PERSONAL SECURITY CONSIDERATIONS ACTION GUIDE: CRITICAL INFRASTRUCTURE WORKERS

INTRODUCTION

In today's current threat environment, remaining vigilant and taking responsibility for your personal security is crucial for all critical infrastructure workers—both on and off the job. Critical infrastructure workers perform a vast array of services that operate, run and maintain key systems and assets necessary for modern American life. Being mindful of any risks or threats associated with your line of work and following all safety procedures will help protect you, those close to you and the infrastructure you serve. Personal safety can be broken into three main parts—Physical Security, Situational Awareness and Online Security. This non-exhaustive action guide can help you assess your security posture and provides options to consider to mitigate threats.[1]

ASSESSING AN APPROPRIATE LEVEL OF PROTECTION FOR CRITICAL INFRASTRUCTURE WORKERS

This guide provides a broad overview of how to stay safe at home, at work, in public and online. It is up to you to decide what measures are most appropriate for your lifestyle, security vulnerabilities and the situations you might encounter.

When assessing your security needs, consider the following:

- **Your occupation and professional role.** Does your job or career make you an attractive target?
- **Specific threats.** Is there credible evidence that suggests a risk to you?
- **Your personal history.** Have you been targeted or threatened in the past?
- **Your personal visual identifiers.** Do you display any group affiliations that make you an attractive target?

Today, critical infrastructure workers potentially face a wide range of threats—from common criminal activity to violent extremists plots. If you answered yes to any or all of the above questions, this could indicate that you and potentially other critical infrastructure employees you work with are at risk and you should evaluate your security needs. As you assess your personal security, it is important to take a balanced approach and remember to account for both your home and work life—**be vigilant in your personal security practices, habits and continually assess your surroundings.** Measures you take should be appropriate for perceived threats. Excessive security actions may cause unnecessary stress and inconvenience; however, insufficient efforts can put you at risk.

The ability to recognize vulnerable situations is vital in order to avoid them or be prepared when they occur. Vulnerability is a physical feature or operational attribute that renders an entity, asset, system, network or geographic area open to exploitation or susceptible to a given hazard.[2] Attackers can be creative when they target individuals. An attacker's goal may be to cause embarrassment, inconvenience, distress or they may intend to cause physical injury, disrupt wellbeing or threaten human lives.

PHYSICAL SECURITY

PROTECTING YOUR HOME

There are a variety of simple measures to consider that can help protect you and your home. Start with installing or improving security systems that surround your residence or property. Secure any doors or windows with locks, keys, alarms, lights and assess the requirement for a closed-circuit television (CCTV) system. Consider the use of an advanced locking system for entry ways and windows with a monitored (multi-view capable) video surveillance system.

1 ProtectUK. 2022. Publicly accessible locations (PALs) guidance: Personal security. Accessed August 8, 2023. protectuk.police.uk/personal-security.

2 U.S. Department of Homeland Security. Risk Steering Committee. 2010. DHS Risk Lexicon 2010 Edition. Accessed August 8, 2023. cisa.gov/resources-tools/resources/dhs-risk-lexicon.

Maintain outdoor property structures like walls and fences and make sure any tools or ladders that could be used to access your home are securely stored. Consider removing anything that could be used to cause damage, such as loose bricks, large stones and garden decorations. Make sure shrubbery, weeds, etc. are trimmed and maintained so the foliage:

- **Cannot be used** by intruders to hide in or gain access to the home.
- **Does not block** the view outside from those inside the home.

Secure external doors and windows with appropriate locking devices, which can include electronic and coded locking mechanisms. It is best to secure an extra set of keys or entry codes for use during an emergency. Consider changing the entire locking system in the event the entry codes become compromised or the keys are lost.

Invest in and maintain external lighting that illuminates external doors, parking areas and walkways around the house. Consider installing cameras with views of doors and windows. Strategically position these lights and cameras to eliminate any blind spots where individuals could evade detection.

If you have a vehicle and cannot secure it in a garage or a locked area, try leaving it in public view. Park in a well-lit area, in the view of a CCTV camera or in a staffed parking lot. Always close any windows, remove valuables from view and lock your car, even if you are just stepping away for a few minutes. Understand how to utilize the type of theft deterrent alarm system within your vehicle. There are systems that include audible and visual notifications in addition to vehicle locator services to assist in expediting police response.

PLAN AHEAD

Consider developing a family emergency action plan and practicing what to do in the case of an emergency.
For help developing a plan, visit:

fema.gov/blog/have-emergency-plan-your-family.

FIREARM ATTACKS

An active shooter is defined as one or more individuals actively engaged in killing or attempting to kill people in a populated area.[3] Active shooter incidents are often unpredictable and evolve quickly. Amid the chaos, anyone can play an integral role in mitigating the impacts of an active shooter incident.

Because active shooter situations are often over within 10 to 15 minutes - before law enforcement arrives on the scene - individuals must be prepared both mentally and physically to respond to an active shooter incident.

In the event of an attack shooter incident, consider implementing a practiced response strategy—such as the Run, Hide, Fight paradigm—in accordance with your organizations security policies. Additional information and resources can be found at CISA's homepage for Active Shooter Preparedness.

FIRE AS A WEAPON

Arson is defined as any willful or malicious burning or attempt to burn—with or without intent to defraud—a dwelling house, public building, motor vehicle, aircraft or other personal property.[4] An arsonist's motivation may include revenge, vandalism, fraud or crime concealment, among others. Accelerants and flames or a type of improvised incendiary device (IID) may be used to start the fire.

The threat of fire as a weapon may be difficult to detect until the attack is underway. You need to understand the steps to take if you smell smoke or see something on fire.

In case of a fire attack, call 9-1-1 and follow directions from emergency personnel. Leave the area of the fire activity immediately and alert others, if possible. Avoid areas where you can smell smoke or see fire. Evacuate indoor premises; close all doors behind you to contain the fire. If you are unable to evacuate, move as far away as possible from the hazard and use fire extinguishers as needed. Maintain situational awareness and watch for suspicious activity or additional threats.

Visit CISA's Fire as a Weapon Action Guide for more tips on mitigating instances when fire is used as a weapon.

IMPROVISED EXPLOSIVE DEVICES (IED)

An IED is a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or

3 Federal Bureau of Investigation, n.d. Active Shooter Safety Resources. Accessed December 1, 2023, fbi.gov/how-we-can-help-you/active-shooter-safety-resources.

4 Cybersecurity and Infrastructure Security Agency. 2021. Fire as a Weapon Action Guide. Accessed August 8, 2023. cisa.gov/resources-tools/resources/fire-weapon-action-guide.

5 U.S. Department of Homeland Security. Federal Bureau of Investigation. n.d. *Security and Resiliency Guide: Counter-Improvised Explosive Device (C-IED) Concepts, Common Goals, and Available Assistance.* Accessed August 8, 2023. Pg 4. cisa.gov/resources-tools/resources/security-and-resiliency-guide-srg-and-annexes.

incendiary chemicals and designed to destroy, incapacitate, harass or distract.[5] Depending on the goals and materials available to the bomb-maker, IEDs range from small, crude devices, such as overpressure devices or pipe bombs most often filled with explosive powders, to large vehicle-borne devices containing bulk quantities of explosives.

Threats can take varying forms. If you are ever concerned about a situation or suspicious item, call your local law enforcement immediately. Examples indicating a bomb include unexplainable wires or electronics, other visible bomb-like components, and unusual sounds, vapors, mists or odors. Improvised explosive device incidents involving a suspected device require a bomb squad response and capability to diagnose and "render-safe" viable devices.

For more information on recognizing suspicious items, refer to the Unattended vs. Suspicious Item Postcard and Poster and watch the video "What to Do: Suspicious or Unattended Item."

PROTESTS AND DEMONSTRATIONS

Regardless of mission or intent, stay calm if a public protest or demonstration takes place near your home, place of business or even on your property. Protests may seem intimidating but are unlikely to lead to a physical threat. Even if the situation becomes volatile, remain calm. Stay inside, close and lock your doors and windows, and draw your curtains/blinds. If you feel unsafe or the situation escalates, call your local law enforcement.

If necessary, note descriptions of individuals and vehicles present. Provide any video surveillance footage, cell phone videos or photographs to the police, as it may help in the event of an investigation.

CISA's Protecting Infrastructure During Public Demonstrations Fact Sheet offers security recommendations for businesses that may be the target of unlawful acts during public demonstrations.

SITUATIONAL AWARENESS

Situational awareness is being aware of what is happening around you, taking everything into account and adjusting your behavior to reduce the risk of injury to you, your family or your coworkers.

VISITORS

Always identify visitors before letting them inside your home. Consider installing a peephole or door camera to help you identify who is on the other side of the door. Ask unknown visitors to identify themselves before opening your door. Once inside your residence, keep them in close proximity, preferably in front of you or in position where they can be visually monitored. Consider carrying a mobile phone at all times.

SENSITIVE MATERIAL

Always properly dispose of or destroy confidential material that may have sensitive or personally identifiable information (PII). PII includes any information that is personal in nature that may be used to identify you.

PEDESTRIAN SAFETY

Prioritize your personal safety when traveling, walking or jogging in public spaces. Taking suitable precautions can help you reduce vulnerabilities and the risk of experiencing violence or aggression. Consider simple measures such as planning a safe route ahead of time, varying your route when going to regular places, and avoiding potential danger points, such as quiet or poorly lit alleys, desolate parking garages and remote parking lots. Whenever you are in public, use discretion and take precautions to hide any work credentials or personal information. Take care when wearing badges or entering passwords while in public spaces. For more facts and tips, visit the National Highway Traffic Safety Administration's website on Pedestrian Safety.

MAINTAIN SITUATIONAL AWARENESS

If you become worried or start to feel unsafe while you are in a public area/setting, move closer to a group of people. If that is not possible, adjust your movements to maximize your situational awareness and **take the following precautions:**

- **Keep your mobile phone** in a position to make an emergency call.
- **Be alert** and remain aware of your exact location and surroundings.
- **Avoid showcasing** any jewelry or valuables.
- **Consider the area lighting, location and proximity** to other local businesses.
- **Face oncoming traffic while walking** to avoid vehicles approaching from behind.
- **Keep your hands free** and remain aware of your surroundings.
- **Avoid talking on the phone**, wearing headphones or sending long texts.
- **Stay alert** when walking and avoid lingering.
- **When using a banking ATM**, refrain from displaying currency in public view.

RIDESHARE SERVICES

When using a rideshare application, consider notifying a friend or colleague of the details of your location and destination. Check the driver's details before accepting the ride and entering the vehicle.

PERSONAL PROTECTION DEVICES

Consider carrying pepper spray, an audible alarm, or additional personal protection device to disorient an aggressor, notify bystanders and to provide yourself an opportunity to escape. Where able, and in accordance with federal and local laws and regulations, carry and utilize personal protection devices.

RECOGNIZE AND REPORT SUSPICIOUS ACTIVITY

Recognize and report suspicious activity - such as people loitering without a specific reason around your home, workplace or vehicle, or people trying to take pictures of you in a covert manner. If you notice someone abandon an object or package near your home, workplace or vehicle, report it to the police immediately. Learn more about reporting suspicious activity by visiting the "If You See Something, Say Something®" campaign.

Paying careful attention to and promptly reporting the following warning signs could help mitigate a potential incident:

- **Verbal or written threat** against you, your home, possessions or place of employment.
- **Damaged or tampered** systems and equipment.
- **Suspicious or unattended items**—including bags, boxes, concealed containers—that may contain hazardous substances.
- **Suspicious questioning** of building floor plans, locations of entrances/exits, elevators, fire extinguishers, water supply, as well as heating, ventilation and air conditioning (HVAC) systems.
- **Unusual quantities or locations of flammable or combustible materials,** including accelerants, paints, degreasers, alcohol-based cleaners, aerosols and propane gas tanks.
- **Social media messaging** that promotes any imagery or ideas for carrying out attacks.

Check out the Suspicious Activity Reporting Indicators and Examples for more information.

CONFRONTATIONS

Finding yourself in a confrontational situation can be stressful. Attention should be focused on observable behaviors that could be indicative of potential violence. In these situations, it is important to remain calm and assess the situation to determine if it is safe to engage. Consider the limits of your own abilities and seek assistance from security staff or law enforcement as soon as it is safe to do so. If you are trained and proficient, consider safely de-escalating heated situations through purposeful actions that include effective listening and communication. Remember "de-escalation" is not something you do; it is the goal.

Visit CISA's De-escalation Series to learn tips on staying vigilant and navigating potentially hostile situations.

MOTOR VEHICLES AND TRAVEL

Before leaving your home or place of work, look around and take note of any suspicious vehicles that might be lurking or loitering. Inspect the area around the vehicle for anything that should not be on or near your vehicle. If a situation does occur, this information may be helpful to the police.

If possible, avoid repeated patterns in your travel arrangements so potential malicious actors cannot predict your whereabouts. Change your routes and vary times of departure as much as possible. Make sure all vehicle doors and trunks remain locked during your journey. Open windows only enough for ventilation. Drive safely and maintain a safe distance from the vehicle in front of you. Also—always ensure your vehicle has enough fuel (or, if electric, is sufficiently charged) for your journey.

If you think you are being followed, try to remain calm and keep your vehicle moving. Close all windows and make sure your doors are locked. Contact law enforcement immediately. If you can, make your way towards the nearest police station—do not drive home. Try to note the license plate number, make and model of any suspicious vehicle.

If you are involved in a vehicle collision or experience a mechanical malfunction, consider your surroundings and contact emergency personnel and vehicle tow service immediately. Follow instructions from law enforcement.

ANONYMOUS PHONE CALLS AND THREATS[6]

Anonymous phone calls and threats are usually intended to cause fear, alarm and distress. Remember to always do the following:

- **Remain calm** and do NOT hang up the phone.
- **Keep the caller on the line** as long as possible. Be polite and show interest to keep them talking. They may reveal important information that can help in the event of a police investigation.
- If possible, **signal or pass a note** to other person(s) around you to listen and help notify authorities.
- **Write down** as much information as possible—caller ID number, exact wording of threat, type of voice or behavior, etc.—that will aid investigators.
- **Record the call,** if possible.

It is against federal law to make threatening or abusive phone calls. If you receive any calls like this, contact your local law enforcement. Additionally, you can report the threat to the FBI. Check out the FBI Threat and Intimidation Response Guide for tips.

As most bomb threats are made via telephone, see the DHS Bomb Threat Checklist and the CISA Bomb Threat Guide, which provide instructions on how to respond to a bomb threat, as well as a comprehensive list of information that will assist law enforcement in a bomb threat investigation.

ONLINE SECURITY

SECURE DOWNLOADS

Download a secure virtual private network (VPN), anti-virus security services and software for all devices including laptops, computers, phones and tablets. Keep software up to date. Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

Only install applications from reputable "app stores" to avoid potentially harmful downloads. Do not download applications from unknown or unverifiable sources. Be mindful of what permissions applications have to access other information on your phone.

Create and maintain a strong password that is unique for each of your devices or accounts. If available, use multifactor authentication for a more secure authorization process.[7]

Whether using a home or business network, the risks remain the same if the wireless network is unsecure. Bad actors can use unsecure networks to steal PII, compromise financial data and listen to or watch users. Consider restricting access by encrypting the data on your network, installing a firewall or using a VPN connection. To learn more about securing networks, visit CISA's webpages on Securing Wireless Networks and Home Network Security.

USE OF ELECTRONIC DEVICES

Mobile devices and networks can hold a variety of personal details, such as online banking information, emails, text messages, contacts, social media and pictures. To keep your device secure, use all security features and make sure you are consistently updating device software. Create strong passcodes for your phone and SIM cards and disable unnecessary location services.[8]

Always change your default PIN for voicemail access. Avoid using public Wi-Fi and hotspots, as they may not be secure. Consider disabling location services on your phone and review privacy settings to prevent others from tracking your movements and identifying your home address or place of work through third party applications. Sometimes videos, photos and other media are geotagged with a location that can reveal private information to unknown third parties. This is a type of metadata, which is data that provides information about other data, such as location, date or time on an image. Remove metadata from pictures, especially ones taken from mobile phones before you post them online.

6 Federal Bureau of Investigation. n.d. Threat Intimidation Guide. Accessed August 8, 2023. fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view.

7 Cybersecurity and Infrastructure Security Agency. 2022. 4 Things You Can Do To Keep Yourself Cyber Safe. Accessed September 20, 2023. cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe.

8 Federal Communications Commission. 2019. Protect Your Smart Device. Accessed September 20, 2023. fcc.gov/consumers/guides/protect-your-mobile-device.

SOCIAL MEDIA

The internet can be a valuable source of information, education and entertainment. However, it is necessary to remain vigilant and take precautions to limit the amount of personal information you publish online—especially on social media.

Popular social media sites allow individuals to create a personal profile and interact with others online. On business networking sites people may add more detail to their profiles and include work history and other background information.

While these tools help you communicate with others and advertise your professional background, publishing personal information online presents potential risks.

Be careful when posting personal information. Malicious actors can use location data from photos, birthdays, full names, home addresses and email details when hacking or committing identity theft. Additionally, information about employment, family members, hobbies or vehicle details are valuable to criminals and hostile parties. Consider not posting about being on vacation at the same time that you are away from home to lessen the potential for a home break-in.

Some social networking sites own any data that you post and will sell your details to third parties. Read through the privacy policies of any social networking site you choose to participate in.

Regularly review your privacy and location tagging settings on these sites, otherwise you risk some, or all, of your personal profile being seen by a large audience, unknown to you.[9, 10] Additionally, your family and friends can unintentionally share information about you if they do not take appropriate measures to protect their own profile information.

DOXING

Doxing refers to the internet-based practice of gathering PII from open source or compromised material and publishing it online for malicious purposes.[11] Terrorists and hacktivists can use this information as blackmail or to incite fear in potential targets.

As you post online, it is important to be aware of what and how you are posting. If you post too much information without applying the appropriate privacy settings, you may be putting your personal safety at risk. People can use this information to build a picture of your relationships, opinions, places of interest and other subjects that they can exploit in the future.

Location-based information can be posted on social networks, especially from GPS-enabled cell phones and mobile devices. This information is not secure and can be seen by anyone, including people who may wish to do you harm. Keep track of what you post and post responsibly to ensure no one is put at risk by the information you make public.

If you believe you are being doxed:

- **Report the incident** to local law enforcement, the social media platform or the website administrators.
- **Document** what occurred and take screen shots to share with investigators.
- **Determine** what information was exploited, the seriousness of the threat and the point of compromise.
- **Work with website administrators** to remove information from websites or applications.
- **Configure privacy settings** to the most private options.
- **Watch for signs** of identity theft, monitor financial accounts, set up fraud alerts and change log-in and password information for all online accounts.

If concerned about physical safety, contact local law enforcement for next steps.

EMAIL SECURITY

Beware of unsolicited email attachments, even from people you know. Many viruses can mimic a return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it is legitimate before opening any attachments.

9 Government of the United Kingdom. National Cyber Security Centre. 2019. Social Media: how to use it safely. Accessed September 20, 2023. ncsc.gov.uk/guidance/social-media-how-to-use-it-safely.

10 Cybersecurity and Infrastructure Security Agency, National Cyber Alliance. 2019. Social Media Cybersecurity. Accessed September 20, 2023. cisa.gov/sites/default/files/publications/NCSAM_SocialMediaCybersecurity_2020.pdf.

11 Cybersecurity and Infrastructure Security Agency. 2021. CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure. Accessed August 8, 2023. cisa.gov/resources-tools/resources/cisa-insights-mitigating-impacts-doxing-critical-infrastructure.

RESOURCES

PHYSICAL SECURITY

- CISA Security and Resiliency Guide
- CISA Active Shooter Preparedness
- FBI Threat Intimidation Guide
- CISA What to Do - Bomb Threat
- CISA De-escalation Series

SITUATIONAL AWARENESS

- Stalking Prevention, Awareness, & Resource Center (SPARC)

ONLINE SECURITY

- CISA Securing Wireless Networks
- CISA Understanding Patches and Software Updates
- CISA Privacy and Mobile Device Apps
- CISA Risks of Using Portable Devices
- CISA Capacity Enhancement Guide Mobile Device Cybersecurity Checklist for Consumers
- CISA Insights on Doxing on Critical Infrastructure
- CISA Good Security Habits
- CISA Home Network Security
- CISA Protecting Portable Devices: Data Security
- CISA Protecting Portable Devices: Physical Security