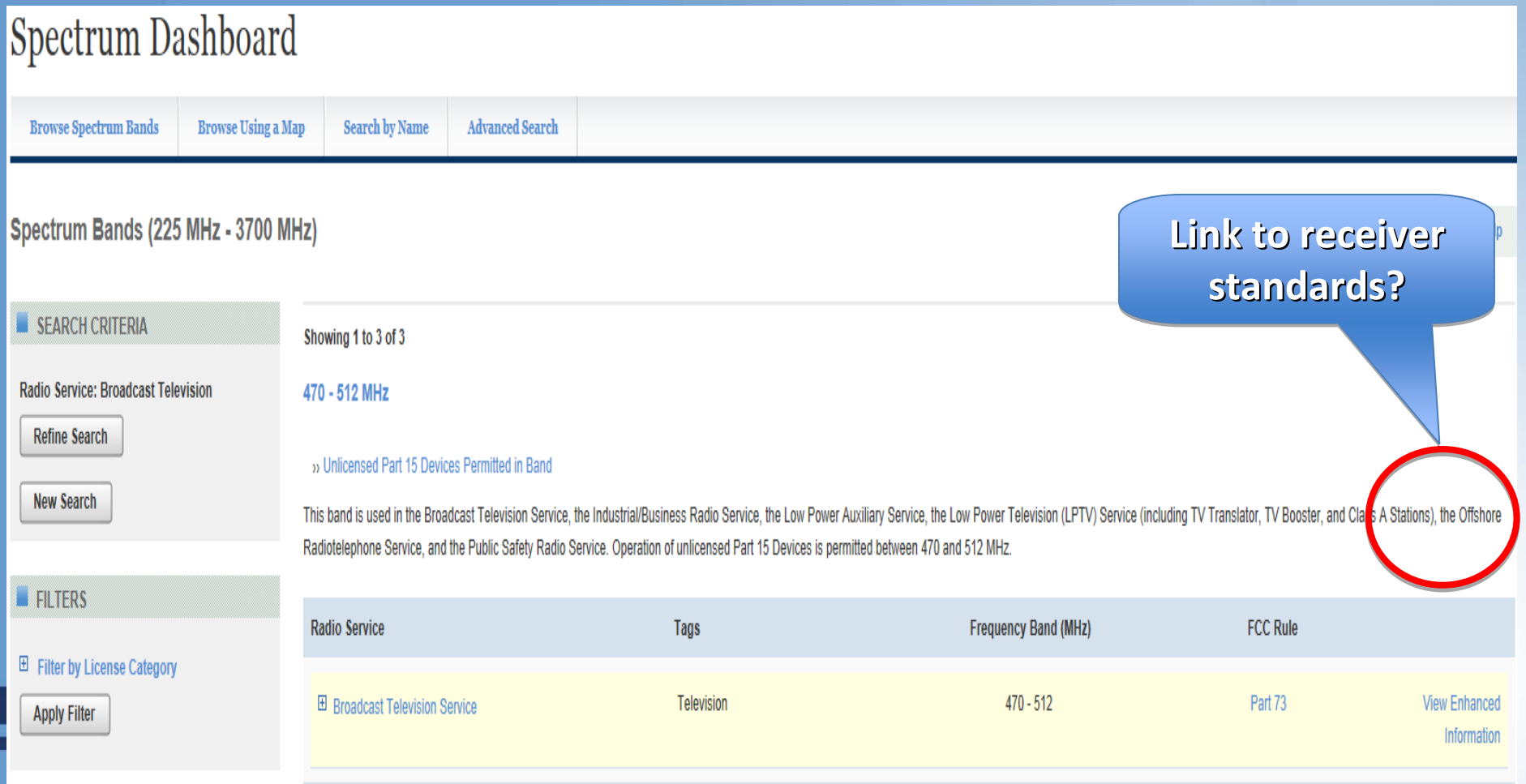
FCC Web Accessible Standards Repository

- **Example: TV receiver standards/recommended practices:**
  - Industry
    - Advanced Television Systems Committee (ATSC) Recommended Practices
    - Consumer Electronics Association (CEA) Standards and Guidelines
    - Society of Cable Telecommunications Engineers (SCTE) Standards
  - Government
    - 47 C.F.R. Part 15 Rules
    - NTIA Rules (Coupon Program for Digital-to-Analog Converter Boxes)
- **Other examples: LMR bands (TIA P25), cellular (3GPP)**

Link Receiver Standards to FCC Spectrum Dashboard?



Link Receiver Standards to FCC Spectrum Dashboard?



Receiver Technology Advancements

Impediments to be overcome

- Receivers expected to operate in changing and unknown future RF environments
- Reduce spectrum waste by minimizing guard bands and taboo reservations
- Limited dynamic range of front-end stage & A/D converter can be overloaded by strong interference
- Flexibility in front end filtering generally has a cost or performance penalty

Key Enablers

- Adaptive, low cost, low power, Software Defined Receivers (SDR) with over-the-air upgrades
- Ability to change receiver architecture over time through firmware upgrades for new services
- Low cost, low power consumption, high dynamic range, analog to digital conversion
- Low cost, low power consumption, digital signal processing
- New modulation waveforms that are more resistant to adjacent interference
- Advanced interference avoidance techniques including band switching and adaptive antennas

Desired Result

- Spectrum use no longer impeded by legacy receivers

Actionable Recommendations

- Multi-Stakeholder (MSH) group defines expectations for current & future minimum receiver performance levels by spectrum segment
- Incentivize “Future Proof”, upgradable receiver architectures

Interference Limits Policy

- Explicit, up-front statements of the adjacent band transmit power profile (interference as a receiver designer would see it) receivers need to tolerate before they can bring a harmful interference claim
- Defined as unwanted received signal strength profile that may only be exceeded at some small percentage of locations and times
- Until now, expectations of receiver performance have almost always been implicit, leading to downstream conflicts due to differing understanding of requirements (e.g. ATC rules - GPS / LightSquared, etc.)
- Unlike receiver performance mandates, interference limits do not mandate receiver performance, leaving system design to industry's discretion
- Unlike interference temperature, interference limits do not use interference ceilings to impose co-channel sharing

Interference Limits Implementation

- Identify band boundaries where interference limits can be tested
  - Focus where boundary separates reasonably different services with prospect of intensified use
  - E.g. cellular/broadcast; licensed/unlicensed broadband; cellular/satellite…
- Use MSH process to work out boundary issues/implementation choices
  - MSH organizations focus on future do not operate under or pursuant to formal government authority
  - Power derives from (a) respect for their processes (e.g., openness, fairness, inclusiveness, transparency, and flexibility) and (b) the quality of their outputs (e.g., standards, best practices, and recommendations)
  - MSH organizations have significant advantages and much of the governance of the Internet has been carried out by such organizations
  - In the best case would agree on parameter values that the FCC could then bless
  - Hopefully they could at least agree on relevant parameters (but not values) and methods;
  - Value even if it just (a) identified critical issues and/or (b) laid out areas of consensus vs. areas where FCC needs to make public interest trade-off decision
- FCC should monitor progress of MSH process
  - Ensure that the record developed provides a thorough basis for NOI and/or NPRM
  - Represent interests of future licensees and stakeholders

Recommendations and Ongoing Work

- Actionable Recommendations:
  - Implement FCC Dashboard enhancement to include receiver standards
    - Issue FCC public notice on web accessible standards repository to secure receiver standards information
  - Initiate Interference Limits Policy trial in appropriate band(s)
    - Identify industry owners for multi-stakeholder (MSH) process
    - Encourage Industry to takes steps to organize MSH groups
- Ongoing Work:
  - 2.4 GHz WiFi receiver testing
  - Develop recommendations on receiver technology incentives (Japanese model evaluation, NSF sponsored research…)

Discussion