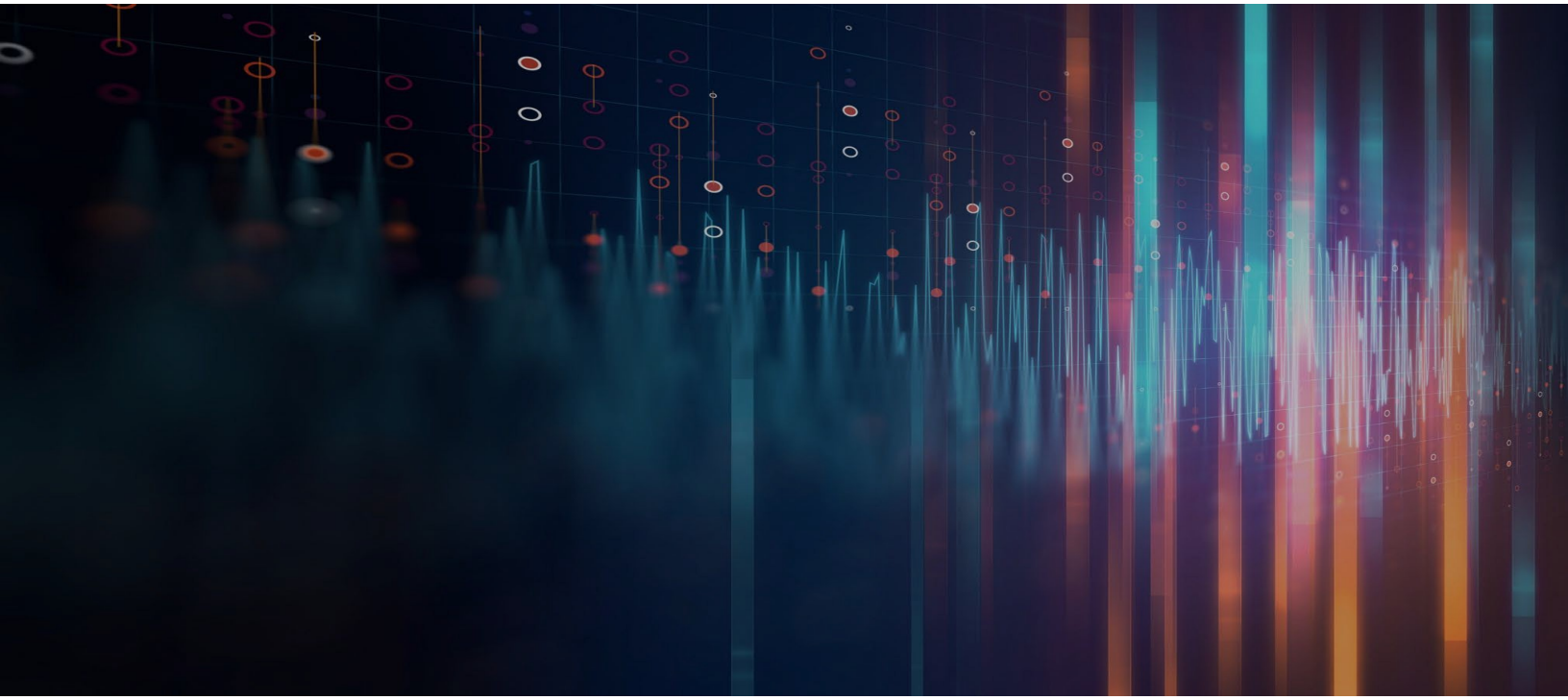

RADIO FREQUENCY INTERFERENCE BEST PRACTICES GUIDEBOOK

FEBRUARY 2020

Cybersecurity and Infrastructure Security Agency
SAFECOM/National Council of Statewide Interoperability Coordinators

Executive Summary

Public safety voice and data communications are continuously at risk of radio frequency (RF) interference, which is defined as "the effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy."[1] RF interference can impact a variety of commonly-used wireless technologies such as land mobile radio (LMR), Long-Term Evolution (LTE), Bluetooth, Wi-Fi, and Global Positioning Systems (GPS). Both manmade and natural sources can generate undesired signals that may cause RF interference capable of disrupting wireless communications, including 911 calls, essential LMR or LTE communications between first responders, and navigational systems using GPS or other satellite-based location services.[2]

To mitigate possible risks to public safety communications, SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) developed the *Radio Frequency Interference Best Practices Guidebook* with the support of the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the Science and Technology Directorate (S&T) to educate public safety organizations on RF interference threats. Specifically, this Guidebook:

- Provides an overview of the different types of RF interference, illegal jamming operations, and the implications they pose to public safety communications;
- Summarizes ongoing efforts related to awareness, preparation, mitigation, and current laws pertaining to RF interference; and
- Offers information on how public safety organizations can best recognize, respond to, report, and resolve RF interference incidents.

Following a review of the current threats posed by RF interference, SAFECOM, NCSWIC, CISA, and S&T recommend that public safety organizations:

- Train personnel to recognize and respond to RF interference that is either: (1) unintentionally caused by naturally occurring or manmade signal sources; or (2) the result of an intentional attempt to disrupt communications;
- Create and routinely test a Primary, Alternate, Contingency, and Emergency (PACE) Plan to ensure communications operability and resiliency;
- Familiarize themselves with how to report incidents of RF interference to the Federal Communications Commission (FCC) and other appropriate authorities; and
- Help legislators and regulators understand the value of RF interference enforcement legislation.

This document does not contain information on specific system requirements, comprehensive operating procedures, or specific governance considerations, but instead provides general recommendations and resources for state, local, tribal, and territorial (SLTT) public safety practitioners.

[1] International Telecommunication Union (ITU), "Radio Regulations Chapter I – Terminology and Technical Characteristics" last accessed January 3, 2020.
[2] Examples of known RF interference include: nearby wireless communications transmitters, vehicle ignition systems, jamming devices, lightning, solar flares, and auroras.

Table of Contents

Figures

Tables

Introduction

> *"A responder's most important tool is his or her communication device. It's what provides the awareness we need to accomplish our mission when responding to an emergency. It is ultimately what serves as our lifeline and determines whether we make it home or not."*
>
> ***Rodney Reed***
> *Assistant Chief, Operational Support*
> *Fire Marshal's Office, Harris County, TX*
> *(The Siren, 2017)*

In day-to-day operations, and even more critically in emergency and disaster situations, resilient communications and situational awareness play a vital part in supporting the missions of public safety and protecting the lives of first responders. Interruption to mission-critical communications may lead public safety personnel into dangerous situations or delay delivery of life-saving services. To minimize disruption, the public safety community must work together to address and mitigate the growing problem of radio frequency (RF) interference.

RF interference is defined as "the effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy."[3]

Effects of interference can range from mild disruption or delays in data throughput to a complete loss of service. All devices that use RF are potentially vulnerable to interference, including radio, cellular, radar, satellite, Wi-Fi, Global Positioning System (GPS), unmanned aircraft system (UAS) communications and control systems, and other technologies. While public safety personnel primarily use land mobile radios (LMR) for emergency communications, the rollout of the Nationwide Public Safety Broadband Network (NPSBN) by the First Responder Network Authority (FirstNet Authority)[4] and a wider array of available mobile communications technologies have required that agencies recognize their current vulnerabilities to RF interference and prepare to mitigate them appropriately.

According to the International Telecommunication Union's (ITU) Radio Regulations (RR), there are three types of RF interference:

- **Permissible interference** (*RR, No. 1.167*): "Observed or predicted interference which complies with quantitative interference and sharing criteria contained in these [ITU RR]…or in ITU Radiocommunication Sector (ITU-R) Recommendations or in special agreements as provided for in these Regulations"[5];
- **Accepted interference** (*RR, No. 1.168*): "Interference at a higher level than defined as permissible interference and which has been agreed upon between two or more administrations without prejudice to other administrations"[6]; and
- **Harmful interference** (*RR, No. 1.169*): "Interference which endangers the functioning of a radio[-]navigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radio…communication service operating in accordance with RR"[7].

[3] Ibid, ITU.
[4] The FirstNet Authority is "the first nationwide public safety broadband network dedicated to public safety…ready to help law enforcement, the fire services, and EMS do their jobs safely and effectively."
[5] Ibid, ITU.
[6] Ibid, ITU.
[7] Ibid, ITU.

There are two sources that can result in harmful interference:

- **Intentional interference sources**, which include illegal jamming devices, radios programmed to use unauthorized frequencies, or other purpose-built solutions; or
- **Unintentional interference sources**, which include low-quality foreign-made electronics (e.g., Universal Serial Bus [USB] chargers, baby monitors transmitting on public safety frequencies); outdated, degraded, or improperly installed signal boosters; lighting ballasts; and solar flares.

RF Interference Categories and Symptoms

RF interference symptoms include disruption or failure of wireless communications or equipment for unknown reasons. More specifically, responders may be experiencing interference if they:[8]

- Cannot communicate in areas where they typically have radio or cell coverage;
- Cannot communicate with normally reliable base radios or repeaters;
- Cannot communicate on multiple communications devices using multiple bands;
- Notice a significant loss of functionality or general failure of GPS systems; or
- Realize communications improve significantly when moving a short distance away from a specific fixed area, or "dead zone."

The severity of the interference will depend significantly on the location of the source in relation to the target. Three categories of RF interference that can affect mission-critical public safety communications – internal/self-interference, external interference, and intentional jamming – are discussed further below.

The U.S. Government, including the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the Science and Technology Directorate (S&T), have established programs to encourage education and information sharing around RF interference threats. Appendix A, *DHS RF Interference Activities*, outlines more information on these ongoing initiatives.

Internal/Self Interference

Internal or self-interference is a type of unintentional RF interference which occurs when an organization's own devices may be operating in a manner that interferes with their internal communications. Most RF interference can be attributed to internal interference, which may be caused by the improper or incorrect setup of communications equipment. Internal interference can occur directly after upgrading equipment, adding new equipment to networks, or changing existing configurations.

Table 1. Internal RF Interference Examples

Internal RF Interference Examples	
Equipment problem	Interruptions may be caused by new installations of or updates to communications technologies. For example, updates to physical infrastructure (e.g., new additions to a tower or relocation of a receiver), as well as upgrades of radio consoles or hubs may cause this kind of internal interference.
Receiver intermodulation	Interruptions may be caused by "non-linear mixing" of external signals inside the receiver.[9] Users will usually hear multiple wireless signal emissions at the same time.
Front-end overload	Interruptions may be caused by inadequate filtering of radio equipment, or equipment that needs adjustment.

[8] DHS S&T, "GOT COMMS? Recognizing and Mitigating Intentional and Unintentional Interference," last accessed January 3, 2020.
[9] Jay M. Jacobsmeyer, "800 MHz Interference: What Is It, How Do We Mitigate It and What Does the Future Hold?" November 6, 2017.

External Interference

Table 2. External RF Interference Examples

External RF Interference Examples	
Co-channel	Caused by more than one transmitter communicating on the same channel due to improper frequency coordination, deteriorating or malfunctioning equipment, or anomalous propagation.[10]
Adjacent channel	Caused by a transmitter operating on an adjacent frequency and its energy spilling over into the desired receive channel.[11] For example, adjacent channel interference occurs along the U.S. Southwest Border where there are reported difficulties coordinating with local Mexican entities.[12]
Spurious emissions	Caused when a transmitter emits on frequencies on which it is not meant to operate. This can be observable by poor audio quality or connectivity.[13]
Natural occurrences	Caused by natural events such as solar flares, northern lights, and other electromagnetic activities.[14] Natural disasters, including hurricanes and floods, can also disrupt and damage RF communications infrastructure.

External interference is a type of unintentional RF interference that can result from sources similar to those associated with internal RF interference but exist outside of an organization's jurisdiction or control. External RF interference may result from a neighboring organization's communication system affecting another's frequency, or naturally occurring space weather events, such as solar flares.

Intentional Interference

Intentional interference – or jamming – is performed by an actor with a willful intent to disrupt, disconnect, or degrade communications. Malicious jamming and nuisance jamming are the two types of intentional interference. Malicious jamming is conducted by individuals with willful and criminal intent. The criminal intent may be to prevent public safety personnel from completing their mission, or conceal an ongoing criminal activity, among other possible motivations.

In contrast, nuisance jammers are willful, but not malicious as they cause interference without criminal intent. [15] Common examples include drivers using mobile GPS jammers to avoid GPS tracking and speed monitoring, and cellular or Wi-Fi jammers used to create "quiet zones" in workplaces, places of worship, and other locations. Despite the lack of malicious intent, nuisance jamming is dangerous as it could impact public safety operations (e.g., blocking 911 calls, impacting radio dispatch), and the first responders should recognize that anyone they interact with daily could be a nuisance jammer, not just individuals or organizations with criminal intent.

RF Jammers

Jamming is a term used to describe one type of intentional interference, a Denial-of-Service (DoS) attack,[16] which can either use a "brute force" method to overwhelm a signal or use relatively low-powered signals to overwhelm public safety communications systems. Illegal jamming devices are designed to emit RF signals—or noise—over specific bands to overpower the intended, legitimate signals. Under Title 47, United States Code (U.S.C.) Sections 302a(a) and 302a(b), the manufacture, importation,

[10] Kenneth Wyatt, "Identifying and Locating Radio Frequency Interference (RFI)," September 7, 2018.
[11] Ibid.
[12] For more on adjacent channel regulation and procedures at U.S. borders, see *Manual of Regulations and Procedures for Federal Radio Frequency Management*.
[13] Telecom ABC, "Spurious Emission," last accessed January 3, 2020.
[14] Jacoba Poppleton, "Solar Storms: A Communication Problem," *Research Matters* 2010, last accessed January 3, 2020.
[15] John Merrill, "Ensuring Resilient Communications – Briefing for Position, Navigation & Timing Advisory Board," May 17, 2018.
[16] United States Computer Emergency Readiness Team (US-CERT), "Understanding Denial-of-Service Attacks," last modified November 20, 2019.

marketing, sale, shipment, or operation of devices capable of interfering with radio communications (e.g., jammers) is illegal in the United States.[17]

Outside the U.S., RF jamming devices are commercially available, however the cost and supported range varyies significantly by device. It is difficult to detect the presence of low powered jammers as they are often cheaply made overseas and emit inconsistent signals. Moreover, these devices, examples of which are outlined in **Figure 1** below, are easily concealed, mobile, and can be effective in concentrated areas.

Figure 1. RF Jammer Examples

Bad actors can obtain illegal jamming devices or utilize their knowledge of RF systems to sufficiently disrupt public safety communications, as illustrated below in **Table 3**:

Table 3. Intentional Interference Examples

Intentional Interference Examples	
Intentional interference within the organization	An internal actor may be causing RF interference through one of the previously discussed methods or through a jamming device.
Intentional external interference	An external actor uses equipment, such as a jamming device, to overpower or send continuous transmissions on communications channels critical for law enforcement or public safety operations, such as smuggling interdiction.

Meaconing

Meaconing describes a system which receives radio beacon signals and rebroadcasts them on the same frequency to intentionally confuse navigation. Meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations. Meaconing introduces position and altitude errors onto a navigation system such as a GPS. Meaconing may be extremely difficult to detect as the GPS receiver may appear to be functioning properly however its position or altitude information is inaccurate.

The threat of intentional interference frequently impacts the public safety community and puts the public at risk. This delay or disruption of public safety communications can result in the loss of life or property, as outlined in the following examples:

Examples of Intentional RF Interference to Public Safety Communications

In 2013, police in Suffolk County, New York, arrested a man who, over a nine-month period, repeatedly interfered with Melville Fire Department's radio transmissions.[18] The Federal Communications Commission (FCC) investigated this complaint and worked closely with local police to resolve this intentional interference to GPS signals.

Examples of Intentional RF Interference

In 2012, the FCC investigated a Federal Aviation Administration (FAA) complaint regarding interference to their Ground-Based Augmentation System (GBAS) at Newark Liberty International Airport. FCC

[17] 47 U.S.C. § 302a (2013)
[18] Frank Eltman, "2 NY Congressman Propose Law on Fire Radio Jammers," *The Washington Times*, March 10, 2014.

agents found the source of interference was coming from an individual using a GPS jammer in his company vehicle while traveling along the New Jersey Turnpike. Although the individual intentionally interfered with GPS to avoid detection and tracking of his vehicle, his intent was not to disrupt the GBAS. The FCC levied a fine of $31,875 against the individual.[19]

Similarly, in 2013, the FCC received an interference complaint from a local wireless service provider. FCC agents investigated and found an individual using a cell phone jamming device in his car during his daily work commute to and from Tampa, Florida, which caused interference to cellular service along Interstate 4, and disrupted police communications. The FCC levied a fine of $48,000 against the individual.[20]

Examples of Federal Government Activity to Counter RF Interference

Agencies along the U.S. Southwest Border face ongoing challenges mitigating unintentional adjacent channel interference originating from Mexico. Cooperation and coordination on the federal, state, and local levels are critical to resolving these incidents.[21]

The U.S. Customs and Border Protection (CBP) has jurisdiction to inspect imported goods as they enter the country via mail facilities and airports, seizing jammers when identified. While these jamming devices are subject to confiscation if properly identified, it is difficult to estimate how many shipments of illegal jammers may have entered the country without impediment.

Legal and Public Safety Responses to RF Interference

Federal Law

The FCC enforces provisions from the *Communications Act of 1934* (the Act), which expressly prohibits the marketing, sale, or use of devices designed to intentionally block, jam, or interfere with authorized radio communications.[22] More specifically: [23]

- **Section 301** states that "no person shall use or operate any apparatus for the transmission of energy or communications or signals by radio…except under and in accordance with [the] Act and with a license in that behalf granted under the provisions of this chapter";
- **Section 302(b)** states that "no person shall manufacture, import, sell, offer for sale, or ship [non-compliant] devices or home electronic equipment and systems, or use devices"; and
- **Section 333** states that "no person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government."

In addition to the Act, other applicable provisions under FCC rules include:

- **Section 2.803** prohibits the importation, marketing, or sale of these devices within the United States;[24]
- **Section 2.805** prohibits operation of these devices within the United States;[25] and
- **Section 2.807** provides for certain limited exceptions, such as the sale to U.S. Government for authorized, official use.[26]

[19] Inside Global Navigation Satellite Systems (GNSS), "FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS," August 31, 2013.
[20] FCC, "FCC Fines Florida Driver $48k For Jamming Communications," May 25, 2016.
[21] CISA, "Southwest Border Communications Working Group Fact Sheet," last accessed January 3, 2020.
[22] FCC, "GPS, Wi-Fi, and Cell Phone Jammers Frequently Asked Questions (FAQs)," last accessed December 20, 2018.
[23] Ibid.
[24] 47 C.F.R. § 2.803
[25] 47 C.F.R. § 2.805
[26] 47 C.F.R. § 2.807

Violators of the Act and associated FCC rules may be subject to the penalties set forth in Title 47, U.S.C. Sections 501 through 510.[27]

- **Section 503** allows the FCC to impose forfeitures for willful or repeated violations of the Act, the Commission's rules, regulations, or related orders, as well as for violations of the terms and conditions of any license, certificate, or other FCC authorization, among other things; and
- **Section 510** allows for seizure of equipment used, possessed, advertised, or sold with knowing intent to violate Title 47, U.S.C. Sections 301 or 302.

State Law

In addition to the prohibitions set forth by the Act, several states have enacted laws that prohibit jamming and intentional interference.

Table 4. State Legislation Overview

State	Legislation	Penalties
Florida	Statute Chapter 877, Section 27	A person who violates this Section commits a felony of the third degree.[28]
Texas	Statute Chapter 38, Section 152	Violations under this Section are considered a Class A misdemeanor.[29]
Arizona	Chapter 13, Section 2922	A person who violates Subsection A is guilty of a Class 6 felony and a person who violates Subsection B is guilty of a Class 1 misdemeanor.[30]
Alabama	Statute Section 13a-10-16	Anyone in Alabama who interferes with public safety communications is charged with a Class C felony.[31]

In addition, Colorado,[32] Connecticut,[33] Illinois,[34] and Tennessee[35] have established laws prohibiting the use of in-vehicle jamming devices.

RF Interference Mitigation

Education

An organization's technical team, radio support personnel, and Communications Unit Leaders (COML) are the most qualified staff to recognize if there is a persistent RF interference problem. However, the key to early detection and data collection is to educate field personnel on the threat and potential mitigation methods. Additionally, having teams formally trained and accredited in RF interference mitigation ensures that staff supporting public safety answering points (PSAP) or other public safety agencies are equipped and trained in mitigation methods. Officials should be made aware that public, state, and local government agencies, including state and local law enforcement agencies, are also prohibited from using jammers or any other type of device that blocks, jams, or interferes with authorized communications.

There are many commercially available training opportunities to expand knowledge of RF Interference Mitigation (RFIM) best practices, as well as courses on RF interference identification and how to use a spectrum analyzer. One example is the International Certification Accreditation Council (ICAC) which offers several accredited training courses and certificate programs related to RFIM. [36] Gaining competency and certification on RFIM enables public safety technicians to quickly identify, mitigate, and

[27] FCC, "Public Notice DA # 05-1776s," June 27, 2005.
[28] FL Stat § 877.27 (2016)
[29] Texas Penal Code § 38.152
[30] AZ Rev Stat § 13-2922 (2017)
[31] AL Code § 13A-10-16 (2014)
[32] CO Rev Stat § 42-4-1415 (2017)
[33] CT Gen Stat § 53a-127c (2016)
[34] IL Vehicle Code 625 ILCS 5/12-613
[35] TN Code § 39-16-610 (2017)
[36] Electronics Technicians Association, "RF Interference Mitigation – RFIM Competency Requirements," last accessed January 3, 2020.

respond to RF interference affecting their communications. Organizations, especially those neighboring one another, should promote information and resource sharing partnerships to raise awareness of anomalous and cross-jurisdictional interference activities. Below are additional examples demonstrating how to mitigate RF interference:

- Train operators to better use radios and switch between channels when communications are not reliable;
- Consider using RF filters to attenuate adjacent channel traffic; and
- Train personnel on courteous operating procedures, allowing operators to practice using equipment, switch between channels, and enable automatic gain control (AGC), among other actions.

Everyday Preparedness

Combining education with everyday preparedness practices further assists RF interference mitigation from the onset. Public safety organizations should engage legal counsel to better understand state, local, territorial, and tribal (SLTT) jamming laws that exist in addition to FCC rules and regulations. On some occasions, the interference is frequency specific. To further minimize impacts, organizations are recommended to procure communications systems in bands different from their primary system, with a preference for high frequency (HF), ultra-high frequency (UHF), or very high frequency (VHF) bands where possible, and change the frequencies in LMRs to mitigate interference. If changing frequency does not work, changing the band of frequencies may mitigate the interference.

It is crucial that organizations only operate devices that have received FCC grants of equipment authorization, and maintain transmission systems that are compliant with FCC-issued licenses. Certain FCC-certified frequency coordinators can receive, investigate, and recommend engineering solutions to resolve complaints of interference to private LMR licensees. If interference arises, licensees should be prepared to provide frequency coordinators with the necessary information as expeditiously as possible.

It is also important to ensure that the FCC equipment authorization remains up-to-date by notifying the FCC of any organizational administrative changes (e.g., entity name, points of contact, address) when applicable. Organizations should maintain active awareness of construction deadlines and expiration dates, as operating pursuant to an expired license or one that terminated due to failure to construct would violate FCC rules and result in the loss of license. Licensees can also face forfeiture for unauthorized operation, though renewals filed no later than 30 days following expiration are typically granted.

Special Events

Special events are situations where RF interference is more likely to occur, as they bring diverse actors with diverse intentions into the operational environment, resulting in an increased likelihood for equipment to be installed or operated improperly. Localities may need to reconfigure their equipment or make rapid adjustments to equipment to counter the challenges that special events create.[37] Below are steps to mitigate RF interference during special events:

- Train security teams, including internal and external stakeholders, on RF interference identification, mitigation tactics, and reporting procedures;
- Monitor events with spectrum analyzers and direction-finding equipment to locate interfering signals; and
- Where possible, ensure that each participating stakeholder has communications systems in multiple bands, and a communications plan to direct back-up procedures (e.g., a Primary, Alternate, Contingency, and Emergency [PACE] plan).

[37] Some physical modifications could invalidate the equipment authorization and using different equipment may require a Special Temporary Authority (STA) request, https://www.fcc.gov/applying-special-temporary-authority. Refer to FCC guidance when modifying equipment.

In addition to these actions, public safety organizations should include knowledgeable staff experienced with RF interference in their special event operations.[38] Stakeholders are encouraged to leverage expertise from federal government entities, such as CISA, FCC, the National Telecommunications and Information Administration (NTIA), and the Wireless Spectrum Research and Development (WSRD) Interagency Working Group (IWG)[39] to support interference identification and resolution.

RF Interference Mitigation Lifecycle

The RF interference mitigation cycle includes five steps: Recognize, Respond, Report, Resolve, and Resilience. In order to robustly defend against RF interference, public safety organizations must employ these steps continuously. It is also recommended that organizations consider sharing information on RF interference with neighboring jurisdictions to further increase resiliency.

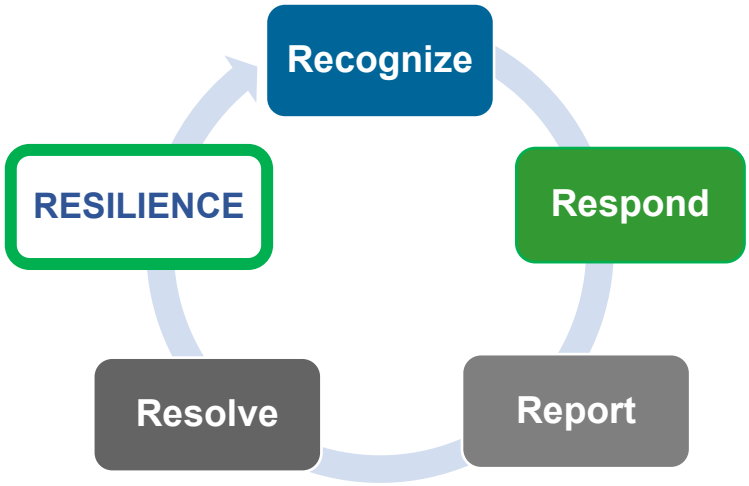

Figure 2. RF Interference Mitigation Lifecycle

Recognize

Figure 3. How to Mitigate RF Interference - Recognize

Although public safety agencies may attribute equipment failure to normal wear or general malfunctioning, disruptions in communications may result from internal or external RF interference. Per the above figure from S&T,[40] identifying the source of the RF interference is a crucial step to mitigating issues and regaining communications capabilities.

S&T offers the following recommendations for public safety network technicians, COMLs, or others responsible for recognizing and mitigating RF interference:

- Track reports of equipment malfunctions/disruptions in communications:
  - If multiple operational assets experience issues simultaneously, or if there are repeated or escalating issues at or near the same location, investigate.[41]
- Characterize the interference using a spectrum analyzer:

[38] Where applicable, agencies should review existing Tactical Interoperable Communications Plans (TICP) and Regional Interoperable Communications Plans (RICP) at the local, county, regional, state, or territorial levels for the existence of additional information or identified best practices for interference mitigation.
[39] The WSRD IWG helps coordinate research and development activities in the federal government and with academia and the private sector. For additional information, visit https://www.nitrd.gov/nitrdgroups/index.php?title=Wireless_Spectrum_Research_and_Development.
[40] DHS S&T, "First Responder Electronic Jamming Exercise," last accessed January 3, 2020.
[41] Technicians troubleshooting RF interference should be aware that narrow band equipment (e.g., 6.25 MHz) requires annual or more frequent retuning. When out of tune, this equipment is less tolerant of receiving signals and may cause RF interference.

- Is there a high noise floor?
- Is there blocking or lack of a control channel? Is the Bit Error Rate (BER) within reasonable bounds? Is audio disabled or degraded? Is the pattern discernable on a particular day of the week or at a particular time of day? Use these clues to help diagnose whether the communications are experiencing RF interference.

Respond

Figure 4. How to Mitigate RF Interference - Respond

As intentional and unintentional disturbances occur in public safety communications nationwide, it is important to know how to mitigate, capture, and maintain interference incident records. Everyday preparedness and mitigation for special events are also crucial elements of RF interference protection. The sections below outline measures agencies can take to mitigate and respond to RF interference.

Immediate Mitigation

- Alert the communications team, commander, and dispatch;
- Attempt rotating the radio antenna element 90°, so the antenna is horizontal to the terrain;
- Switch to tactical channels;
- Switch to a different means of communication, preferably on a different band (e.g., switching from cellular to UHF or VHF bands or Satellite Communications [SATCOM] could be a potential course of action);
- Shield the mobile radio behind a wall or large vehicle; and
- Find higher ground.

Capturing and Maintaining Local RF Interference Incident Records

- Report the incident to dispatch;
- After being alerted, dispatch should pass the information to the organization's internal Information Technology (IT) or Communications Division;
- The IT or Communications Division should deploy trained technicians to the area with spectrum analyzers to observe the issue; and
- Technicians should capture, catalog, and record in a local database details of the incident to track the issue in case of future occurrences in the same area.

Report

Figure 5. How to Mitigate RF Interference - Report

Capturing and Reporting RF Interference at a National Level

After performing local mitigations, it is important for officials to report RF interference to the appropriate national-level authorities. Those reporting should be prepared to provide as many details as possible on the incident, including:

- Complaining party's name, contact information, agency, date, time, duration, location, and affected mission or operations;

- Nature of the disruption (e.g., single occurrence, recurring, intermittent, or loss of signal indication), the affected equipment (e.g., type, model, application) and any devices that continue to function properly;
- Recordings, spectrum analyzer screenshots, and incident logs with location tagging;
- Environmental conditions (e.g., weather, topography, terrain, time of day);
- Steps taken to improve or regain ability to use equipment; and
- Possible cause of the disruption, information on the suspected interfering/jamming device, and details on the suspected operator of the illegal equipment (e.g., name, date of birth, vehicle tag).

Public safety organizations should report incidents to the FCC and state and local authorities (where applicable) both for potential legal action and to ensure that there are consistent records. Without complete reporting, it is impossible for the FCC, other federal agencies, and state and local authorities to fully understand the regularity and severity of RF interference incidents. This makes it challenging to identify trends such as locations, sources, and targeted bands that could help law enforcement enforce or prevent jamming. Although a few states are beginning to adopt FCC guidance on RF interference rules into their own legislation, these laws are limited and difficult to enforce. While jamming is illegal under federal law, state and local law enforcement agencies may not have the authority to confiscate or act under their laws. Jamming may also be prosecuted as interfering with police business or as cybercrime, in conjunction with jamming-specific charges.

NTIA is responsible for management of spectrum usage of the federal government. Section 8.2.30 of the NTIA *Manual of Regulations and Procedures for Federal Radio Frequency Management* addresses interference reporting procedures,[42] and the electronic reporting form is available at their website.[43]

Additionally, civilian non-aviation GPS outages can be reported to the U.S. Coast Guard (USCG), civil aviation GPS outages to the Federal Aviation Administration (FAA), while military and Department of Defense (DOD) GPS outages can be submitted to the United States Air Force (USAF) at the GPS Operations Center (GPSOC) for response.[44]

Contact information and links to additional resources are provided below:

Table 5. Authority Contact Information for RF Interference Reporting

Authority	Contact Information
FCC 24/7 Operations Center	• Website - https://fccprod.service-now.com/psix-esix/ • Phone number - (202) 418-1122 • Email - FCCOPS@fcc.gov
Non-Aviation GPS Outages: USCG	• Website - https://www.navcen.uscg.gov/?pageName=gpsUserInput
Aviation GPS Outages: FAA	• Website - https://www.faa.gov/air_traffic/nas/gps_reports/
Military GPS Outages worldwide: GPSOC	• Website - https://gps.afspc.af.mil/ (may not open for non-military users)

PIRT Reporting

The Purposeful Interference Response Team (PIRT) is an interagency organization chartered by the National Security Council (NSC) to facilitate U.S. Government collaboration with commercial owners, operators, and allies to attribute and resolve satellite interference. The PIRT includes seven core member agencies: DOD, Department of State (DOS), Department of Commerce (DOC), DHS, Department of Transportation (DOT), Office of the Director of National Intelligence (ODNI), and the FCC, with several

[42] NTIA, "Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook)," last accessed January 3, 2020.
[43] NTIA, "NTIA Interference Report Form," last accessed January 3, 2020.
[44] The GPS Operations Center (GPSOC) at Schriever Air Force Base, Colorado, is the focal point in the DOD for operational issues and questions concerning military use of GPS. The GPSOC, part of Air Force Space Command, provides DOD and allied GPS users worldwide with anomaly reports and other information 24 hours a day, seven days a week.

other conditional member agencies. The FCC is one of the founding members of the PIRT and actively supports the resolution of domestic and international instances of satellite interference.[45]

Resolve

Figure 6. How to Mitigate RF Interference - Resolve

Once public safety agencies have recognized, responded to, and reported an RF interference incident, they must resolve it by identifying lessons learned at an agency level so they can apply them to improve future incident response. To better prepare, an agency should focus on the following:

Educate

As indicated in the previous section, public safety agencies need to educate their operational personnel on how to best recognize and respond to incidents of RF interference. It is important that personnel can distinguish the different types of interferences and know which reporting process they should follow.

Prepare

Public safety agencies should update personnel and agency policies, understand interference reporting requirements, and conduct operational exercises. Agencies should also routinely conduct maintenance, upgrades, and exchange of transmission system components as they occur, and inspect transmission system components on a regular basis and after severe weather events.

It is also critical to develop a PACE Plan for communications and train all agency operators on it. The PACE Plan includes a "waterfall" of communications methods, and regular training will help all operators know what to do if their primary means of communication is disabled by RF interference or equipment failure. A PACE Plan allows agencies to pre-set their continuity plans for communications—usually switching between multiple channels, bands, or devices—ensuring that operators understand what other avenues and tools are available in case of an interruption and that all operators go to the same back-up methods in the same order. The PACE Plan should also be routinely tested and exercised to ensure its effectiveness in maintaining communications operability and resiliency.

Evaluate

Public safety agencies need to evaluate their baseline of communications resiliency by assessing how well personnel are prepared to identify, locate, and mitigate RF interference. If communications vulnerabilities are exposed, organizations should address gaps as needed, develop after action reports to review how RF interference incidents were handled, and identify lessons learned to incorporate throughout the agency.

Resilience

Figure 7. How to Mitigate RF Interference - Resilience

Applying best practices from this document will help public safety organizations become more resilient to RF interference. Everyday preparedness through training, developing and implementing standard operating procedures (SOP) for special events, and educating staff on the threats of RF interference incidents will enable entire organizations to be vigilant. When more staff learn to recognize, respond to,

[45] FCC, "Satellite Interference Monitoring and Resolution," last modified December 4, 2015.

report, and resolve RF interference incidents, the organization becomes more resilient and can return to efficiently operating without disruption.

Conclusion

RF interference is not a temporary communications issue. RF interference, including internal, external, and malicious sources, will continue to be a threat to key communications systems and mission-critical communications in public safety.

Public safety organizations may be dealing with daily RF interference, and the effects of unresolved RF interference may be detrimental to mission-critical communications. Educating and informing members of the public safety community on best practices and procedures surrounding RF interference will allow for effective response and mitigation.

The public safety community must continue to share best practices and methods to combat and protect against RF interference. Public safety organizations must work with legal authorities when responding to RF interference incidents. Except for a few states that have adopted legislation, local law enforcement agencies do not have the authority to confiscate RF jamming devices. It is important that key members of public safety organizations understand their legal and procedural capabilities and limitations associated with cases of RF interference and to whom they should report these incidents.

The guidance surrounding RF interference in the public safety space is continuing to evolve and improve. As a result, the community must continue to speak about, educate themselves, and share best practices in order to strive for communications resilience.

Appendix A: DHS RF Interference Activities

The Department of Homeland Security (DHS) has several initiatives to help the public safety community address radio frequency (RF) interference and communications resiliency. Examples include the Cybersecurity and Infrastructure Security's (CISA) RF Testing and Analysis Assistance, the Science and Technology Directorate's (S&T) First Responder Electronic Jamming Exercises (JamX),[46] development of devices to detect RF interference of communications systems, and purchasing RF interference detection and spectrum analysis equipment through grants.

CISA RF Testing & Analysis Assistance

Since September 2017, CISA has been assisting agencies with RF coverage testing and analysis, which plays a critical role throughout the life cycle of a land mobile radio (LMR) system. RF coverage testing and analysis are used to:[47]

- Define and refine system coverage requirements;
- Supplement baseline coverage studies;
- Provide supplemental information related to Coverage Acceptance Testing (CAT);
- Provide in-building coverage measurement including assistance in locating interfering signals; and
- Assist with system optimization as well as ongoing maintenance.

The RF Testing and Analysis System is also able to identify interference and signal degradation related to mobile Long-Term Evolution (LTE) systems.

S&T

2016 and 2017 First Responder Electronic Jamming Exercises

S&T is working to combat RF interference by evaluating jamming's impact, testing mitigation technologies and tactics, working with public safety agencies to update training procedures, and raising awareness of jamming threats and interference reporting channels. First, S&T hosted the 2016 JamX event, a multi-agency operational exercise at White Sands Missile Range.[48] The exercise assessed the impact of illegal jamming on public safety communications systems and mission response, and identified gaps in training, techniques, and procedures. DHS used illegal commercial-grade jamming devices that were representative of the types of jammers that public safety agencies may routinely encounter in their communities. The results proved that jamming threats could significantly impact the communications of law enforcement and public safety organizations across the country.

JamX 17 was held at the Department of Energy (DOE)'s Idaho National Laboratory (INL) and focused on strengthening resilience against jamming threats on a community and national level.[49] During JamX 17, DHS and public safety, law enforcement, private sector, and academic partners simulated the impact of jamming on a variety of communications systems and evaluated tactics and technologies to help responders better identify, locate, and mitigate the impact of jamming.[50] As a result, S&T and CISA are working together to provide robust recommendations to law enforcement and public safety agencies on how to improve their resiliency to jamming and all other forms of RF interference.

In 2021, S&T plans to host JamX 21 to further evaluate how public safety agencies have implemented DHS communications resiliency recommendations, assess advancements in counter-jamming technologies, profile non-jamming interference sources, and provide an interference testbed for industry.

[46] DHS S&T, "First Responder Electronic Jamming Exercise," last accessed January 3, 2020.
[47] DHS CISA, "Interoperable Communications Technical Assistance Program Resources", last accessed January 3, 2020..
[48] DHS S&T, "2016 First Responder Electronic Jamming Exercise," July 18, 2016.
[49] DHS S&T, "2017 First Responder Electronic Jamming Exercise," January 25, 2017.
[50] DHS S&T, "First Responder Electronic Jamming Exercise," last accessed January 20, 2020.

Table 6. DHS S&T Jamming Exercise Contact Information

Authority	Contact Information
S&T	• Website - https://www.dhs.gov/science-and-technology/ngfr • Email - Jamming.Exercise@hq.dhs.gov

Device Research and Development

S&T is partnering with private sector companies to develop a solution to identify RF interference incidents. An S&T Small Business Innovation Research Program (SBIR) grant identified three companies to develop a device that can detect RF interference, which completed the SBIR phase I in December 2018. [51] Subsequently, a SBIR phase II grant was awarded in April 2019 to one of the companies to continue development of their miniature intelligence spectral analyzer, which will alert first responders to RF interference so they can carry out back-up mitigation, and reporting procedures.[52] In addition, S&T is in development of an innovative solution toward a low-cost portable sensory device that can be used in a mobile environment to detect impacts resulting from RF signal interference from both intentional or unintentional RF sources and alert responders to the hazard.

Grants and Purchasing

S&T coordinated with the Federal Emergency Management Agency (FEMA) Grant Programs Directorate (GPD) to add two new items to the authorized equipment list (AEL) to make it easier for responders to purchase tools capable of identifying and locating RF interference using grant funding:

- **06CP-07-RFDF – Equipment, RF Direction Finding:** Devices (e.g., handheld detectors, deployable networks, fixed sensor networks) that measure, triangulate, and identify the location from which signals (including interference signals) are being transmitted;[53] and
- **06CP-07-RFSA – Equipment, RF Detection and Spectrum Analysis:** Devices that detect, identify, and analyze RF signals from radios, cellular devices, Global Positioning Systems (GPS), Wi-Fi, and other emitting devices. These devices can be used to identify transmissions from suspicious or threatening sources, including interference that may be blocking or damaging first responder communication.[54]

[51] DHS S&T, "News Release: DHS Awards Nearly $3 Million to Small Businesses for Innovative Research," May 24, 2018.
[52] DHS S&T, "News Release: Nine Small Businesses Awarded $10M to Advance Homeland Security Research Projects," May 2, 2019.
[53] FEMA, "06CP-07-RFDF - Equipment, RF Direction Finding," last accessed January 3, 2020.
[54] GovTribe,"Market Survey Report Radio Frequency (RF) Detection, Spectrum Analysis, and Direction Finding Equipment," last modified June 11, 2018.

Appendix B: Acronym List

Acronym	Definition
AEL	Authorized equipment list
AGC	Automatic gain control
BER	Bit Error Rate
CAT	Coverage Acceptance Testing
CBP	Customs and Border Protection
CISA	Cybersecurity and Infrastructure Security Agency
COML	Communications Unit Leader
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DoS	Denial-of-Service
DOS	Department of State
DOT	Department of Transportation
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FirstNet	First Responder Network Authority
GBAS	Ground-Based Augmentation System
GPD	Grant Programs Directorate
GPS	Global Positioning System
GPSOC	Global Positioning System Operations Center
HF	High frequency
ICAC	International Certification Accreditation Council
ICTAP	Interoperable Communications Technical Assistance Program
INL	Idaho National Laboratory
IT	Information Technology
ITU	International Telecommunication Union
ITU-R	International Telecommunication Union Radiocommunication Sector
IWG	Interagency Working Group
JamX	First Responder Electronic Jamming Exercise
LMR	Land mobile radio
LTE	Long-Term Evolution
NCSWIC	National Council of Statewide Interoperability Coordinators
NPSBN	Nationwide Public Safety Broadband Network
NSC	National Security Council
NTIA	National Telecommunications and Information Administration
ODNI	Office of the Director of National Intelligence
PACE	Primary, Alternate, Contingency, and Emergency
PIRT	Purposeful Interference Response Team
PSAP	Public safety answering point
RF	Radio frequency
RFIM	Radio Frequency Interference Mitigation
RR	Radio Regulations
S&T	Science and Technology Directorate
SATCOM	Satellite communications
SBIR	Small Business Innovation Research Program
SLTT	State, local, tribal, and territorial
SOP	Standard operating procedure

Acronym	Definition
TDoS	Telephony Denial-of-Service
UAS	Unmanned aircraft systems
UHF	Ultra-high frequency
USAF	United States Air Force
U.S.C.	United States Code
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
WSRD	Wireless Spectrum Research and Development
VHF	Very high frequency

Appendix C: DHS-FCC Jammer Infographic

Appendix D: Disclaimer of Liability

The *Public Safety Radio Frequency Interference Best Practices Guidebook* (hereinafter the "document") is provided by the Department of Homeland Security (DHS) and is intended to provide guidance. The document does not contain or imply any official requirements, policies, or procedures, nor does it supersede any existing official emergency operations planning guidance or requirements documents.

As a condition of the use of the document, the recipient agrees that in no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected to the document or the use of information from the document for any purpose.

DHS does not endorse any commercial product or service referenced in the document, either explicitly or implicitly. Any reference therein to any specific commercial products, processes, or services does not constitute or imply its endorsement, recommendation, or favoring by the United States Government or DHS.

The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or DHS and shall not be used for advertising or product endorsement purposes. Rules and regulations (at all levels of government) related to radio frequency (RF) interference change; it is the responsibility of the reader to ensure they remain informed and up-to-date of any changes to RF interference rules, regulations, and available technologies.