

FCC

Small and Rural Carrier Webinar

June 17, 2019



Public Safety and Homeland Security Bureau
Office of Communications Business Opportunities
Wireline Competition Bureau



Agenda

- I. Welcome and Introduction
- II. Small Business Cybersecurity - Network Protection
- III. Communications Security, Reliability and Interoperability Council (CSRIC) Recommendations for Small Carriers on Transition to NG9-1-1
- IV. Introduction to Network Outage Reporting System (NORS) & Disaster Information Reporting System (DIRS)
- V. Supply Chain Notice of Proposed Rulemaking

***Questions? Send an email to networkresiliencywebinar@fcc.gov ***



Small Business Cybersecurity – Network Protection



Sanford S. Williams, Esq., MBA, B.S. Engr.

Director

Office of Communications Business Opportunities



Background

- Economic loss due to cybercrime is predicted to reach \$3 trillion by 2020, and 74% of the world's businesses can expect to be hacked in the coming year.¹
- In 2018, the global cost of cyber security reached \$600 billion dollars.²
- America's 30 million small businesses create about two out of every three new jobs in the U.S. each year, and more than half of Americans either own or work for a small business.³
- The number of cyber attacks on small businesses is rising according to a 2018 study -- with 67 percent experiencing a cyber attack and 58 percent experiencing a data breach in the last 12 months.⁴

1. World Economic Forum, *Safeguarding our Planet* (January 22-25, 2019), <https://www.weforum.org/events/world-economic-forum-annual-meeting/stream/day-4-6acd005c-8dda-44d7-9ed5-6a9fcbea6609>.

2. Amy Jordan & Andy Bates. *Helping Small Businesses Fight Cybercrime Benefits the Global Ecosystem* (May 8, 2019), <https://www.weforum.org/agenda/2019/05/helping-small-businesses-fight-cybercrime-benefits-the-global-ecosystem/>.

3. United States Small Business Administration, *SBA Open Government Plan*, <https://www.sba.gov/document/report--sba-open-government-plan> (last visited June 7, 2019).

4. Ponemon Institute, *2018 State of Cybersecurity in Small & Medium Size Businesses – 2018 at 1* <https://keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf>



Background

- The aforementioned 2018 Ponemon Study states -- 60% of small businesses surveyed cited a negligent employee or contractor as being the root cause for a breach, compared to 37% pointing to an external hacker.
- Respondents indicated their two biggest password-related pain points are having to deal with passwords being stolen or compromised (68%) and employees using weak passwords (67%).
- Small businesses continue to struggle with insufficient personnel and budget. 74% of respondents note they do not have the appropriate personnel and budget (55%) to effectively mitigate cyber risks.
- Yet, nearly half of respondents (47%) say they have no understanding of how to protect their companies against cyber attacks.



The Small Biz Cyber Planner 2.0 is an Online Resource to Help Small Businesses

1. Train employees in security principles

- *Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior.*

2. Protect information, computers, and networks from cyber attacks

- *Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.*

3. Provide firewall security for your Internet connection

- *A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.*



The Small Biz Cyber Planner 2.0 is an Online Resource to Help Small Businesses

4. Create a mobile device action plan

- *Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password-protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.*

5. Make backup copies of important business data and information

- *Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.*



The Small Biz Cyber Planner 2.0 is an Online Resource to Help Small Businesses

6. Control physical access to your computers and create user accounts for each employee

- *Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.*

7. Secure your Wi-Fi networks

- *If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router, so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.*

8. Employ best practices on payment cards

- *Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. Add additional security obligations pursuant to agreements with your bank or processor.*



The Small Biz Cyber Planner 2.0 is an Online Resource to Help Small Businesses

9. Limit employee access to data and information, limit authority to install software

- *Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.*

10. Passwords and authentication

- *Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.*



FCC and Other Federal Resources

- FCC Resources
 - FCC Cyber Planner: <https://www.fcc.gov/cyberplanner>
 - FCC Cybersecurity Tip Sheet: <https://docs.fcc.gov/public/attachments/DOC-306595A1.pdf>
 - FCC OCBO Cybersecurity Page: <https://www.fcc.gov/general/cybersecurity-small-business#block-menu-block-4>
- Other Federal Resources
 - Small Business Cybersecurity Corner: <https://www.nist.gov/itl/smallbusinesscyber>
 - Cybersecurity Resources Road Map: <https://www.us-cert.gov/sites/default/files/c3vp/smb/DHS-SMB-Road-Map.pdf>
 - Cybersecurity for Small Business: <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity>
 - Managing a Business: <https://www.sba.gov/managing-business/cybersecurity>
 - Cyber Crime: <https://www.fbi.gov/investigate/cyber>



Communications Security, Reliability and Interoperability Council (CSRIC) Recommendations for Small Carriers on Transition to NG9-1-1



Ryan Hedgpeth

Telecommunications Systems Specialist, Cybersecurity and
Communications Reliability Division

Public Safety and Homeland Security Bureau



CSRIC VI Recommendations on the Transition to NG9-1-1

- [CSRIC's](#) mission is to provide recommendations to the FCC to ensure, among other things, security and reliability of communications systems, including telecommunications, media, and public safety.
- CSRIC VI reviewed how service providers support the public safety community's transition to NG9-1-1 and developed recommended measures to improve both legacy 9-1-1 and NG9-1-1 systems as well as actions the FCC could take to encourage the private sector to detect or deter threats to 9-1-1 before they reach the ESINet perimeter.⁵
- These resulting recommendations identify tools that are already available and not burdensome to implement as well as offer a set of best practices for carriers and 9-1-1 service providers.

5. Communications Security, Reliability and Interoperability Council, Recommendations for 9-1-1 System Reliability During the NG9-1-1 Transition- 2019 at 67, <https://www.fcc.gov/file/15312/download>.



CSRIC VI Recommendations for Small Carriers on NG9-1-1 Implementation

- The FCC tasked CSRIC VI with recommending an “NG9-1-1 readiness checklist” for small carriers analogous to the one the Task Force on Public Safety Answering Point Architecture (TFOPA) developed for PSAPs.
- CSRIC VI developed recommendations for the FCC on:
 - *what small carriers should do to be ready on time to deliver their 9-1-1 traffic in an NG9-1-1 compatible manner;*
 - *what economic disadvantages, if any, may impede small carriers in the implementation of NG9-1-1; and*
 - *what barriers to implementation, if any, the FCC should address.*⁶

6. Communications Security, Reliability and Interoperability Council, Final Report - Small Carrier NG9-1-1 Transition Considerations – 2018 at 11, <https://www.fcc.gov/files/csric6wg1sept18ng911reportdocx>



CSRIC VI Recommends Four Key Transition Activities

CSRIC VI Identified Four Key Transition Activities:

- 1. Understanding the plans and timeline for the state/regional 9-1-1 Authority.*
- 2. Identifying the technology changes that need to be implemented on the network.*
- 3. Identifying organizational impact such as training and job duties.*
- 4. Understanding the interoperability requirements with the ESI-net and other carriers.*



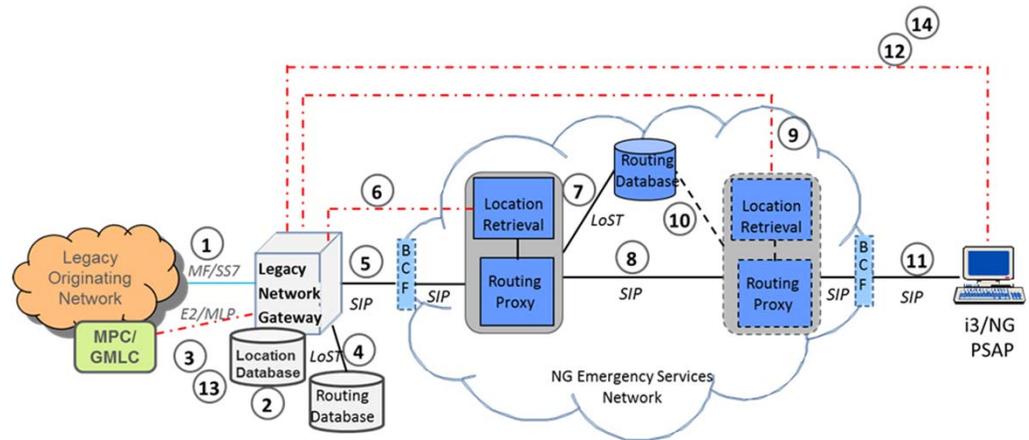
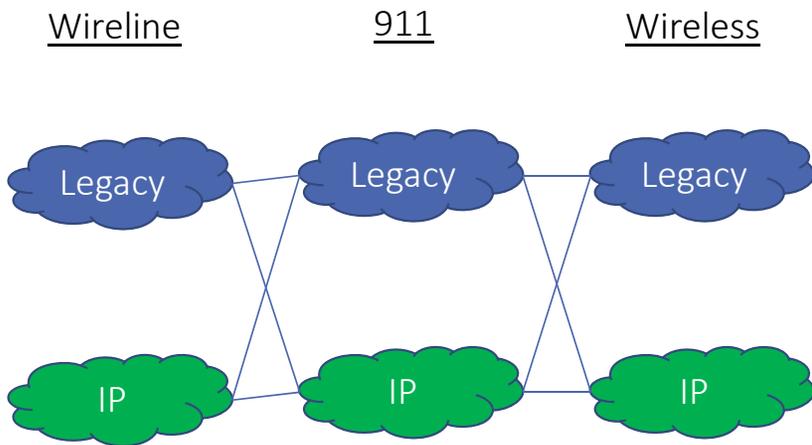
CSRIC Transition Activity 1: Understanding the Plans and Timeline for the State/Regional 9-1-1 Authority

- The National 911 Program annually surveys the states regarding their progress towards evolving NG9-1-1
- The 2017 Annual Survey⁷ showed that of the 45 states that responded:
 - *20 States have developed a State-wide NG9-1-1 Plan*
 - *20 States have issued RFPs for NG9-1-1 Components*
 - 22 States have installed/deployed and tested NG9-1-1 systems or component
 - 10 States can 100% process and interpret NG9-1-1 location and caller information
- The National 911 Program is currently collecting 2018 data.

7. National 911 Program, 2017 National 911 Progress Report – (2017), <https://www.911.gov/pdf/National-911-Program-Profile-Database-Progress-Report-2017.pdf>



CSRIC Transition Activity 2: Identifying the Technology Changes to Implement on the Network



ALI – Automatic Location Identification
 BCF – Border Control Function
 GMLC – Gateway Mobile Location Center
 LNG – Legacy Network Gateway
 LoST – Location to Service Translation
 MF – Multi-Frequency
 MLP – Mobile Location Protocol

MPC – Mobile Positioning Center
 NG – Next Generation
 PSAP – Public Safety Answering Point
 SIP – Session Initiation Protocol
 SR – Selective Router
 SRDB – Selective Router Database
 SS7 – Signaling System Number 7



CSRIC Transition Activity 3: Identifying Organizational Impact such as Training and Job Duties

Organizational Impact of the CSRIC Recommendations

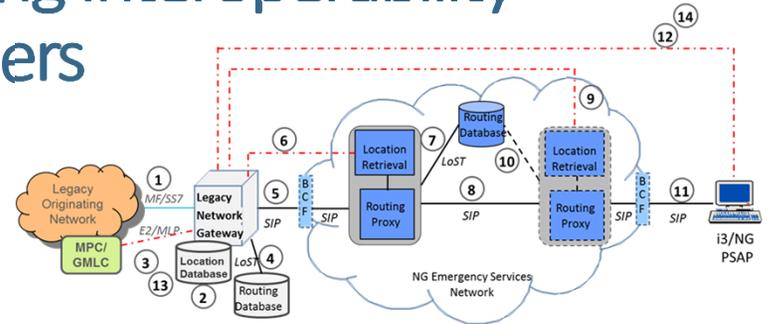
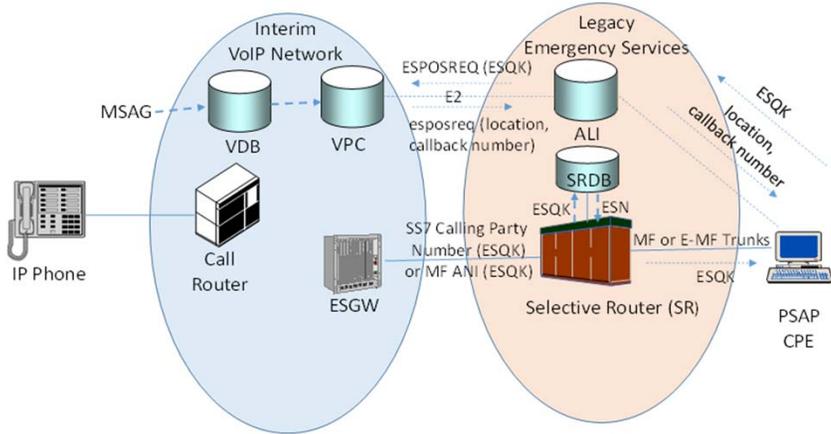
- The implementation team should include a coordinator and key staff members who will be responsible for implementing and maintaining the carrier's NG9-1-1 ecosystem.
- Carriers should consider SIP training and best practices to enable their staff to provision reliable and secure SIP trunks.

Security

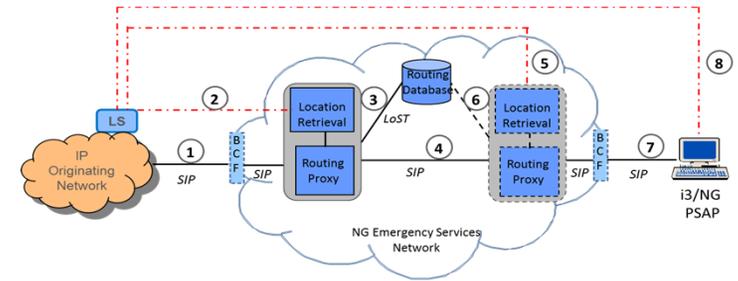
- Prepare workforce through identifying the team responsible for protecting the NG9-1-1 ecosystem, clarifying roles, training the team and updating job descriptions.
- Leverage Security Best Practices:
 - *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*
 - *NIST Cybersecurity Framework (NCF)*
 - *Multiple US Department of Homeland Security Resources*



CSRIC Transition Activity 4: Understanding Interoperability Requirements with the ESInet and Carriers



- ALI – Automatic Location Identification
- BCF – Border Control Function
- GMLC – Gateway Mobile Location Center
- LNG – Legacy Network Gateway
- LoST – Location to Service Translation
- MF – Multi-Frequency
- MPL – Mobile Location Protocol
- MPC – Mobile Positioning Center
- NG – Next Generation
- PSAP – Public Safety Answering Point
- SIP – Session Initiation Protocol
- SR – Selective Router
- SRDB – Selective Router Database
- SS7 – Signaling System Number 7



- BCF – Border Control Function
- IP – Internet Protocol
- LoST – Location to Service Translation
- LS – Location Server
- NG – Next Generation
- PSAP – Public Safety Answering Point
- SIP – Session Initiation Protocol



CSRIC Provides a Checklist of Activities to Support Small Carriers' Transition to NG9-1-1

- **Legacy stage** is characterized as the point in time where 9-1-1 services are provided by the traditional E9-1-1 Service Provider switch circuit-switched infrastructure and ALL circuits. And, the small carrier interconnects with public safety systems using legacy protocols.
- **Transitional state** is where the NG9-1-1 SSP has deployed aspects of NG9-1-1 as discussed in the Transitional State, Intermediate State or Jurisdictional End State as defined by the TFOPA Report.⁸
- **End State** is where the small carrier has deployed an IP-based network and the NG9-1-1 SSP has deployed aspects of NG9-1-1 as discussed in the Jurisdictional End State as defined by the TFOPA Report.

⁸ Federal Communications Commission, Task Force on Public Safety Answering Point (PSAP) Architecture – 2016 at 41 <https://docs.fcc.gov/public/attachments/DA-16-179A2.pdf>



CSRIC Identifies Seven Essential Elements of Readiness

- **Public Safety Governance and Regulatory Matters** - How public safety 9-1-1 Authorities organize and design their systems can impact the manner in which service providers support the delivery and processing of 9-1-1 services.
- **Routing and Location** - The systematic approach that is used to determine 9-1-1 call routing to the appropriate emergency services network, and the supporting data functions.
- **GIS Data** - GIS data provided by the 9-1-1 Authority, or access to it will allow for updated jurisdictional polygons for 9-1-1 call handling. GIS data may also be utilized within the small carrier (or with access to it) for the validation (LVF) function to support customer address validation.
- **Network** - The network area capabilities represent the various technology mechanisms for connecting small carrier networks to either a legacy SR or an ESI-net for the purposes of processing 9-1-1 calls.
- **Security** - Security includes capabilities, operations and best practices for the interconnection to the ESI-net.
- **Operational Planning** - Operations planning addresses aspects of execution, oversight, plan management and efforts to support on-going evolution with the planning of connection to the ESI-net and the transition to the NG9-1-1 processing model and services.
- **Optional Interfaces** - Optional Interfaces addresses services and interfaces that interconnect with the ESI-net but apply beyond NG Core Services primary functions.



Conclusion

CSRIC VI Recommends:

- Carriers should stay abreast of the NG9-1-1 transition to better understand the ecosystem, timelines, and implications for their companies.
- Carriers should establish contact with NG9-1-1 Authorities within their service areas and gather information such as implementation schedules and functionality expectations.
- Carriers should consider SIP training and best practices to enable their staff to provision reliable and secure SIP trunks.
- Carriers should prepare their staff for Cybersecurity issues related to NG9-1-1.



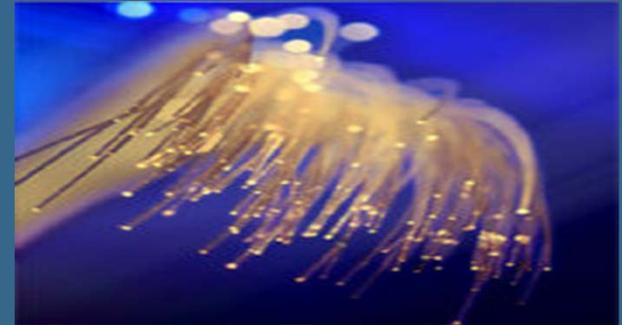
Introduction to NORS/DIRS



Julia Tu

Electronics Engineer, Cybersecurity and
Communications Reliability Division

Public Safety and Homeland Security Bureau

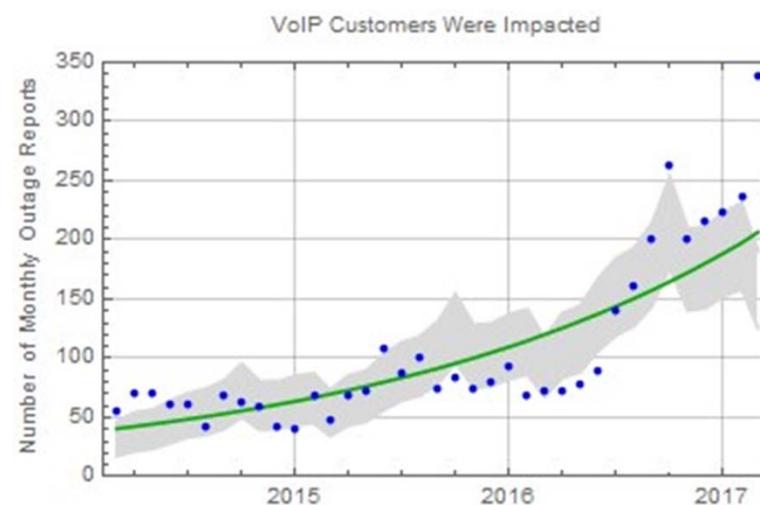


Network Outage Reporting System (NORS)

<https://www.fcc.gov/network-outage-reporting-system-nors>

- Goals
 - *Improve network reliability*
 - *Have situational awareness of major events*
- Scope
 - *E911 outages*
 - *Wireline outages*
 - *Wireless outages*
 - *VoIP outages*
 - *Facility outages*
- Information filed is presumptively confidential, and only shared with DHS.
 - *However, aggregated information may be shared with the public.*

Checking for Trends in Outage Categories



The FCC Uses Specific Thresholds to Determine Reportable Events

At least 30 minutes long and at least one of the following criterion is satisfied:

VoIP –

900,000 User minutes

Wireline –

900,000 User minutes

90,000 Blocked calls

Wireless –

900,000 User minutes

90,000 Blocked calls

Mobile Switching Center outage

Cable Telephony – 900,000 User minutes,
90,000 blocked calls

Emergency Services –

E911 – 900,000 User Minutes

Infrastructure Failures –

OC3 – 667 OC3 minutes (Effective 2/1/2018)

OC3 – Simplex greater than 4 days (Effective 2/1/2018)

SS7 Failures

Failures of Special Facilities –

Airport

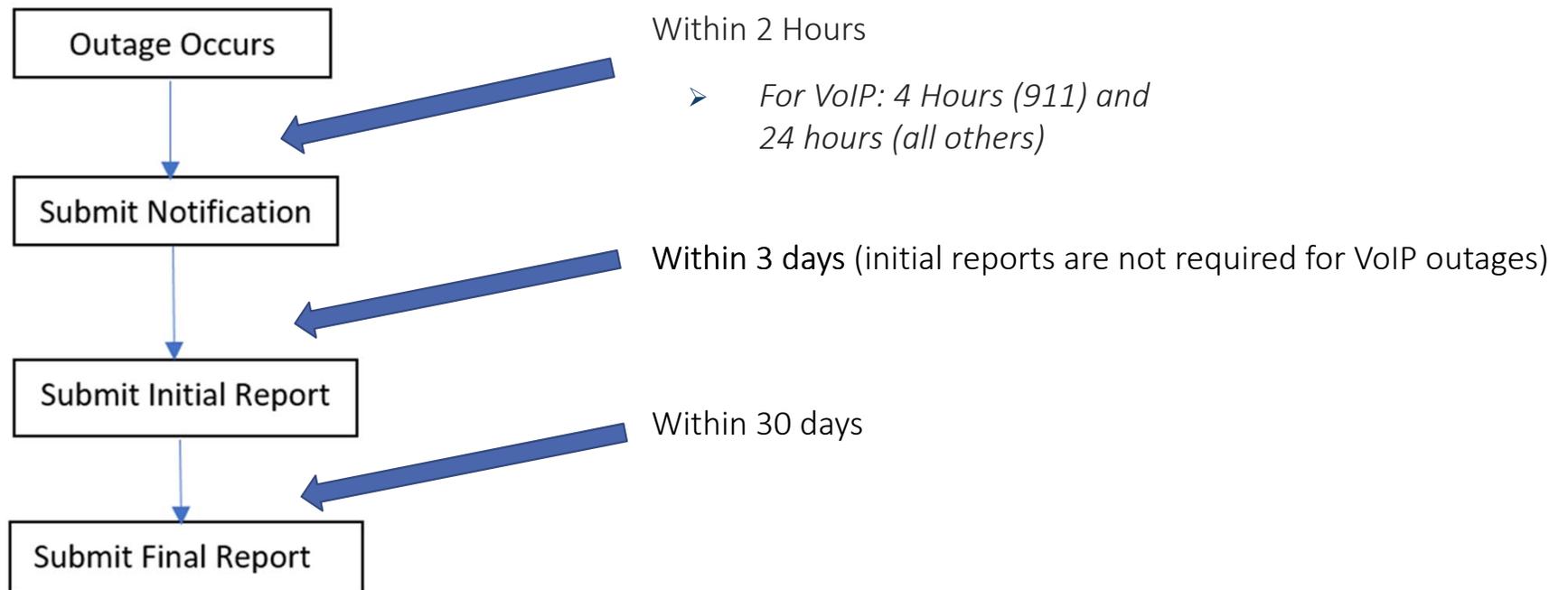
Other Special Facilities - (Military, Nuclear, etc.)

Paging

Satellite



The NORS Reporting Processes



NORS Final Reports Contain a Number of Elements

- When outage occurred
- Description of event
- Duration of outage – including partial restorations
- Location of the effects of the event
- Effects of the outage – number of customers affected
- Causes of the event
- Whether malicious or not
- Part of network involved
- Steps taken to prevent future occurrences
- Best Practices related to the outage
- Contact information about the outage



Analyzing the NORS Data

- Provide a daily review of major outages
 - *E9-1-1 outages*
 - *Major wireless outages*
 - *Major wireline outage*
 - *VoIP outages*
- On a quarterly basis, the NORS team:
 - *statistically analyze final reports for outage trends provide a statistical analysis of outage reports for the Network Reliability Steering Committee, and*
 - *prepare analyses of individual company results for meetings with those companies.*

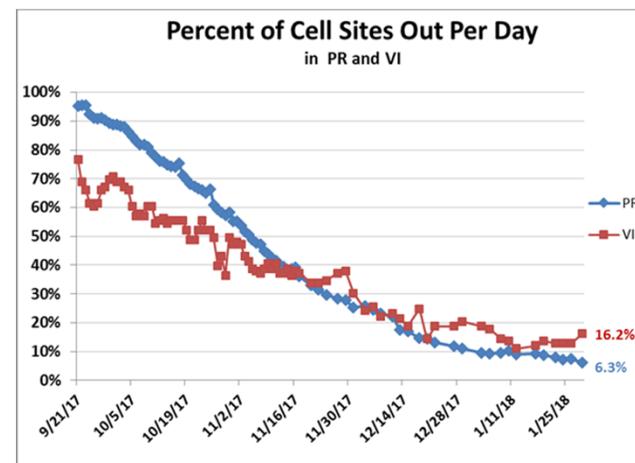
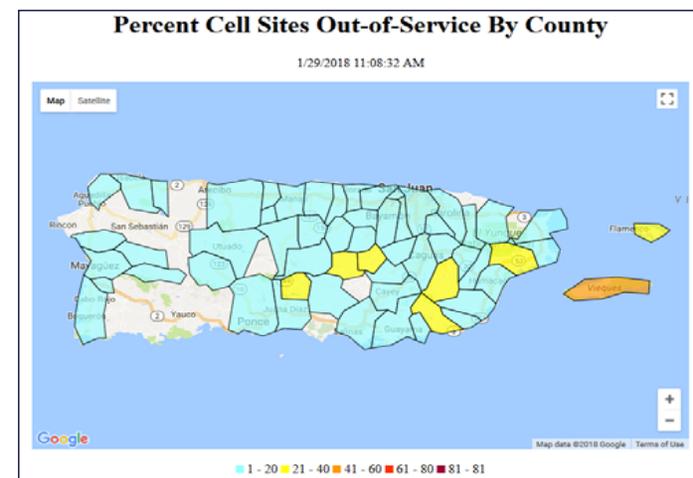


Disaster Information Reporting System (DIRS)

<https://www.fcc.gov/nors/disaster/>

- Goals
 - Track status of communications assets during disasters
 - Track recovery efforts
 - Consistent information
- Scope
 - PSAPs (E911)
 - Major equipment (switches, headends, MSC, etc.)
 - Customers out-of-service
 - Blocked calls
 - Facilities/TSP
 - Cell site by county
 - Radio and TV stations
- Information filed is presumptively confidential, and only shared with DHS.
 - However, aggregated information may be shared with the public.

DIRS Products for Hurricane Maria

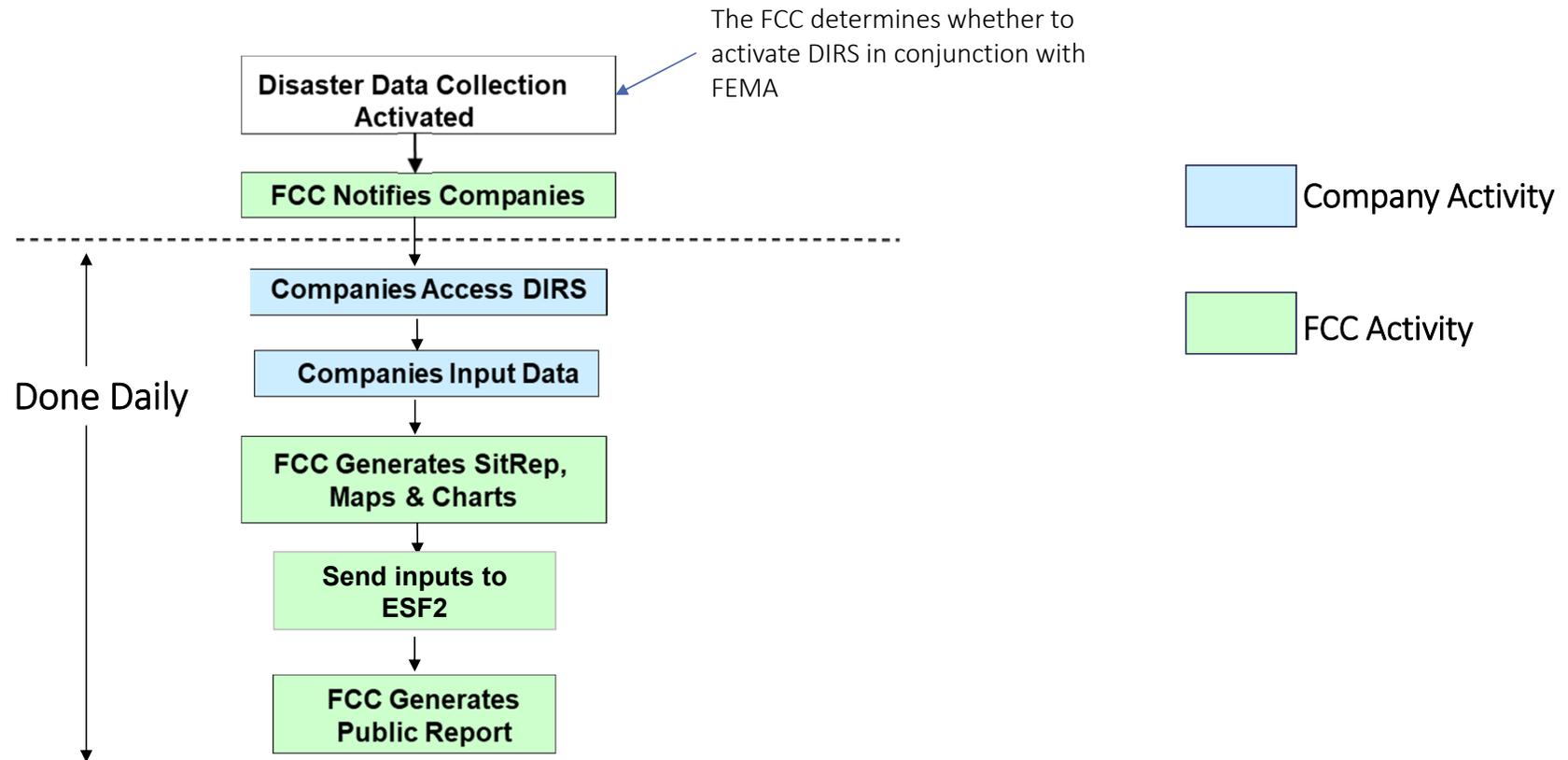


DIRS - Benefits for Communications Providers

- **Designate contact:** Allows communications providers to identify the appropriate contact for his/her station during emergencies.
- **Receive help:** Provides an avenue for communications providers to restore their operations and receive additional help during emergencies, e.g., securing generators, fuel, etc.
- **Streamline requests:** Reduces the number of requests from various government agencies for status of each station. Other government agencies will rely on the FCC (DIRS) for status of each broadcast station.
- **Aid your community:** Better ensures that communications providers will be able to serve their communities, providing them with critical updates and risk communications information from reliable and credible sources during emergencies.



The DIRS Reporting Process

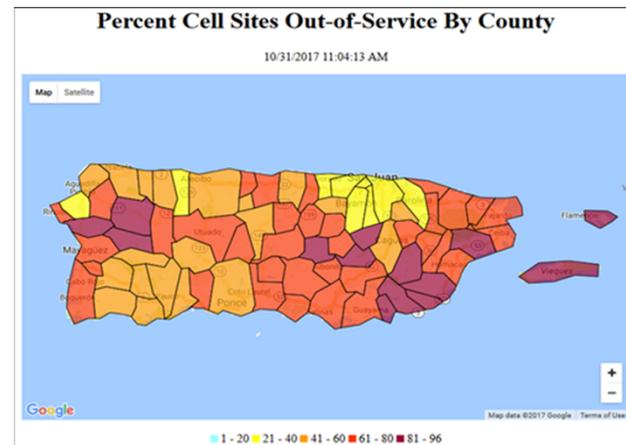
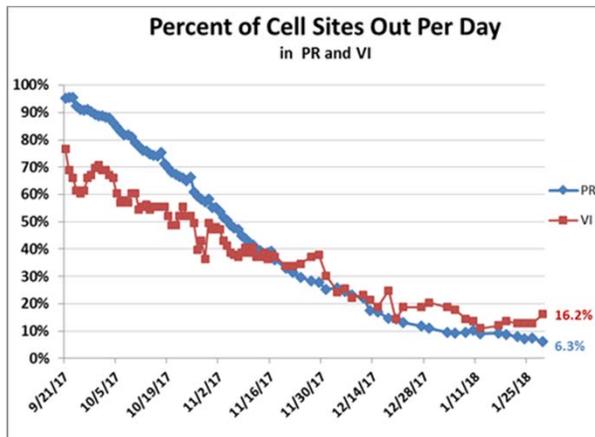
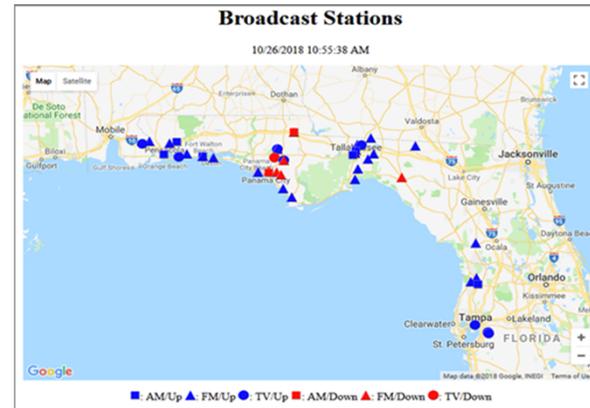
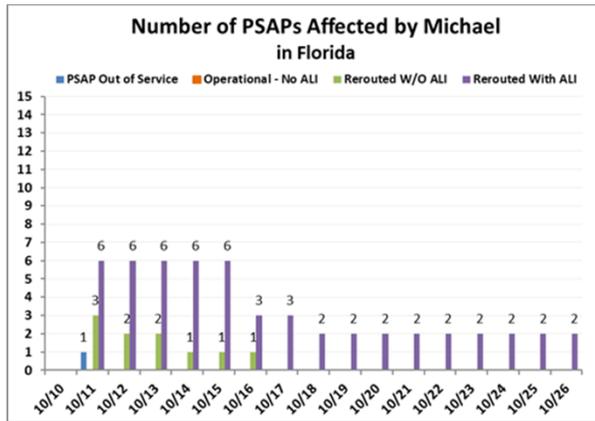


Scope of DIRS Data

- PSAP
- Major Equipment – Wireline, Cable
- Wireless MSC/STP
- Wireless Cell Site by County
- Interoffice Facilities/TSP
- Remote Aggregation Devices/Distribution
- IXC Blocking
- Broadcast – AM, FM, TV Stations
- Cable Systems



DIRS Graphical Products



NRSC Emergency Checklist

https://www.atis.org/01_committ_forums/nrsc/documents/

General guidance regarding preparedness for and response to a wide array of emergency situations. Some examples are:

- *Assess whether critical facilities, network equipment, and power connections are located in areas that are likely to flood*
- *Assess whether mitigation plans are implemented in sites located in flood prone areas (e.g., elevation of platforms)*
- *Deploy a high tensile strength aerial service wire*
- *Negotiate a wider right-of-way to prevent trees from obstructing aerial cable*
- *Design the outside portion of the network to better withstand flooding and severe weather, and make restoration easier*



Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs



Justin Faulb

Legal Advisor, Office of the Bureau Chief

Wireline Competition Bureau



Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs (“USF Supply Chain NPRM”)

- Adopted on April 17, 2018.
- Sought comment on a proposal to “prohibit, going forward, the use of Universal Service Fund money to purchase equipment or services from any communications equipment or service providers identified as posing a national security risk to communications equipment or the communications supply chain.”
- Follows Executive and Legislative branch action over the last decade, including:
 - *2012 House Permanent Select Committee on Intelligence – recommended US government agencies and federal contractors to exclude from their systems equipment from certain companies with connections to hostile foreign governments.*
 - *May 2013 Presidential Policy Directive – required federal agencies to work together to identify vulnerabilities in communications infrastructure and to increase the resilience of critical infrastructure.*
 - *May 2017 Executive Order – emphasized the importance of the security of federal networks and critical communications infrastructure.*
 - *2018 National Defense Authorization Act – bars the Department of Defense from using Huawei or ZTE for critical programs and bars all federal agencies from using products or services from Kaspersky Lab*



USF Supply Chain NPRM (con't)

- More recent Executive and Legislative branch developments:
 - *2019 National Defense Authorization Act – prohibits executive agencies from expending loan or grant funds to procure systems or services “covered telecommunications equipment” as a substantial or essential component of a system and requires the head of the FCC to prioritize available funding and technical support to affected entities.*
 - *May 2019 Executive Order - The EO authorizes the Secretary of Commerce to regulate the acquisition and use of information and communications technology services from a “foreign adversary.”*



USF Supply Chain NPRM (con't)

- Also sought comment on:
 - *The types of equipment and services that should be covered by the proposed rule. Should the Commission prohibit use of USF funds on any purchases from companies identified as raising national security risks? Or, are there reasons to exempt certain categories or types of equipment or services from the scope of the proposed rule?*
 - *The effective date for the proposed rule. What should that date be? How long would USF recipients need to begin complying with the rule? How does the presence of multiyear contracts impact the effective date?*



USF Supply Chain NPRM (con't)

- Sought comment on additional issues:
 - *How should the Commission identify companies that pose a national security risk to the integrity of communications networks or a communications supply chain?*
 - *For example, should the FCC rely on existing statutes or on a list of companies maintained by another federal agency?*
 - *What are the costs and benefits associated with the proposed rule?*
 - *What is the Commission's legal authority to act?*



Public Notice on Section 889 of the NDAA

- Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA) was enacted in August 2018.
 - *Section 889(b)(1) of the 2019 NDAA prohibits the head of an executive agency from obligating or expending “loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems” “that use[] covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.”*
 - *The 2019 NDAA defines “covered telecommunications equipment or services” as including telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation or any subsidiary or affiliate of such entities.*
 - *Section 889(b)(2) provides that heads of executive agencies administering “loan, grant, or subsidy programs,” specifically naming the head of the Federal Communications Commission, shall, “[i]n implementing the prohibition in paragraph (1),” prioritize available funding and technical support to assist entities affected by the prohibition in section 889(b)(1).*
 - *The Public Notice seeks comment on the impact of the NDAA on the FCC’s USF Supply Chain proceeding.*
 - *Public Notice released October 26, 2018.*



Executive Order on Securing the Information and Communications Technology and Services Supply Chain

- Issued May 15, 2019.
- The EO authorizes the Secretary of Commerce to regulate the acquisition or use of information and communications technology services from a “foreign adversary.”
- The EO provides that the Secretary of Commerce—in consultation with other agencies, including the FCC—may prohibit “any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States” for certain transactions deemed to pose unacceptable risks to national security.



Executive Order on Securing the Information and Communications Technology and Services Supply Chain (con't)

- The Secretary of Commerce, in consultation with other named departments, agencies, and offices within the federal government, including the FCC, has 150 days (until October 15, 2019) to issue regulations consistent with the EO.
- Upon the Secretary determining that particular transactions or classes of transactions pose a threat to national security, the EO will apply to such transactions initiated, pending, or completed after the date of the EO



Executive Order on Securing the Information and Communications Technology and Services Supply Chain (con't)

- The EO also includes a number of reporting requirements:
 - *The Secretary of Commerce, in consultation with the Secretary of State, is “authorized to submit recurring and final reports to the Congress on the national emergency declared” in the EO.*
 - *The Director of National Intelligence is required to “produce periodic written assessments” of threats to the communications supply chain to the President and the Secretary of Commerce. The first assessment is due within 40 days of the EO, with further assessments “completed at least annually.”*
 - *The Secretary of Homeland Security, in coordination with “sector-specific agencies and coordinating councils,” must produce an assessment of vulnerabilities that pose the greatest threats to national security within 80 days of the EO and annually thereafter.*
 - *Within one year of the date of the EO and annually thereafter, the Secretary of Commerce, in consultation with the Secretaries of Treasury, Homeland Security, State, Defense, as well as the Attorney General, United States Trade Representative, Director of National Intelligence, and the Chairman of the Federal Communications Commission, shall “assess and report to the President whether the actions taken by the Secretary pursuant to this order are sufficient and continue to be necessary to mitigate the risks identified in, and pursuant to,” the EO.*



Importance of Supply Chain Security for Small Businesses

- All carriers—including small carriers—must be mindful of supply chain security.
- With the forthcoming deployment of 5G networks, the security of networks takes on a new level of importance. Nations hostile to the United States could use equipment to access sensitive information, harm critical infrastructure, or conduct economic and industrial espionage.
- Do you have equipment, or are you considering equipment in your network, that would be potentially impacted by the FCC's proposed rule or other recent federal activities concerning U.S. supply chain security?
- Plan ahead and participate. While comment periods are closed, the FCC's USF Supply Chain proceeding is ongoing

