Agenda

10:00 am Welcome and Opening Comments: Attorney General Brian Frosh
10:05 am SME Presentation: “5G and Cybersecurity”
11:00 Council Business
11:05 Discussion & Approval of the 21 January 2020 Meeting Minutes
11:15 am Updates: Attorney General Frosh

11:20 am Subcommittee Reports
  ◦ Law, Policy, and Legislation (Senator Susan Lee)
  ◦ Cyber Operations and Incident Response (Secretary Leahy)
  ◦ Critical Infrastructure (Markus Rauschecker)
  ◦ Education and Workforce Training (Senator Katie Fry Hester)
  ◦ Economic Development (Bel Leong-hong)
  ◦ Public Awareness and Outreach (Dr. Anton Dahbura for Sue Rogan)

11:55 Other Business
12:00 Adjourn
5G & Cybersecurity


Why 5G requires new approaches to cybersecurity

Racing to protect the most important network of the 21st century

Tom Wheeler and David Simpson - Tuesday, September 3, 2019
Hope or Hype?

“The race to 5G is on and America must win”
President Trump April 2019
Five Facts About 5G

**5G is Revolutionary:** From Hardware to Software built on IP – New Network Topology

**5G is Evolutionary:** Designed to be Progression from 4G – Will Roll Out in Steps

**5G is Not Transformational, per se:** How the network is used is what is transformational

**5G is Spectrum Dependent:** Allocation of New Spectrum and Reuse of Old

**5G is a Cybersecurity Risk:** Distributed Software-based vs. Centralized Hardware-based
What’s All the Fuss??

The Landscape of 5G
5G will differentiate itself by delivering various improvements:

- **10x**
  - **Decrease in latency:** Delivering latency as low as 1 ms.
  - **Connection density:** Enabling more efficient signaling for IoT connectivity.
  - **Experienced throughput:** Bringing more uniform, multi-Gbps peak rates.

- **3x**
  - **Spectrum efficiency:** Achieving even more bits per Hz with advanced antenna techniques.

- **100x**
  - **Traffic capacity:** Driving network hyper-densification with more small cells everywhere.
  - **Network efficiency:** Optimizing network energy consumption with more efficient processing.
A Standard Confused With A Service
“The cybersecurity threat now poses an existential threat to the future of the nation”
President’s National Security Telecommunications Advisory Committee, November 2019

A Different Huawei Threat
Focus on Huawei Distracts from Other Efforts

Five Ways 5G Expands Cyber Risks
- From Centralized, Hardware-based Switching to Distributed, Software-defined Routing
- Virtualized Activities Built on IP and Well-Known OS
- Network Managed by Software That is Vulnerable
- Expansion of Antennas are New Physical Threat
  Dynamic Spectrum Sharing is New Functional Threat
- Tens of Billions of Attached Devices
Leaders won’t just be “Deciders” ... they will need to establish & evolve “Decision Operations”

- Information Intensive/Data Rich
  - Privacy & Security Expectations
- Internet of Things – Sense, Process, Act
- Compute, Storage & Communications move to the edge
  - Machine Learning ➔ Artificial Intelligence
  - Policy matters (Algorithms, Analytics, ...)

*Industrial-era public policy that makes rulemaking activity cumbersome is not optimized for 5G enabled ecosystems*
Decision Operations... must be actively managed ‘to the left’ of the decisions

Elements for AI “Decision Operations”

- **Data Analysis**
  - Inspecting, Cleansing, Transforming & Modeling Data with the goal of discovering useful information, suggesting conclusions and supporting Decision Making
  - Ford’s Chief Data Officer – *new data science hires “understand the math” but don’t know how to frame problems!*

- **Information Systems & Software**
  - IT, Industrial Controls, SCADA, AI & Machine Learning .... a growing “system of systems” challenge

- **Security**

- **Physical, Environment, Reputation, Cyber, Supply Chain, Insider Threats, International, National, Human & Machines .... Proactive Risk Reduction**
Smart Buildings will evolve to physical nodes in a larger AI enabled functional chain.
Smart Cities will employ sensor & actuator grids anticipating needs & executing dynamic risk reduction.
Smart Planning Activity will need to move to the left ... for every vertical
Critical Infrastructure sectors will manage their own 5G slices & utilize data from other CI slices.

*Identify & actively manage data/risk interdependencies between Critical Infrastructure (CI) sectors*
5G Cyber Risk Responsibility & Accountability not well defined

Cyber Risk RACI will be a major challenge for Public Safety jurisdictions in a 5G world
Public Safety Moving to Internet Protocol Comms

- Citizen Smart Phones
- PSAP Next Generation 9-1-1 (ESINets)
- AT&T FirstNet and Vz Public Safety Private Core
- Wireless Emergency Alerts
- Broadcast Emergency Alert System (ATSC 3.0)
- 5G Public Safety Slices
- Geo-tagging, Face Recognition, Data Retention, Evidentiary Standards, Privacy (direct & aggregated), Cybersecurity ...

... now exponentially expand the number of data points ... while moving citizen risk reduction expectations to the left
Public Safety Cyber Risk Considerations

- Bad cyber-actors incentive to overcome defenses is typically greater than the incentive to improve the protection
- Industry stakeholders fear exposing internally identified risk factors at precisely the time when sharing information about attacks would be of greatest value for a collective defense

... Cyber threat actors with Public Safety attack objectives have been better organized than the Public Safety entities they seek to attack ... they only have to be right once
Cyberspace Solarium Commission:

“The digital connectivity that has brought economic growth, technological dominance, and improved quality of life to nearly every American has also created a strategic dilemma. The more digital connections people make and data they exchange, the more opportunities adversaries have to destroy private lives, disrupt critical infrastructure, and damage our economic and democratic institutions.”
Cyberspace Solarium Commission:

“The digital connectivity that has brought economic growth, technological dominance, and improved quality of life to nearly every American has also created a strategic dilemma. The more digital connections people make and data they exchange, the more opportunities adversaries have to destroy private lives, disrupt critical infrastructure, and damage our economic and democratic institutions”
Beyond Technology - Behaviors

Market Forces Alone Won’t Provide Protections
  • ROI vs. Cyber
  • Protections of One Undone by Inaction of Another

Consumers Don’t Consider Cyber – Thus Suppliers Don’t

2019 Report Council of Economic Advisors:
“underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment”
Cyber Duty of Care for Companies

- New 5G Network, New Challenge
- Forethought vs. Afterthought
- From Lag Indicators to Leading Indicators
- Entire Ecosystem Not Just Big Companies
- Reverse Chronic Underinvestment
- Quit “Looking Through a Straw” – Implement AI
New Regulatory Paradigm

- Industrial Model No Longer Sufficient
  - *Stable Markets with Stable Technology Permitted Slow, Rules-Based Oversight*
- Joint Standards with Enforcement Oversight
- Consumer Information/Transparency
- Certification of Connected Devices
- Close Supply Chain Gaps
- Reengage With International Bodies
Maryland & Local Public Safety Leader Cyber Roles

- **Define:**
  - 5G Transformation Objectives
  - Identify new Cyber Universe (IT, OT, Mission Systems, Cognitive)
  - Current Risk Thresholds
- **Establish:**
  - Governance & Accountability (Cyber Risk RACI)
  - Objective Cyber Risk Thresholds
  - Cyber Budget
  - Internal Controls
  - Cyber Audit Program
- **Iteratively Assess, Appreciate & Address Cyber Risk**
- **Lead Cyber Incident Response & Recovery**
- **Build Smart**
  - 5G Foundation – communication/storage/compute at the edge
  - Move from DevOps to DevSECOps
  - Align Supply Chain Risk Reduction goals with Resiliency Goals
  - Embed Cyber into all Contracts and Service Obligations
• **Play to our strengths:**
  • We missed the 5G H/W moment ... lead the 5G S/W evolution
  • Incent U.S. 5G & 5G Ecosystem Patents
  • Stimulate Open-source Radio Access Network (O-RAN) Development (Think Linux for 5G SDN)
  • Build prototype ‘secure’ smart city implementation (Think SELinux)
  • Partner with U.S. Cybercom, NSA, NIST, FTC and the FCC
• Reimagine & create an agile state regulatory approach for continuous Cyber risk reduction
• Consider a Baltimore-U.C. Cybercom Prototype Smart City Initiative ... gain congressional advocacy to ‘jump start’ municipal readiness for 5G Critical Infrastructure Initiative
Questions?
Business Agenda

11:00 Discussion & Approval of the 21 January 2020 Meeting Minutes

11:05 am Updates: Attorney General Frosh

11:20 am Subcommittee Reports

- Law, Policy, and Legislation (Senator Susan Lee)
- Cyber Operations and Incident Response (Secretary Leahy)
- Critical Infrastructure (Markus Rauschecker)
- Education and Workforce Training (Senator Katie Fry Hester)
- Economic Development (Bel Leong-hong)
- Public Awareness and Outreach Dr. Anton Dahbura for Sue Rogan

11:55 Other Business

- Next Meeting: October 15, 2020

12:00 Adjourn
Thank You