



---

# **Federal Communications Commission Public Safety and Homeland Security Bureau**

## **Cybersecurity and Public Safety Communications**

**APCO Broadband Summit  
May 5, 2015**

**Erika E. Olsen  
Senior Legal Counsel  
Public Safety and Homeland Security Bureau**



# Public Safety Networks in Transition



- Often driven by commercial technologies and consumer expectations
  - IP Transitions
  - LTE
  - Texting, social media, streaming video, app culture
- Increased integration of broadband data by public safety
  - Commercial offerings
  - FirstNet



# Challenges



- Identifying Resources
- Budget and Personnel Constraints
- Complex IT and Management Interdependencies
- Diverse Sensitive Systems



# Tools



- NIST Cybersecurity Framework
- NIST Cybersecurity Workforce Framework



# CSRIC WG 4



- Develop voluntary mechanisms which give the FCC and the public assurance that communications providers are taking the necessary steps to manage cybersecurity risks across the enterprise;
- Such assurances:
  - (1) can be tailored by individual companies to suit their unique needs, characteristics, and risks (i.e., not one-size-fits-all),
  - (2) are based on meaningful indicators of successful (and unsuccessful) cyber risk management (i.e., outcome-based indicators as opposed to process metrics), and
  - (3) allow for meaningful assessments both internally (e.g., CSO and senior corporate management) and externally (e.g., business partners).
- Demonstrate how communications providers can reduce cybersecurity risks through the application of the NIST Cybersecurity Framework or an equivalent construct.
- Develop implementation guidance to help communications providers use and adapt the Cybersecurity Framework developed last year by the National Institute of Standards and Technology (NIST).



# Lessons



- Holistic approach to risk management
- Collaboration and accountability
  - Information sharing
  - Flexibility
- FCC considering next steps



*Cybersecurity is an enterprise-wide, strategic risk management matter, rather than a narrow information technology or network management domain.*



# TFOPA WG1



- Considering specific cybersecurity risk management strategies for the NG911 and transitional environment
- Leveraging NIST, CSRIC and related work as applied to this sector
- Understanding of challenges specific to public safety environment
- Work is ongoing



# Workforce



- The National Cybersecurity Workforce Framework classifies the typical duties and skill requirements of cybersecurity workers.
- The Framework organizes cybersecurity into seven high-level Categories, each comprised of several Specialty Areas. Each of the 31 Specialty Areas contains standard tasks and KSAs needed to successfully complete those tasks.
- May provide particular challenges in public safety environment







---

# Thank You!

Contact Information:

Telephone: (202) 418-2868

E-mail: [erika.olsen@fcc.gov](mailto:erika.olsen@fcc.gov)