Agenda

- **Review of 2012 and Introduction of Work Groups - Tom Wheeler**
- **Overview of Work Program for Cybersecurity Executive Order - David Turetsky**
- **TAC discussion of proposed Work Groups**
  - **Purpose**
  - **Potential Objectives**
  - **Issues**
- **Work Group Assignments**

FCC Actions on TAC Recommendations – 2011

- FCC has taken action on eight recommendations:
- (Jointly) Municipal Race-to-the-Top Program ; Best Practices/Technology Outreach to State & Local Governments
  - FCC cited the TAC recommendations in its April NOI on Broadband Acceleration and is collecting data on best practices
  - NOI record closed September 30. FCC staff reported to the Chairman on recommended next steps, including timelines and necessary resources.
- Broadband Infrastructure Executive Order (#2)
  - Executive Order 13616 signed to accelerate commercial broadband deployment on federal land
- Promote Small Cell Deployment (#8)
  - Following initial FCC/GSA talks, TAC recommended holding a workshop to explore implementing public & private building deployment
  - FCC organized workshop in October

FCC Actions on TAC Recommendations – 2011

- FCC took immediate action on four recommendations:
- Prepare for PSTN Transition & Stranded Investments
  - FCC hosted a workshop on the PSTN transition Dec. 14.
- New Metrics to Measure Broadband Network Quality
  - FCC hosted a workshop on Public Safety network reliability in Sept.
  - FCC worked with ISPs as part of Broadband Measurement Program (i.e. Measuring Broadband America effort) to gain agreement on and, in the longer term, standardize metrics for broadband service
- Facilitate a National IPv6 Transition
  - Established IPv6 working group in CEA
  - Incorporating IPv6 metrics in broadband measurement program
  - Coordinating with other federal agencies on IPv6 deployment issues
- Develop Materials Highlighting Benefits of Broadband Deployment in Private Buildings (#11)
  - FCC staff in WCB and CGB have been assigned to come up with ideas for materials by January 2012

FCC Actions on TAC Recommendations - 2011

- FCC is waiting on further analysis on three recommendations:
- Advocacy for Rapid Tower Siting (#3)
  - "Shot Clock" order held on appeal. Statutory legislation passed covering collocation/antenna replacement timelines
- Model an Online Deployment Coordination System (#5)
  - Referred to Interagency Advisory Committee
- Develop Consensus on Spectrum Efficiency Categories and Metric Definitions (#10)
  - Order on VoIP outage requirements, Measuring Broadband America Program established metrics with industry/academia and submitted standards proposal to IETF and Broadband Forum, CAF program requires service metrics to be met

FCC Actions on TAC Recommendations – 2012

- Recommendation on small cell deployment
  - NPRM on small cell use of 3.5 GHz spectrum 12/12/2012 Commission Meeting
- Recommendation on Spectrum Efficiency
  - Receiver group white paper on interference policy

TAC 2012 Activities

- Workshop on spectrum efficiency and receivers – 3/12
- Forum on Future of Wireless Broadband Plans – 7/12
- Forum on M2M at CTIA 10/12
- Met with industry trade groups, companies, government experts, academics and organized a number of sub-groups to pursue recommendations on specific issues
- PSTN Group white paper on VoIP interconnection
- Receivers and Spectrum Working Group
  - Developed case studies to identify issues
  - Proposed FCC standards/receiver interference website
  - Proposed strategies to define expectations for received evolution and accommodate change
  - Proposed policy for Interference limits

Work Groups/FCC Staff

- **Spectrum Frontiers**
  - Michael Ha
  - John Liebovitz
- **Expanding Wireless COTS**
  - Walter Johnston
  - Chris Heltzer
- **Spectrum and Receiver Performance**
  - Julius Knapp
  - Bob Pavlak
- **Resiliency in a Broadband Network**
  - Henning Schulzrinne
  - Rebekah Goodheart
- **Communications Infrastructure Security**
  - Ahmed Lahjouji
  - Greg Intoccia

Spectrum Frontiers

- The challenges for obtaining new spectrum remain formidable. Options to clear large areas of spectrum are limited, leading to proposals for spectrum sharing. Remaining spectrum options in currently attractive bands (5 GHz and below) involve smaller bandwidth allocations which are often encumbered by technical or legacy issues. Future spectrum options may also involve higher frequencies such as the upper microwave into the millimeter wave band where bandwidth is greater but propagation is more limited. Technical innovation may mitigate some of these issues included unpaired allocations. Multiband radios may permit the aggregation of smaller spectrum blocks. New components and standards may support operation at frequencies presently thought undesirable. Improvements in receiver performance or changes in policy may allow operation in spectrum bands presently encumbered by legacy operations. Looking to the future, what spectrum bands have the potential to become the new “beachfronts”. What technical or policy changes will be needed to make this realizable? What timeframes might be anticipated in making this happen?

Expanding Wireless COTS

- The reality of mobile broadband is stimulating a massive investment in both licensed and unlicensed infrastructure to support its growth. At the same time, new data driven applications are emerging seeking either separate spectrum or infrastructure for deployment. Diverse applications such as Smart Grid, Intelligent Transportation System, public safety, and specialized enterprise applications are seeking wireless infrastructure specific to their needs. Even allowing for the benefits that dedicated wireless infrastructure may present for specific applications, the economic challenge to build new wireless infrastructure at scale is daunting and, at minimum, will impede the rapid deployment of applications. How can the multibillion dollar investment in current commercial broadband systems and products be better leveraged to support these "mission critical" vertical uses? What are the major challenges in supporting QOS, reliability, security, cybersecurity and other issues that such applications require? What technical evolution will be required to broaden the use of current and evolving infrastructure? What policy initiatives should be developed to leverage utilization of existing wireless infrastructure? How can greater use of COTS technology increase the potential for spectrum sharing? What models might be developed to support increased utilization from the current service provider centric model(s) to virtual models or wholesale variants?

Spectrum and Receiver Performance

- In 2012, the TAC identified that it is critical for interference management policies to include receivers as part of the overall equation in making more spectrum available. The work group will provide support as the Commission considers the TAC recommendations, including the TAC white paper, possible implementation of the Interference Limits Policy, establishment of a multi-stakeholder group, identification of spectrum bands for initial application of this policy, enforcement and various other matters related to receiver performance. The group, in consultation with the full TAC and the FCC staff, will also explore and potentially make recommendations in several other areas towards improving access to and the efficient use of the radio spectrum. These areas may include: emerging technologies that offer improved interference rejection and greater reuse of spectrum, new interference cancellation technologies; software defined radio technology that may be used to future-proof against harmful interference as new services are introduced over time; methods for analyzing interference risk on a statistical basis as opposed to worst case assumptions; and, evaluation of the noise floor, its impact and steps the FCC might take to improve it. The work group may choose from among these or other related areas based on consultation with the full TAC and the FCC staff.

Resiliency in a Broadband Network

- Recent disasters have focused attention on the importance of our communications infrastructure as well as its limitations. Traditional methods of protecting communications infrastructure have focused on hardening and redundancy. In a future environment of a wireline broadband infrastructure and wireless broadband macro, micro, pico and femtocells, new approaches may be possible. The transition from the PSTN to a broadband IP based infrastructure may provide alternative mechanisms and architectures to sustain communications in emergencies. In a future environment where communication services span texting, voice communications, emergency services, Internet access and video services, what should be the goals for a resilient communications infrastructure? What are the implications of different categories of services (e.g. normal voice traffic, 911, M2M, etc.) in a resilient environment? What should be the goals for portability of service capabilities during emergencies? What capabilities will be required to leverage network services to best support the needs of the public and public safety during a crisis?

Communications Infrastructure Security

- The evolution of the nation's communications infrastructure towards a broadband IP-based network is occurring at an ever faster rate. This evolution includes an environment in which Cloud-based services are increasingly relied upon as substitutes for desktop applications, and where attributes such as mobility, identity, and presence influence both the capability to access data as well as the context in which data may be presented. In an emerging era where consumers and business will rely upon cloud services for critical functions, what are the key areas of concern for security? As these issues relate to the communications infrastructure on the nation, how can we best develop awareness of these issues and ensure that the ongoing evolution incorporates industry best practices, ensuring adequate protection for key services.

CYBERSECURITY DEVELOPMENTS:

EXECUTIVE ORDER (E.O. 13636) and PRESIDENTIAL POLICY DIRECTIVE (PPD-21)

Presentation by DAVID TURETSKY
Chief, Public Safety & Homeland Security Bureau
Federal Communications Commission

OVERVIEW

- Background
- Executive Order (EO)
- Presidential Policy Directive (PPD)

BACKGROUND

- **May 2009**
  - President declared digital infrastructure a “strategic national asset”
  - recognition that protecting networks/computers that deliver oil, gas, power, and water are a national security priority.

- **2011-2012** – Administration mad cybersecurity legislative proposal and Congress considers possible legislation

- **Feb 2013** - President signed an Executive Order to strengthen the cybersecurity of the nation’s critical infrastructure

  – Executive Order ensures federal agencies take steps to secure our critical infrastructure from cyber attack, as a down-payment on expected further legislative action
  – Broad agreement on need
  – For the most part, it incorporates approaches supported by business leaders, researchers, and members of Congress

- **Feb 2013** – Presidential Policy Directive released at the same day Executive Order was signed

EXECUTIVE ORDER (EO)

- **Intended to strengthen the Federal government's partnership with critical infrastructure to address cyber threats in two ways:**
  - **New cybersecurity information sharing programs to provide threat and attack information to U.S. companies.**
  - **Development of a Cybersecurity Framework.**

EO Cybersecurity Information Sharing

- Strengthening Governmental-Critical Infrastructure (CI) partnership by information sharing (Section 4):
  - New cybersecurity information sharing programs will provide both classified and unclassified threat and attack information to U.S. companies.
  - Intended to increase the volume, timeliness and quality of cyber threat information shared with the private sector:
    - Requires Federal agencies to produce unclassified reports of threats to U.S. companies
    - Expands the Enhanced Cybersecurity Services program, enabling: near real time sharing of cyber threat information to assist participating critical infrastructure companies in cyber protection efforts.

EO Cybersecurity Framework

- Strengthening governmental-critical infrastructure (CI) partnership by development of Cybersecurity Framework (Section 7):
  - Directs the National Institute of Standards and Technology (NIST) to lead the development of a framework of cybersecurity practices to reduce cyber risks to CI
  - NIST will work with industry to develop the framework, relying on existing proven international standards, practices, and procedures – applicable to CI
  - Cybersecurity Framework will enable technical innovation by providing guidance that is technology neutral and enables the CI sectors to benefit from a competitive market

EO Additional Provisions

- DHS will promote adoption of the Cybersecurity Framework, and will create incentives designed to promote participation in the Program. (Section 8)
- DHS must establish a consultative process to coordinate improvements to cybersecurity of CI. This will include advice from critical infrastructure owners and operators; Sector-Specific Agencies; and independent regulatory agencies [including FCC]. (Sec.6)

EO Additional Provisions

- Identification of CI at greatest risk (Section 9):
  - DHS will use a risk-based approach to identify CI where a cybersecurity incident could result in catastrophic effects on public safety, economic or national security.
    - In doing so, DHS shall use the consultative process, including drawing on the expertise of Sector-Specific Agencies and other relevant agencies.
  - Within 90 days of publishing preliminary Framework (not yet established), agencies with responsibility for regulating the security of CI shall submit a report to President stating if agency has authority to establish requirements based on Cybersecurity Framework to address cyber risks to critical infrastructure.
  - If current regulatory requirements are insufficient, within 90 days of publishing the final Framework, agencies with responsibility for regulating the security of CI shall propose prioritized, risk-based, efficient, and coordinated actions.

EO Additional Provisions

- Protections of Privacy and Civil Liberties (Section 5):
  - Executive Order includes strong privacy and civil liberties protections based on the Fair Information Practice Principles, and execution of the Order will be reviewed by governmental privacy officers.
  - Agencies required to incorporate privacy and civil liberties safeguards in their activities.
  - Safeguards will be based upon applicable privacy and civil liberties policies, principles, and frameworks.
  - Agencies will conduct regular, public assessments of privacy/civil liberties impacts of their activities.

EO Additional Provisions

- Voluntary Promotion of Cybersecurity Framework (Section 10)
  - Executive Order establishes a voluntary program to promote the adoption of the Cybersecurity Framework.
  - DHS will work with Sector-Specific Agencies to develop a program to assist companies with implementing the Cybersecurity Framework and to facilitate adoption.

EO Additional Provisions

- Regulatory agencies will use Cybersecurity Framework to
  - assess their cybersecurity regulations;
  - determine if existing requirements are sufficient; and
  - determine if any existing regulations can be eliminated
- If existing regulations are ineffective or insufficient, agencies will propose new regulations in consultation with their regulated companies.
- *Independent regulatory agencies are encouraged to leverage the Cybersecurity Framework to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities*

PRESIDENTIAL POLICY DIRECTIVE

Released same day as EO

- Intended to "strengthen and maintain secure, functioning, and resilient critical infrastructure against both physical and cyber attacks" – including the assets, networks, and systems that are vital to public confidence and the nation.
- Focus is on "resiliency and security," broader than cyber
- Clarifies Federal roles/responsibilities across the Federal government for CI;
- Seeks to improve information sharing;
- Shows Federal government's commitment to partner with CI owners/operators to secure CI against threats.
- Updates previous focus on protecting CI against **terrorism** to protecting, securing, and making the nation's CI more **resilient to all hazards** – including natural disasters, manmade threats, pandemics, and cyber attacks.

PPD: Strategic Imperatives

- **Three strategic imperatives** drive the Federal approach to strengthen CI:
  - Clarify Federal relationships – Refine and clarify functional relationships across Federal Government to advance unity of effort to strengthen CI security and resilience;
  - Identify baseline requirements – Enable effective information exchange by identifying baseline data and systems requirements for the Federal government; and
  - Ensuring informed CI decisions – Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.
- **Accomplishment of imperatives will be driven through successful completion of key deliverables.**

PPD First Strategic Imperative

- Clarify Federal relationships:
  - Refine and clarify functional relationships across Federal Government to advance unity of effort to strengthen CI security and resilience
  - As part of structure, there will be two national critical infrastructure central functions operated by DHS:
    - one for physical infrastructure
    - one for cyber security
  - Both will function in an integrated manner as focal points for CI partners to obtain situational awareness and actionable information

PPD Second Strategic Imperative

- Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government
  - This includes an ability to facilitate a timely exchange of information and information that allows for the development of situational awareness during incidents.
  - Greater information sharing must be done while respecting privacy and civil liberties.

PPD Third Strategic Imperative

- Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.
- This will include capability to collect and assess threat and hazard information to
  - aid in prioritizing assets and managing risks to critical infrastructure;
  - anticipate cascading impacts; and
  - support incident management and restoration efforts related to CI

PPD: Agencies' Roles

- DHS provides strategic guidance, coordinator of Cybersecurity Framework.
- Roles for other agencies include: DOS, DOJ, DOI, Intelligence Community, GSA, NRC, and FCC
- Sector-Specific Agencies (SSAs) are to leverage their expertise and relationships to promote the Cybersecurity Framework, do incident response, and report on implementation to the President.
- SSAs include:
  - Communications: Department of Homeland Security
  - Emergency Services: Department of Homeland Security
  - Information Technology: Department of Homeland Security
  - Transportation Systems: Department of Homeland Security and Department of Transportation

PPD: FCC Role

The FCC is described as having "specialized or supporting functions" with the following responsibilities:

"[T]o the extent permitted by law, [the FCC] is to exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends."