

# Marsha MacBride

Chief of Staff,  
Office of Chairman Powell

Director, Homeland Security Policy Council

Federal Communications Commission



# Homeland Security Sectors

---

Agriculture

Chemical Industry

Emergency Services

Food

**Information and  
Telecommunications**

Transportation

Public Health

Banking and Finance

Defense Industrial Base

Energy

Government

Postal and Shipping

Water

- All other sectors rely on the Information and Telecommunications sector

# FCC's Homeland Security Mission

---

- Evaluate and strengthen measures for protecting the Nation's communications infrastructure.
- Facilitate rapid restoration of that infrastructure in the event of disruption.
- Develop policies that promote access to effective communications services by public safety, public health, and other emergency personnel in emergency situations.

# FCC's Homeland Security Focus

---

- Interagency and Industry Partnerships
- Infrastructure Protection
- Communications Reliability
- Public Safety Communications
- Spectrum Policy
- New Technologies

# FCC's Homeland Security Partnerships

**Executive Office of the President**

**Sister  
Agencies**



**Federal  
Communications  
Commission**



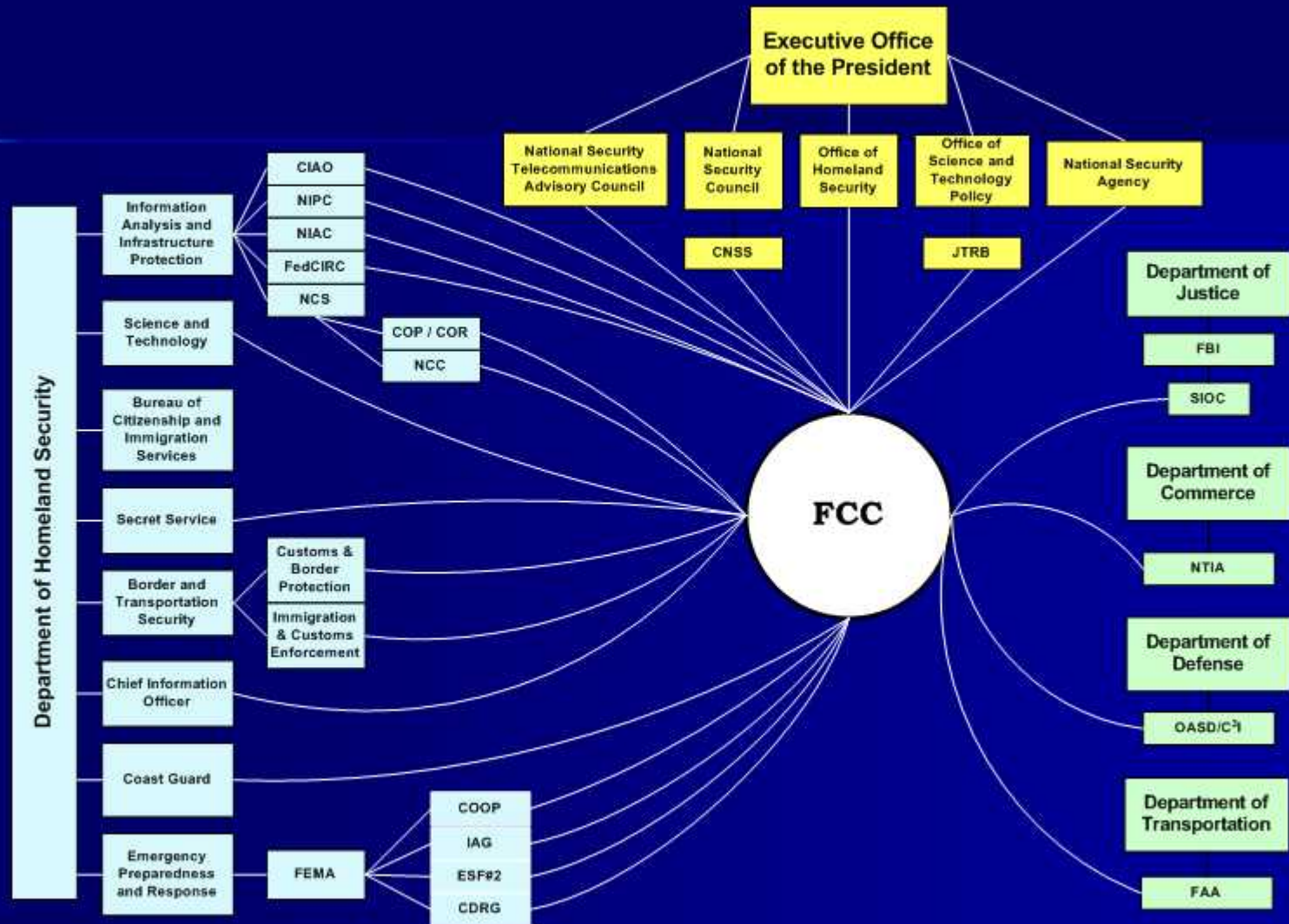
**State and  
Local  
Governments**

**Federal  
Advisory  
Committees**

**Industry and  
Trade  
Organizations**



# Interagency Efforts: View from the FCC



# FCC Partnership with NCS/NCC

---

- The National Communications System (NCS) continues to be our strongest partner in our efforts to coordinate industry response to a network outage or attack.
- FCC is assisting NCS in promoting its efforts to improve emergency communications through the Telecommunications Service Priority (TSP), Government Emergency Telecommunications System (GETS) and Wireless Priority Access (WPAS) programs.

# NCC Membership





# FCC's Homeland Security Focus

---

- Interagency and Industry Partnerships
- **Infrastructure Protection**
- Communications Reliability
- Public Safety Communications
- Spectrum Policy
- New Technologies

# Infrastructure Protection

---

- FCC rechartered our Network Reliability and Interoperability Council (NRIC VI) federal advisory committee in January 2002 to focus on homeland security issues. ([www.nric.org](http://www.nric.org))
- FCC created a new Media Security and Reliability Council (MSRC) federal advisory committee in March 2002 to address broadcast, cable and satellite homeland security issues. ([www.mediasecurity.org](http://www.mediasecurity.org))

# Network Reliability and Interoperability Council

---

- First chartered in 1993. NRIC has a 10-year history of improving network reliability.
- Expanded membership in 2001 charter.
- December 2002 - Delivered best practices for securing the physical and cyber networks.
- March 2002 - Delivered best practices for service restoration and disaster recovery.

# NRIC Best Practices – Summary of Results – Dec `02

---

## Creation of Best Practices to Fortify and Harden Networks

- Systematic assessment of communications infrastructure vulnerabilities
- Creation of an Integrated Vulnerabilities – Threats – Best Practices Framework

## Physical Security Best Practices

- 200 Best Practices/3,500 Participant-Hours in working meetings
- Sample Best Practices:
  - Network Operators should ensure intra-office diversity of all critical resources including spares, power, timing source and signaling leads (e.g., SS7).
  - Where feasible, Network Operators should provide both physical and logical diversity of critical facilities links (e.g., nodal, network element). Particular attention should be paid to telecom hotels and other choke points.

## Cybersecurity Best Practices

- 103 Best Practices/Over 3,000 Participant-Hours in working meetings
- Sample Best Practices:
  - Equipment deployed in insecure or remote locations should include intrusion detection mechanisms that enable stored critical information to be destroyed upon detection of attack.
  - Network Operators and Service Providers should know and validate who you are accepting routing information from to protect against global routing table disruptions.

# NRIC Best Practices – Summary of Results March '03

---

## Creation of Best Practices to Facilitate Recovery from Attacks

- Business Continuity
- Disaster Recovery and Service Restoration
- Communications Industry Support for Public Safety Community

## Business Continuity

- 103 Best Practices
- Sample Best Practice:
  - Service Providers, Network Operators and Equipment Suppliers should consider establishing a designated Emergency Operations Center. This center should contain tools for coordination of service restoral including UPS, alternate means of communications, maps, and documented procedures to manage business interruptions and/or disasters.

## Service Restoration

- Over 150 Best Practices in the area of Physical Security and Cybersecurity
- Sample Best Practices:
  - If the Domain Name System (DNS) server is under attack, 1) Implement reactive filtering to discard identified attack traffic, if possible 2) Rate-limiting traffic to the DNS server complex 3) Deploy additional DNS server capacity in a round-robin architecture 3) Utilize Denial of Service (DoS) tracking methods to identify the source(s) of the attack.

## Communications Industry Support for Public Safety Community

- Recommendations and best practices to support communications needs of public safety personnel in an emergency

# Media Security and Reliability Council

---

- MSRC Objectives:
  - Ensure the security and sustainability of broadcast and multichannel video programming distribution (MVPD) facilities.
  - Ensure the availability of adequate transmission capability during natural disasters or man-made attacks.
  - Facilitate the rapid restoration of broadcast and MVPD services in the event of significant disruptions.
- Two Working Groups:
  - Public Communications and Safety.
  - Communications Infrastructure Security, Access and Restoration.
- Work Plans:
  - Monthly meeting schedule to develop best practices.
  - Initial recommendations to be presented at May 2003 council meeting.
  - Additional recommendations released on an ongoing basis.

# FCC's Homeland Security Focus

---

- Interagency and Industry Partnerships
- Infrastructure Protection
- **Communications Reliability**
- Public Safety Communications
- Spectrum Policy
- New Technologies

# Communications Reliability

---

- Promote NRIC and MSRC best practices.
- Measure success of best practices implementation.
- Enhance and improve NRIC and MSRC best practices as we learn more.
- Partner with National Communications System (NCS) to promote TSP, GETS, and WPAS.



# FCC's Homeland Security Focus

---

- Interagency and Industry Partnerships
- Infrastructure Protection
- Communications Reliability
- **Public Safety Communications**
- Spectrum Policy
- New Technologies

# Public Safety Communications

---

- Provide access to new spectrum in support of Public Safety.
  - 700 MHz, 4.9 GHz
- Ensure 911 and E-911 implementation.
  - April 29, 2003 launch of E911 Coordination Initiative
- Ensure interoperability of Public Safety radio systems.
- Coordinate with DHS on Project SAFECOM.
- Resolve Public Safety interference at 800 MHz.

# FCC's Homeland Security Focus

---

- Interagency and Industry Partnerships
- Infrastructure Protection
- Communications Reliability
- Public Safety Communications
- **Spectrum Policy**
- New Technologies

# Spectrum Policy

---

- FCC Spectrum Policy Task Force
  - Focused on facilitating access to spectrum by removing regulatory impediments and improving interference avoidance.
  - Concluded that spectrum currently set aside for public safety use should remain subject to “command-and-control” model to ensure provision of essential life-and-safety services.
  - Proposed providing public safety users flexibility to lease spectrum capacity during lower-use periods to other users because of high variability of public safety use.
  - Short and long-term implementation ongoing.

# FCC's Homeland Security Focus

---

- Interagency and Industry Partnerships
- Infrastructure Protection
- Communications Reliability
- Public Safety Communications
- Spectrum Policy
- **New Technologies**

# New Technologies

---

## FCC Actions

- Foster implementation of new technology
  - Ultra-Wideband (UWB)
  - Telemedicine
  - Software Defined Radios (SDR)

# Conclusion

---

The FCC is just one component of a complex network of public and private partnerships dedicated to improving the security and reliability of our Nation's telecommunications infrastructure.

# Contacting The FCC

---

- You may contact the FCC Homeland Security Policy Council at **Homeland@fcc.gov.**
- Or contact the Policy Council Deputy Director Linda Blair directly at (202) 418-7450.
- **[www.fcc.gov/homeland](http://www.fcc.gov/homeland)**

