



# Resource Booklet for Reproductive Health Care Providers and Their Staffs

National Task Force on Violence Against Reproductive Health Care  
Providers  
November 7, 2022

# Table of Contents

<b>Introduction</b> .....	2
<b>Reducing Risk</b> .....	3
Reducing Risk at Places of Business .....	3
Reducing Risk at Home .....	4
Reducing Risk of Cyber Attacks.....	5
<b>Threats</b> .....	7
<b>Suspicious Packages and White Powder Letters</b> .....	8
<b>Active Shooters</b> .....	9
<b>Federal Statutes</b> .....	11
<b>Appendix A: The FACE Act</b> .....	15
<b>Appendix B: References</b> .....	18
<b>Appendix C: Example Checklists</b> .....	19

## Introduction

This instructional booklet is intended to provide reproductive healthcare providers and other similar organizations with practical information and proactive security measures that can be used to reduce risk and prevent violence against personnel and facilities. Please share this booklet with all staff members.

A series of forms and checklists with important phone numbers and procedures are included in the appendices. These can be printed out and should be placed where they are most needed.

On November 9, 1998, the Department of Justice established the Task Force on Violence Against Health Care Providers. The Assistant Attorney General for the Civil Rights Division of the Department of Justice chairs the Task Force, and the Task Force Director is an attorney with the Criminal Section of the Civil Rights Division. The Task Force is staffed by attorneys and other staff from the Civil Rights, Criminal and National Security Divisions of the Department of Justice, and by investigators and other representatives from the Federal Bureau of Investigation (FBI), the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the United States Postal Inspection Service (USPIS), and the United States Marshals Service (USMS). For additional information please visit the National Task Force on Violence Against Health Care Providers website <https://www.justice.gov/crt/national-task-force-violence-against-reproductive-health-care-providers>.

You can contact the National Task Force on Violence Against Health Care Providers at: [Clinicviolence.Taskforce@usdoj.gov](mailto:Clinicviolence.Taskforce@usdoj.gov)

A digital copy of this resource booklet can be found at the following websites:

<https://www.justice.gov/crt/security-recommendations-enhance-safety-and-protection-providers>

<https://www.fbi.gov/investigate/civil-rights>

## **Reducing Risk**

Since the passage of the Freedom of Access to Clinic Entrances (FACE) Act, 18 U.S.C. §248, in 1994, the number of large-scale clinic blockades has declined. However, incidents of violence and threats towards reproductive health care providers and their staff members have continued. Although laws exist to combat and address this behavior, providers and their staff members are encouraged to take active steps to reduce their own risk of victimization.

Forging a relationship with law enforcement in your area is an important step in reducing risk to your facility. Contact the FBI and U.S. Attorney's Office in your area to establish a liaison should you have legal questions or concerns. The U.S. Marshal's Service can provide information on improving your physical security. It is also important to establish a relationship with your local law enforcement agencies to ensure that they understand your concerns.

### **Reducing Risk at Places of Business**

Reproductive health care clinics, which includes, both abortion clinics and pregnancy centers, have been targets of arson, bombing, vandalism and other dangerous and disruptive activities. Below is a list of suggestions to reduce and mitigate the risks of such activities:

- Install dead bolt locks on office doors leading to hallways and other public areas.
- Consider installing a "buzzer" entry door system.
- Consider installing a perimeter fence.
- Managers should issue and control keys, conduct regular inventories, and have locks changed when keys are missing.
- Have offices cleaned during business hours.
- Ensure that cleaning personnel do not have access to security alarm codes.
- Instruct all employees on operation of your security system.
- Do not allow visitors access to secure areas.
- Immediately report persons who appear unannounced in your work area.
- Be cognizant of suspicious individuals loitering in public areas outside of your facility.
  - Take note of extra baggy clothing and nervous behavior.
  - Record description of suspicious persons or vehicles including license plates.
- Do not admit unexpected repair or delivery people.
- Check with a security company for information on available equipment and services.
- Install video surveillance and exterior lighting.
- Control exterior vegetation to eliminate hiding places.
- Develop a comprehensive inventory including serial numbers, pictures and values.
- Keep a list of suppliers with phone numbers, addresses and points of contact.
- Develop a list of minimum equipment and supplies needed to reestablish the clinic.
- Keep a copy of all important documents in a safe, off-site location.

- Evaluate the need for a security guard.
- Develop a written emergency response plan for threats and refresh employee training. Information can be found at: <https://www.ready.gov/business/implementation/emergency>.
- Ask local police and/or U.S. Marshal Service to evaluate your emergency response plan.
- Keep bomb threat/personal threat checklists by each telephone and ensure staff is familiar with the forms, which can be found at: <https://www.cisa.gov/publication/dhs-bomb-threat-checklist>.

## **Reducing Risk at Home**

Anti-abortion and pro-choice extremist activity is not always confined to public places. Reproductive healthcare providers and their staff members have also been targeted for protest activity at their private residences. Most often, this activity consists of picketing, leafleting, or posting flyers in residential neighborhoods. Many cities and towns have enacted residential picketing laws in order to restrict or prevent picketing at private residences. The National Abortion Federation compiled a list of such injunctions and ordinances and listed them by state. The list is not exhaustive and is current as of 2017. To obtain a copy of this legal remedies resource, contact the National Abortion Federation: <http://www.prochoice.org>.

In addition to picketing, some extremists have also engaged in stalking, vandalism and even murder. The following is a list of safety measures providers and their staff members may want to incorporate in order to reduce their risk of being victimized at home:

- Do not put your name on the outside of your residence or mailbox.
- Install an appropriate security system.
- Have good outside lighting.
- Control vegetation to eliminate hiding places.
- Entrances should have deadbolt locks and one-way peep-holes.
- Account for all copies of house keys.
- Change locks if keys are lost or stolen and when moving to a new residence.
- Keep doors locked, even if you are at home.
- Develop friendly relationships with neighbors.
- Arrange for unlisted/unregistered home and mobile telephone numbers.
- Use a timer to turn lights on and off at varying times and locations.
- Leave a radio playing while you are away (best with a timer).
- Notify the police or a trusted neighbor of your absence.
- Report and maintain a record of all suspicious activity.
- Ensure law enforcement is aware of any concerns you may have.

## **Reducing Risk of Cyber Attacks**

According to National Abortion Federation statistics, between the years 2010 and 2019 abortion providers reported over 128,000 incidents of either hate email or internet harassment. And, since the United States Supreme Court's 2022 decision in *Dobbs v. Jackson Women's Health Organization*, which overruled *Roe v. Wade*, and removed the Constitutional protections afforded to abortion care, pregnancy centers and other anti-abortion organizations have reported a significant increase in such incidents at their facilities. In addition to threats and harassment, providers and their staff members have had their photographs and personal information posted online, making them targets for cyber stalking and other types of cyber crimes. As uses of the internet and social media continue to increase, ideologically driven individuals may choose to target reproductive healthcare centers, providers and their staff for a variety of cyber attacks. These attacks can include phishing (attempts to obtain financial or other confidential information from internet users, typically by sending an email that looks as if it is from a legitimate organization, but contains a link to a fake website that replicates the real one); denial of service attacks (attacks designed to incapacitate a network by flooding it with useless traffic); defacement of websites (attacks changing the visual appearance of a website); and computer intrusion to either steal or demand ransom for clinic data about staff and patients. Following these tips on your work and home computers and internet connected devices will help reduce the risk of victimization:

### **Users**

- Verify the spelling of web addresses, websites, and email addresses that look trustworthy but may be imitations of legitimate election websites.
- Update anti-malware and anti-virus software and conduct regular scans.
- Do not enable macros on documents downloaded from an email unless absolutely necessary, and after ensuring the file is not malicious.
- Do not open emails or attachments from unknown individuals. Do not communicate with unsolicited email senders.
- Never provide personal information of any sort via email. Be aware that many emails requesting your personal information may appear to be legitimate.
- Disable or remove unneeded software applications.
- Verify the website you visit has a Secure Sockets Layer (SSL) certificate.

### **IT Administrators**

- Require multi-factor authentication for remote access to IT networks.
- Enable strong spam filters to prevent phishing emails from reaching end users. Filter emails containing executable files from reaching end users.
- Implement a user training program and simulated attacks for spear phishing to discourage users from visiting malicious websites or opening malicious attachments and reinforce the appropriate user responses to spear phishing emails.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by

- implementing URL blocklists and/or allow lists.
- Update software, including operating systems, applications, and firmware on IT network assets, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to determine which OT network assets and zones should participate in the patch management program.

### **Victim Reporting and Additional Information**

The FBI encourages the public to report information concerning suspicious or criminal activity to their local field office ([www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices)) or the FBI's Internet Crime Complaint Center ([www.ic3.gov](http://www.ic3.gov)).

## Threats

Although certain behaviors can be upsetting, the FACE Act criminalizes only those threats that are “true threats.” A true threat is defined as a serious communication of an intent to commit an act of unlawful violence against an individual or group. Absent additional circumstances, carrying graphic signs, videotaping patients or doctors, writing down license plates, and even screaming or shouting would not typically rise to the level of a being considered a true threat.

With the explosion of internet use and social media, cyber threats are no longer limited to just threats received via email. Threats can be posted on message boards, social media pages, and comments sections. These threats don’t have to be posted on the provider’s sites or social media to be considered threats. Threats can be posted on the comments section of a news story or in issue-specific chat rooms. Regardless of where the threat is found, it should be taken very seriously.

The following steps should be taken for threats:

- Notify local law enforcement if there is any reason to believe the threat is imminent.
- For cyber threats:
  - Take a screen shot, print a copy, and/or download an electronic copy if possible.
  - Immediately notify your IT and security professionals.
  - Do not delete the threat message.
- For threats received by telephone:
  - Use a bomb checklist to record information (see example in Appendix C below).
  - Do not hang up – even if the caller does.
  - Stay calm and ask the caller as many questions about the threat as possible.
  - Note as many details about the caller as possible.
  - Record the telephone number of the caller.
- For threats received by mail:
  - Limit the number of people that handle the letter to preserve evidence.
  - See the below section on Suspicious Packages
- Notify the local FBI office.

# Suspicious Packages and White Powder Letters

## Characteristics of a suspicious package:

- Packages that you are not expecting or from businesses/people you are not familiar with.
- Words spelled incorrectly.
- Return address and postmark do not match.
- Envelope is addressed generically to “Medical Director” or “Security Director.”
- No return addresses or return address typed on adhesive labels.
- Possibly mailed from outside the U.S.
- Envelopes or packages from businesses with no business stationary.
- Protruding wires.
- Strange odor, oily stains, discolorations, or crystallization on wrapper.
- Excessive tape or string.
- Excessive postage.
- Granular material in the package.
- Rigidity or bulkiness.

## If you discover a suspicious letter or package:

- Do not open it.
- Treat it as suspect.
- Isolate it—don’t handle.
- Contact building security, if available.
- *If there is a medical emergency or chemical reaction with a letter or package, call 911.*

## If you suspect a bomb:

- Evacuate immediately.
- Call 911 for police, fire and hazmat unit.
- Move to designated meeting area away from the building.

## If there is a release of gas or powder:

- Turn off fans or ventilation units and shut down the air handling system in the building.
- Leave area immediately.
- Close the door or section off the area to prevent others from entering.
- Notify your building security official or a supervisor and call 911.
- List all people who were in the room or area. Give the list to public health authorities.
- FBI will conduct a thorough risk and threat assessment. The item will then be transported by the FBI laboratory for testing.

## **Active Shooters**

On November 27, 2015, Robert Lewis Dear, Jr. attacked a Planned Parenthood clinic in Colorado Springs, Colorado. A police officer and two civilians were killed; five police officers and four civilians were injured. After a standoff that lasted five hours, police SWAT teams crashed armored vehicles into the clinic's lobby and the attacker surrendered.

An "active shooter" is an individual who is engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms and there is no pattern or method to their selection of victims.

When an active shooter is in your vicinity, you must be prepared both mentally and physically to deal with the situation. You have three options:

### **RUN**

- Wherever you go, be aware of alternate exits.
- Quickly and cautiously evacuate in a direction away from the attacker.
- Don't hesitate. Seconds matter.
- Remember windows and emergency exits.
- Leave belongings behind.
- Keep empty hands raised and clearly visible.
- Follow all instructions from the police.
- Don't stop until you are sure you have reached a safe location.

### **HIDE**

- If there is no safe escape route, find a good hiding place.
- Lock and barricade the door.
- Silence cell phones.
- Prepare a defense plan.

### **FIGHT**

- Fight only as a last resort.
- Use available objects as improvised weapons.
- Use teamwork and surprise, a coordinated ambush can incapacitate an attacker.
- You are fighting for your life, don't fight fair!

### **Information to provide to 911 operations:**

- Location of the active shooter (provide street address if possible).
- Number of shooters.

- Physical description of shooter.
- Number and type of weapons shooter has.
- Number of potential victims at location.

**When law enforcement arrives (typical law enforcement response is three minutes):**

- Remain calm and follow instructions.
- Drop items in your hands (e.g., bags, jackets).
- Raise hands and spread fingers.
- Keep hands visible at all times.
- Avoid quick movements toward officers, such as holding on to them for safety.
- Avoid pointing, screaming or yelling.
- Do not ask questions when evacuating.

The first officers to arrive on scene will not stop to help the injured. Responding officers will move to the sounds of gun fire with the intent to neutralize the shooter. Expect rescue teams to follow initial officers. These rescue teams will treat and remove the injured.

Once you have reached a safe location, you will likely be held in that area by law enforcement until the situation is under control and all witnesses have been identified and questioned. Do not leave the area until law enforcement authorities have instructed you to do so.

More information including a video to show employees can be found on the FBI website at <https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources>.

Another good source of information is the DHS website at <https://www.cisa.gov/active-shooter-preparedness>.

## **Federal Statutes**

From the mid-1980s through the 1990s, clinic violence and harassment escalated across the nation. Clinics experienced increased blockades, arsons, bomb threats, death threats, vandalism, and harassment. On March 10, 1993, the first murder of a reproductive health care provider occurred. Dr. David Gunn, a physician who provided abortion services, was murdered during an anti-abortion protest at a Pensacola, Florida clinic. In response to the alarming trend of increased violence, the U.S. Congress enacted the Freedom of Access to Clinic Entrances (FACE) Act, Title 18 of the U.S. Code, Section 248, in May of 1994. In addition to the FACE Act, the below laws and others not listed may be used in the investigation and prosecution of illegal acts against reproductive health care providers and their staffs.

### **Freedom of Access to Clinic Entrances (FACE) Act, 18 U.S.C. § 248**

The FACE Act makes it a federal crime to use force, threat of force, or physical obstruction to intentionally injure, intimidate, or interfere with persons because they are seeking or providing reproductive health services, or to intimidate others or attempts to injure, intimidate, or interfere with any person because they are seeking or providing such services. In addition, the law prohibits damage or destruction of the property of a facility because the facility provides reproductive health care services. Violators of the FACE Act are subject to criminal penalties, including imprisonment and fines. The severity of the punishment depends upon the nature of the offense and whether or not the person is a repeat offender. The FACE Act also allows providers and seekers of reproductive health care services, the United States Attorney General, and State Attorneys General to sue for civil remedies against conduct which violates the Act. The civil remedies can include injunctions, including buffer zones, and monetary damages. The full text of the FACE Act is set forth in Appendix A.

The FACE Act does not reach all forms of abusive conduct directed at reproductive health care providers. For example, patients and staff may often feel “intimidated” or “interfered with” by people expressing anti-abortion or pro-choice views. However, absent use of force, threat of force, or an act of physical obstruction, offensive conduct is not prohibited by the FACE Act. Nonetheless, the FACE Act is an important means of combating and deterring violence and threats of violence against all reproductive health care providers and patients. If you feel that you have been a victim of conduct in violation of the FACE Act, notify your local FBI or United States Attorney’s Office. Contact information for your local FBI office can be found here:

<https://www.fbi.gov/contact-us/field-offices>.

Contact information for your local U.S. Attorney’s Office can be found here:

<https://www.justice.gov/usao/us-attorneys-listing>.

### **Conspiracy Against Rights, 18 U.S.C. § 241**

Section 241 of Title 18 establishes a federal criminal offense where two or more persons to conspire to injure, oppress, threaten, or intimidate any person in the exercise or enjoyment of any right or privilege secured to him or her by the Constitution or laws of the United States, which includes a violation of the FACE Act. The charge carries a penalty of up to 10 years imprisonment; or, if death results from the acts or if such acts involve kidnapping or an attempt to kidnap, aggravated sexual abuse or attempt to commit aggravated sexual abuse, or an attempt to kill, the offender may be sentenced to any term of years, or for life, or in certain cases may be sentenced to death.

### **Damage or Destruction of Property Used in Interstate Commerce, 18 U.S.C. § 844(i)**

Section 844(i) of Title 18 establishes a federal criminal offense where an individual “maliciously damages or destroys, or attempts to damage or destroy, by means of fire or an explosive, any building, vehicle, or other real or personal property used in interstate or foreign commerce or in any activity affecting interstate or foreign commerce.”

Since many reproductive health services clinics serve patients from other states and order medical supplies from other states, clinics may qualify as property used in interstate commerce. Charges under § 844(i) frequently have been brought in cases of arson or bombing of reproductive health services clinics. The charge carries a penalty of 5 to 20 years in prison absent physical injury and 7 to 40 years if injury results. Where death results from a violation of this statute, the offender may be sentenced to death.

### **Use of a Firearm in the Commission of a Felony, 18 U.S.C. § 924(c)**

Section 924(c) of Title 18 establishes a federal criminal offense where an individual uses or carries a firearm during or in relation to a crime of violence or drug trafficking crime prosecutable in federal court, or, in furtherance of any such crime, possesses a firearm. The mandatory minimum penalty is 5 years imprisonment. The penalty increases to 7 years if the firearm is brandished during the offense, and 10 years if it is discharged. Penalties for subsequent offenses are significantly increased, as are penalties for the use of certain illegal and proscribed firearms and silencers. The use of a firearm in the commission of a felony offense related to a clinic might warrant prosecution under § 924(c).

### **Use of the Mails or Commerce for Bomb or Fire Threats, 18 U.S.C. § 844(e)**

Section 844(e) of Title 18 establishes a federal criminal offense to use the United States Mail, a telephone, or other instrument of interstate commerce to communicate a threat or to convey false information concerning a threat. Cases brought under § 844(e) generally involve bomb or arson threats. This offense carries a penalty of up to 10 years imprisonment.

### **Threats Made by Use of Interstate or Foreign Commerce, 18 U.S.C. §§ 875 and 876**

These statutes prohibit the use of interstate or foreign commerce, generally telephones, internet communications and electronic mail, and the mails, to convey threats to kidnap or injure another. Increased penalties are provided where the threat is made with the intent to extort a “thing of value.” Courts have found that actions taken for the purpose of harming a business (including a clinic) may demonstrate an intent to extort a thing of value. The Department of Justice has used § 875 to prosecute a case involving computer-generated threats made by electronic mail to, among others, reproductive health care providers. Violations of this statute carry a penalty of up to 20 years in prison.

### **Interference with Commerce by Threats or Violence, 18 U.S.C. § 1951**

Section 1951, more commonly referred to as the “Hobbs Act,” prohibits conduct that obstructs, delays or affects commerce by means of robbery or extortion. The statute also covers attempts to commit these acts, conspiracy to commit the acts, and any threats made to cause injury or damage to a person or property in order to commit these acts. Attempts to coerce a reproductive health care provider to limit or halt operations may constitute a violation of this statute. Violations carry a penalty of up to 20 years in prison.

### **Interstate Travel or Transportation to Aid in Racketeering Enterprises, 18 U.S.C. § 1952**

More commonly referred to as the “Travel Act,” Section 1952 sets a penalty of up to 5 years for persons who either travel in interstate or foreign commerce, or use the mails or other facility in interstate or foreign commerce, to commit any crime of violence in furtherance of some unlawful activity, or to promote, manage, establish, carry on or facilitate the promotion, management, establishment or carrying on of any unlawful activity. In sum, this statute makes it illegal to travel between states, or between another country and the United States, in order to commit certain illegal acts. Traveling across state lines to perpetrate a crime of violence against a reproductive health care provider might warrant prosecution under § 1952.

### **Use of Certain Weapons of Mass Destruction, 18 U.S.C. § 2332a**

Section 2332a prohibits the use, threat of use, or attempted or conspired use of a weapon of mass destruction, including a biological agent, toxin, or vector against any person within the United States the results of which affect interstate commerce. The term “weapon of mass destruction” is also defined under this Section and includes any destructive device as defined under § 921 of this title, any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; any weapon involving a disease organism; or any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. Use or threatened use of a chemical weapon is covered under 18 U.S.C. § 229. The offender is eligible to be sentenced to any term of years, or for life, or in certain cases may be sentenced to death.

## **Concurrent Jurisdiction with State and Local Authorities**

Many criminal activities that affect reproductive health care providers constitute crimes at the federal, state, and local level. Many jurisdictions have local ordinances for trespassing and disorderly conduct, for example, which may prohibit conduct not covered by a federal statute. Some states have adopted statutes almost identical to FACE, providing for concurrent jurisdiction in many cases.

Charging decisions involving offenses related to reproductive health care providers generally are made by the Civil Rights Division's Criminal Section in consultation with United States Attorney's Office (USAO) and in cooperation with state and local authorities. Per a July 31, 2009, directive from the Attorney General, USAOs must notify the Criminal Section of the Civil Rights Division immediately upon learning of any potential FACE Act violations within their district and to consult with the Criminal Section prior to making any charging or non-charging decisions.

## **Civil Remedies**

In addition to criminal penalties that may arise in relation to conduct affecting reproductive health care providers, federal law provides for civil remedies where private parties or the federal or state governments bring suit.

Civil actions under the FACE Act may be brought by an aggrieved private party (such a health care provider), the United States Attorney General, or the Attorney General for any state. As a general matter, establishing a civil violation under the FACE Act requires proof of the same elements outlined in the criminal discussion of the statute. However, the remedies available in the civil context differ, and may include injunctive relief, civil penalties, actual or statutory damages, punitive damages, and attorney fees for actions that are not brought by a government. Additionally, in a civil case, the private or public plaintiff need only prove the case by a preponderance of the evidence, rather than beyond a reasonable doubt.

The United States Department of Justice, through the Special Litigation Section of the Civil Rights Division, has secured a number of important decisions using the civil remedies of the FACE Act to win permanent injunctive relief against persons who violated the Act in the context of blockades, "lock-and-blocks," threats, and other obstructive conduct. The government has secured judgments that bar specific defendants from entering the property of certain clinics, and the government has secured rulings requiring "buffer zones" around clinics in order to balance the interests of legitimate and protected protest and the rights of clinics to operate their legal businesses.

For more information regarding the civil aspects of the Freedom of Access to Clinic Entrances Act, visit the Special Litigation Section's webpage at <https://www.justice.gov/crt/special-litigation-section>.

## Appendix A: The FACE Act

### Freedom of Access to Clinic Entrances (FACE) Act of 1994 – Title 18 U.S. Code, Section 248

#### (a) PROHIBITED ACTIVITIES- Whoever-

(1) by force or threat of force or by physical obstruction, intentionally injures, intimidates or interferes with or attempts to injure, intimidate or interfere with any person because that person is or has been, or in order to intimidate such person or any other person or class of persons from, obtaining or providing reproductive health services;

(2) by force or threat of force or by physical obstruction, intentionally injures, intimidates or interferes with or attempts to injure, intimidate or interfere with any person lawfully exercising or seeking to exercise the First Amendment right of religious freedom at a place of religious worship; or

(3) intentionally damages or destroys the property of a facility, or attempts to do so, because such facility provides reproductive health services, or intentionally damages or destroys the property of a place of religious worship, shall be subject to the penalties provided in subsection (b) and the civil remedies provided in subsection (c), except that a parent or legal guardian of a minor shall not be subject to any penalties or civil remedies under this section for such activities insofar as they are directed exclusively at that minor.

#### (b) PENALTIES- Whoever violates this section shall -

(1) in the case of a first offense, be fined in accordance with this title, or imprisoned not more than one year, or both; and

(2) in the case of a second or subsequent offense after a prior conviction under this section, be fined in accordance with this title, or imprisoned not more than 3 years, or both; except that for an offense involving exclusively a nonviolent physical obstruction, the fine shall be not more than \$10,000 and the length of imprisonment shall be not more than six months, or both, for the first offense; and the fine shall be not more than \$25,000 and the length of imprisonment shall be not more than 18 months, or both, for a subsequent offense and except that if bodily injury results, the length of imprisonment shall be not more than 10 years, and if death results, it shall be for any term of years or for life.

(c) CIVIL REMEDIES-

(1) RIGHT OF ACTION

(A) IN GENERAL - Any person aggrieved by reason of the conduct prohibited by subsection (a) may commence a civil action for the relief set forth in subparagraph (B), except that such an action may be brought under subsection (a)(1) only by a person involved in providing or seeking to provide reproductive health services, and such an action may be brought under subsection (a)(2) only by a person lawfully exercising or seeking to exercise the First Amendment right of religious freedom at a place of worship or by the entity that owns or operates such a place of worship.

(B) RELIEF- In any action under subparagraph (A), the court may award appropriate relief, including temporary, preliminary or permanent injunctive relief and compensatory and punitive damages, as well as the costs of suit and reasonable fees for attorneys and expert witnesses. With respect to compensatory damages, the plaintiff may elect, at any time prior to the rendering of final judgment, to recover, in lieu of actual damages, an award of statutory damages in the amount of \$5,000 per violation.

(2) ACTION TAKEN BY ATTORNEY GENERAL OF THE UNITED STATES

(A) IN GENERAL - If the Attorney General of the United States has reasonable cause to believe that any person or group of persons is being, has been, or may be injured by conduct constituting a violation of this section, the Attorney General may commence a civil action in any appropriate United States District Court.

(B) RELIEF - In any action under subparagraph (A), the court may award appropriate relief, including temporary, preliminary or permanent injunctive relief, and compensatory damages to persons aggrieved as described in paragraph (1)(B). The court, to vindicate the public interest, may also assess a civil penalty against each respondent—

(i) in an amount not exceeding \$10,000 for a nonviolent physical obstruction and \$15,000 for other first violation; and

(ii) in an amount not exceeding \$15,000 for a nonviolent physical obstruction and \$25,000 for any other subsequent violation.

(3) ACTIONS BY STATE ATTORNEYS GENERAL

(A) IN GENERAL- If the Attorney General of a State has reasonable cause to believe that any person or group of persons is being, has been, or may be injured by conduct constituting a violation of this section, such Attorney

General may commence a civil action in the name of such State, as parens patriae on behalf of natural persons residing in such State, in any appropriate United States District Court.

(B) RELIEF- In action under subparagraph (A), the court may award appropriate relief, including temporary, preliminary or permanent injunctive relief, compensatory damages, and civil penalties as described in paragraph (2)(B).

DEFINITIONS—As used in this section:

(1) FACILITY- The term 'facility' includes a hospital, clinic, physician's office, or other facility that provides reproductive health services, and includes the building or structure in which the facility is located.

(2) INTERFERE WITH- The term 'interfere with' means to restrict a person's freedom of movement.

(3) INTIMIDATE- The term 'intimidate' means to place a person in reasonable apprehension of bodily harm to him/herself or to another.

(4) PHYSICAL OBSTRUCTION- The term 'physical obstruction' means rendering impassable ingress to or egress from a facility that provides reproductive health services or to or from a place of religious worship, or rendering passage to or from such a facility or place of religious worship unreasonably difficult or hazardous.

(5) REPRODUCTIVE HEALTH SERVICES- The term 'reproductive health services' means reproductive health services provided in a hospital, clinic, physician's office, or other facility, and includes medical, surgical, counseling or referral services relating to pregnancy or the termination of a pregnancy.

(6) STATE- The term 'State' includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

## Appendix B: References

### Government Agencies

Department of Justice Civil Rights Division	<a href="https://www.justice.gov/crt">https://www.justice.gov/crt</a>
Federal Bureau of Investigation	<a href="https://www.fbi.gov">https://www.fbi.gov</a>
US Marshals Service	<a href="http://www.usmarshals.gov">http://www.usmarshals.gov</a>
Bureau of Alcohol, Tobacco, Firearms	<a href="https://www.atf.gov">https://www.atf.gov</a>
US Postal Inspection Service	<a href="https://postalinspectors.uspis.gov">https://postalinspectors.uspis.gov</a>
Federal Emergency Management Agency	<a href="http://www.fema.gov">http://www.fema.gov</a>

### Non-Governmental Organizations

Planned Parenthood	<a href="https://www.plannedparenthood.org">https://www.plannedparenthood.org</a>
National Abortion Federation	<a href="http://prochoice.org">http://prochoice.org</a>
Feminist Majority Foundation	<a href="http://feminist.org">http://feminist.org</a>
Care Net	<a href="https://www.care-net.org">https://www.care-net.org</a>
Heartbeat International	<a href="https://www.heartbeatinternational.org">https://www.heartbeatinternational.org</a>
National Institute of Family and Life Advocates	<a href="https://nifla.org">https://nifla.org</a>

### Information on Cyber Threats

Department of Homeland Security Cyber Security Information
<a href="https://www.dhs.gov/topic/cybersecurity">https://www.dhs.gov/topic/cybersecurity</a>
More information of Cyber Crimes
<a href="https://www.fbi.gov/investigate/cyber">https://www.fbi.gov/investigate/cyber</a>
Internet Crimes Complaint Center
<a href="http://www.ic3.gov">http://www.ic3.gov</a>

### Information on Bomb Threats

DHS Bomb Threat Checklist
<a href="https://www.cisa.gov/publication/dhs-bomb-threat-checklist">https://www.cisa.gov/publication/dhs-bomb-threat-checklist</a>
FBI suspicious package info sheet
<a href="https://www.fbi.gov/file-repository/suspicious-package-indicators.pdf/view">https://www.fbi.gov/file-repository/suspicious-package-indicators.pdf/view</a>
FEMA Emergency Response Plan
<a href="https://www.ready.gov/explosions">https://www.ready.gov/explosions</a>
More information on Emergency Response Plans
<a href="https://www.ready.gov/business/implementation/emergency">https://www.ready.gov/business/implementation/emergency</a>

### Information on Active Shooters

FBI Active Shooter Video
<a href="https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources">https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources</a>
DHS Active Shooter resources
<a href="https://www.cisa.gov/active-shooter-preparedness">https://www.cisa.gov/active-shooter-preparedness</a>

## Appendix C: Example Checklists



*The National Explosives Task Force (NETF) coordinates rapid integration of explosives expertise with intelligence and law enforcement information to support operational activities. Products are peer-reviewed by explosives experts from participating agencies.*

### National Explosives Task Force

#### Suspicious Package Indicators and Recommended Response Procedures

Package bombs, which include letters, parcels, and anything delivered by postal or courier service, are not a new technique and have been used by terrorists and anarchist groups. Many of these bombs are triggered when victims handle or open the packages, although they can be initiated in other ways.

Package bombs come in a variety of shapes and sizes, and they may look harmless. There are a number of characteristics that may lead you to become suspicious of a letter or package.

If you believe a letter or package is suspicious:

- Stop. Do not handle or open.
- Do not use cell phones, pagers, or two-way radios near suspected devices.
- Be aware of secondary devices.
- Evacuate and isolate the immediate area.
- If applicable, activate the facility's emergency plan.
- Make note of the characteristics that caused suspicion.
- Call 911.

#### Formal Screening Procedures

Commercial or government entities with mail screening procedures are advised to review existing procedures for screening packages, identifying suspicious items, and instituting the appropriate safety protocols. If no current procedures are in place, guidance should be

**SUSPICIOUS MAIL OR PACKAGES**

**Protect yourself, your business, and your mailroom.**

**If you receive a suspicious letter or package:**

- Stop. Don't handle.
- Isolate it immediately.
- Don't open, smell, or taste.
- Activate your emergency plan. Notify a supervisor.

Restrictive markings. No return address. Sealed with tape. Misspelled words. Badly typed or written. Unknown powder or suspicious substance. Possibly mailed from a foreign country. Excessive postage. Protruding wires. Rigid or bulky. Legible or unclean. Incorrect bills or addressed to title only. Strange odor. Oily stains, discolorations, crystallization on wrapper. Excessive tape.

**If you suspect the mail or package contains a bomb (explosive), or radiological, biological, or chemical threat:**

- Isolate area immediately
- Call 911
- Wash your hands with soap and water

sought from local, state, and/or federal resources. Planning considerations should include (but not be limited to) recurring training for screeners, an understanding of the standards and limitations for operating times, and regularly scheduled maintenance of screening equipment, such as calibration, updates, and testing.

### **Response Procedures**

The NETF prepared this document to raise awareness of package bombs and the need for diligence and safety procedures in evaluating suspected improvised explosive devices. If a suspicious package is found, call 911. Any diagnostic or render safe actions should be performed only by FBI Hazardous Devices School (HDS) certified public safety bomb technicians or current U.S. military explosive ordnance disposal technicians.

The U.S. government has resources on mail security available to citizens and businesses. More information can be found at <http://about.usps.com/securing-the-mail/mail-security-center.htm>

To report suspicious activity, call 911 or contact local law enforcement.

Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit: <https://nsi.ncirc.gov/resources.aspx>.

*March 2018*

#### When law enforcement arrives:

- Remain calm and follow instructions.
- Drop items in your hands. (e.g., bags, jackets)
- Raise hands and spread fingers.
- Keep hands visible at all times.
- Avoid quick movements toward officers, such as holding on to them for safety.
- Avoid pointing, screaming or yelling.
- Do not ask questions when evacuating.

#### Information to provide to 911 operators:

- Location of the active shooter.
- Number of shooters.
- Physical description of shooters.
- Number and type of weapons shooter has.
- Number of potential victims at location.

#### For questions or additional assistance contact:

Your local FBI Office:

FBI Headquarters National Press Office: (202) 324-3691



Federal Bureau of Investigation  
935 Pennsylvania Avenue, NW  
Washington, DC 20535

U.S. Department of Justice  
Federal Bureau of Investigation



## ACTIVE SHOOTER EVENT QUICK REFERENCE GUIDE

An active shooter is an individual actively engaged in killing or attempting to kill people in a populated area.

- › *Victims are selected at random.*
- › *Event is unpredictable and evolves quickly.*
- › *Knowing what to do can save lives.*

## ACTIVE SHOOTER EVENTS

When an Active Shooter is in your vicinity, you must be prepared both mentally and physically to deal with the situation.

### You have three options:

#### 1 RUN

- Have an escape route and plan in mind.
- Leave your belongings behind.
- Evacuate regardless of whether others agree to follow.
- Help others escape, if possible.
- Do not attempt to move the wounded.
- Prevent others from entering an area where the active shooter may be.
- Keep your hands visible.
- Call 911 when you are safe.

#### 2 HIDE

- Hide in an area out of the shooter's view.
- Lock door or block entry to your hiding place.
- Silence your cell phone (including vibrate mode) and remain quiet.

#### FIGHT 3

- Fight as a last resort and only when your life is in imminent danger.
- Attempt to incapacitate the shooter.
- Act with as much physical aggression as possible.
- Improvise weapons or throw items at the active shooter.
- Commit to your actions . . . your life depends on it.

The first officers to arrive on scene will not stop to help the injured. Expect rescue teams to follow initial officers. These rescue teams will treat and remove the injured.

Once you have reached a safe location, you likely will be held in that area by law enforcement until the situation is under control and all witnesses have been identified and questioned. Do not leave the area until law enforcement authorities have instructed you to do so.

# BOMB THREAT PROCEDURES

This quick reference checklist is designed to help employees and decision makers of commercial facilities, schools, etc. respond to a bomb threat in an orderly and controlled manner with the first responders and other stakeholders.

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of call, DO NOT HANG UP, but from a different phone, contact authorities immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call \_\_\_\_\_
- Handle note as minimally as possible.

If a bomb threat is received by e-mail:

- Call \_\_\_\_\_
- Do not delete the message.

## Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

\*Refer to your local bomb threat emergency response plan for evacuation criteria

## DO NOT:

- Use two-way radios or cellular phone. Radio signals have the potential to detonate a bomb.
- Touch or move a suspicious package.

## WHO TO CONTACT (Select One)

- **911**
- **Follow your local guidelines**

For more information about this form contact the Office for Bombing Prevention at: [OBP@cisa.dhs.gov](mailto:OBP@cisa.dhs.gov)



# BOMB THREAT CHECKLIST

DATE:

TIME:

TIME CALLER HUNG UP:

PHONE NUMBER WHERE CALL RECEIVED:

## Ask Caller:

- Where is the bomb located? (building, floor, room, etc.)

- When will it go off?

- What does it look like?

- What kind of bomb is it?

- What will make it explode?

- Did you place the bomb? Yes No

- Why?

- What is your name?

## Exact Words of Threat:

## Information About Caller:

- Where is the caller located? (background/level of noise)

- Estimated age:

- Is voice familiar? If so, who does it sound like?

- Other points:

### Caller's Voice

### Background Sound

### Threat Language

Female

Male

Accent

Angry

Calm

Clearing throat

Coughing

Cracking Voice

Crying

Deep

Deep breathing

Disguised

Distinct

Excited

Laughter

Lisp

Loud

Nasal

Normal

Ragged

Rapid

Raspy

Slow

Slurred

Soft

Stutter

Animal noises

House noises

Kitchen noises

Street noises

Booth

PA system

Conversation

Music

Motor

Clear

Static

Office machinery

Factory machinery

Local

Long distance

Incoherent

Message read

Taped message

Irrational

Profane

Well-spoken

Other Information: