VIOLENT EXTREMIST
MOBILIZATION INDICATORS
AND THE CRITICAL INFRASTRUCTURE SECTOR

The National Counterterrorism Center (NCTC), the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) are committed to safeguarding the rights guaranteed by the United States Constitution and applicable law. It is therefore important to emphasize that many of the mobilization indicators included in this booklet may also relate to constitutionally protected activities. Each indicator listed may be, by itself, lawful conduct or behavior and may constitute the exercise of rights guaranteed by the US Constitution. It is most important to look critically and contextually at the specific actions of the individual and their intent. Law enforcement action should never be taken solely based on constitutionally protected activities; on the apparent or actual race, age, ethnicity, national origin, religion, gender, sexual orientation, or gender identity of the subject; or on any combination of these factors. Individuals are encouraged to contact law enforcement if—based on the totality of these behavioral indicators and the situational context—they suspect an individual is mobilizing to violence or engaging in violent extremist activities. No single indicator should be the sole basis for action.

NCTC, FBI, and DHS's *US Violent Extremist Mobilization Indicators 2021 Edition* is a booklet of 42 indicators—or observable behaviors—that suggest an ideologically motivated US-based violent extremist may be mobilizing to violence.[a] This supplement is intended to show how these indicators can be used to help detect threats against 16 critical infrastructure sectors.[b] Critical infrastructure is a frequent and enduring target of US violent extremists, in part because of messaging from foreign terrorist organizations and other violent extremists that highlight critical infrastructure as an accessible and high-impact target.

This supplement is organized into two sections:

- Section 1 lists examples of behavioral indicators likely to be observed by individuals working in the 16 critical infrastructure sectors. Industry professionals are well-positioned to observe these indicators—from violent extremists seeking virtual or physical access to critical infrastructure assets or facilities or from potential insider threats by violent extremists. These indicators are organized by six behavior types and are broadly applicable to each critical infrastructure sector, partly because lone offenders[c] can develop plans to target one sector before opportunistically shifting to another based on their unique circumstances.

[a]Ideologically motivated US-based violent extremists consist of homegrown violent extremists (HVEs) and domestic violent extremists (DVEs). An HVE is defined by the FBI and DHS as a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization but is acting independently of direction by a foreign terrorist organization. HVEs are distinct from traditional domestic terrorists who engage in unlawful acts of violence to intimidate civilian populations or attempt to influence domestic policy without direction or influence from foreign actors. A DVE is defined by the FBI and DHS as an individual based in and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals, wholly or in part, through unlawful acts of force or violence. The mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may not constitute extremism and may be constitutionally protected.

[b]Presidential Policy Directive 21 (PPD 21) established 16 sectors of critical infrastructure: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, health care and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems.

[c]A lone offender is defined by the FBI and DHS as an individual acting alone or without the witting support of others to further social or political goals, wholly or in part, through activities that involve unlawful acts of force or violence. Lone offenders may act within the context of recognized domestic extremist ideologies, their own interpretation of those ideologies, or personal beliefs. The mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics does not constitute extremism, and may be constitutionally protected.

- Section 2 provides a sector-specific reference aid of potential observers and examples of behavior, broken out by each of the critical infrastructure sectors. This section is meant to be illustrative, not exhaustive, because of the size and scale of each critical infrastructure sector, many of which involve multiple subsectors or critical dependencies with other sectors.

It is important to consider the totality of an individual's circumstances, including their typical access to critical infrastructure facilities, when observing potential indicators. We incorporated the word "unusual" in many of these examples to remind observers that we are looking for concerning behavior that is different from an individual's normal or expected activity. Many of these indicators are constitutionally protected activities, and the presence of a single indicator does not necessarily mean that an individual is mobilizing to violence. However, when observed in combination with other suspicious behaviors, these indicators may raise suspicion in a reasonable person and constitute a basis for reporting to law enforcement.

Additional Resources

Please consult DHS's Cybersecurity and Infrastructure Security Agency (CISA) website,[d] as well as the websites of each designated sector risk management agency (SRMA), for additional sector-specific information and resources. We encourage our public- and private-sector critical infrastructure partners to report any observations of ideologically motivated calls for, or acts of, violence specific to their sector to NCTC, FBI, and DHS to enhance the accuracy and utility of future editions of this booklet.

We also encourage users of this supplement to explore First Responder's Toolbox products from the Joint Counterterrorism Assessment Team (JCAT).[e] Many of these JCAT products contain additional examples of behavioral indicators and US Government resources for specific sectors or subsectors. Most are available through the JCAT website,[f] contacting your regional NCTC Representative, or accessing FBI's Law Enforcement Enterprise Portal or DHS's Homeland Security Information Network.

Presidential Policy Directive 21 (PPD 21) established 16 categories of critical infrastructure.

Chemical

Commercial Facilities

Communications

Critical Manufacturing

Dams

Defense Industrial Base

Emergency Services

Energy

Financial Services

Food and Agriculture

Government Facilities

Health Care and Public Health

Information Technology

Nuclear Reactors, Materials, and Waste

Transportation Systems

Water and Wastewater Systems

[d]https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[e]JCAT is a longstanding collaborative effort of NCTC, DHS, and FBI to improve information sharing among federal, state, local, tribal, and territorial governments as well as with private-sector partners to enhance counterterrorism public safety.

[f]https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox

🔴 Mobilization ⬛ Preparation 🟡 Motivation

2 Engaging in a threatening interaction or violently refusing to comply with law enforcement based on an observed violent extremist ideology

3 Disseminating one's own martyrdom or last will video or statement (for example, a pre-attack manifesto)

5 Identifying—in person or online—specific details of an intended violent activity, including targets, timeframes, and participant roles

8 Communicating in person or online an intent to engage in violence or a direct threat with justification for action, particularly if presented as necessary or inevitable

28 Professing an intent to harm law enforcement if law enforcement takes action or stating an intent to harm others if confronted

30 Threatening specific violence against a particular physical target, especially in response to current news reporting on political and legislative issues or other flashpoint events that speak to one's ideological concerns

31 Threatening violence toward specific individuals, including civilian, government, law enforcement, or military personnel

34 Expressing acceptance of violence as a necessary means to achieve ideological goals and saying that nonviolent means are ineffective or unavailable

Potential Examples:

- Posting violent extremist media naming or providing instructions on how to access specific critical infrastructure targets, including those providing coordinates, infra-maps, or street view imagery.

- Posting or sharing misinformation or disinformation[h] about a particular critical infrastructure sector while communicating a threat against a company- or site-specific location.
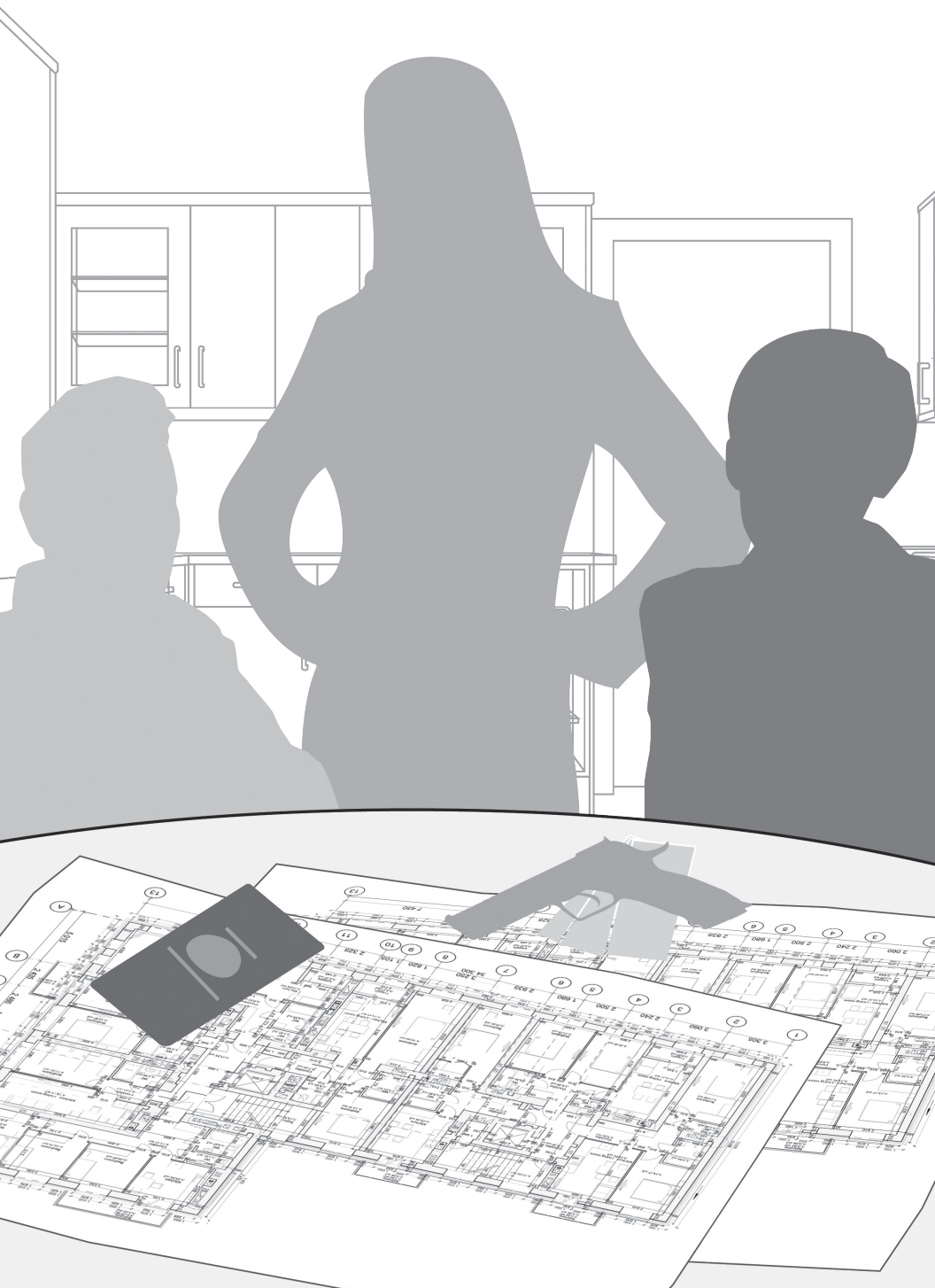
[g]The six behavioral indicator types—as well as the indicators and corresponding numbers—listed throughout this supplement all come from *US Violent Extremist Mobilization Indicators 2021 Edition*. For a full copy, please access the QR code on the back of this booklet or go to: https://www.dni.gov/files/NCTC/documents/news_documents/Mobilization_Indicators_Booklet_2021.pdf.

[h]Misinformation is false, inaccurate, or misleading information that is spread regardless of the intent to deceive. An individual's intent can change misinformation to disinformation. Disinformation is false or misleading information that is deliberately created or spread with the intent to deceive or mislead

TACTICS

Acquiring or developing skills, knowledge, or materials to engage in violent extremist activities

● Mobilization ■ Preparation ⬡ Motivation

4 Conducting a dry run of an attack or assault or attempting to gain proximity or access to targets

9 Unusual building or testing of explosives, especially if tailored to a specific target

15 Surveilling potential attack targets

16 Increased use of physical concealment tactics in support of planning a specific act of violence

17 Increased use of online concealment tactics in support of planning a specific act of violence

20 Acquisition of weapons for suspected criminal purposes

25 Conducting research for target or tactic selection for violent acts

26 Pursuing or exploiting jobs or personnel who provide sensitive access to enable violent acts

27 Attempting to seek technical expertise to enable planned violence

Potential Examples:

- Unusual online research into specific critical infrastructure sector vulnerabilities, loopholes, or bypasses. This could include downloading leaked confidential, protected, or sensitive information pertaining to a critical infrastructure sector's assets, physical location, or security, such as the delivery schedules of critical materials.

- Unusual acquisition of long-range firearms or attempts to manufacture or acquire privately made firearms (e.g., 3D printed guns), especially when coupled with indicators of the intent to pursue specific targets or evade security screening measures.

- Unusual pursuit of employment in an infrastructure field, particularly focused on specific access that does not align with prior educational and professional experience.

- Unusual attempts to physically surveil potential targets to include taking photos or video of security features or using UAS for aerial reconnaissance. This could also include unidentified persons making multiple visits to a site, especially when combined with signs of tampering to locks or fencing intrusions; or the theft, unlawful acquisition, or misappropriation of credentials, key fobs, or uniforms.

Interacting with others, including family or other violent extremists

🔴 Mobilization　🟧 Preparation　🟡 Motivation

7 Unusual goodbyes or post-death instructions

14 Breaking away from a larger group or creating a more exclusive or operationally secure group to discuss or plan specific violent activity

24 Creating, joining, or implying membership or association—in person or online—with violent extremists for the purpose of furthering violent activity

35 Attempting to radicalize others, especially family members and peers to violence

38 Engaging in outbursts or fights with or condemning behavior of family, peers, community, or authority figures while advocating violent extremist ideology

42 Isolating oneself from family and peers, particularly if citing violent extremist doctrine or ideology

Potential Examples:

- Unusual attempts to seek detailed information from family, friends, fellow employees, or strangers about facility security or other sensitive site information. This could include unsolicited phone calls or emails to employees by individuals requesting information while posing as researchers, government officials, or potential visitors without providing appropriate credentials.

- Online or in-person efforts to recruit specific critical infrastructure sector employees to engage in a violent action against a critical infrastructure target.

TRAVEL
Transiting within the United States or abroad to prepare for or conduct violence

🔴 Mobilization   🟧 Preparation   🟡 Motivation

1 Traveling, within the United States or abroad, to carry out or participate in violent extremist activity

11 Planning or preparing to travel within the United States to participate in violent extremist activity

22 Planning or pursuing suspicious travel activity in a manner that raises suspicion of potential violence

Potential Examples:

- Discussing, posting about, or organizing meet-up groups or events associated with violent extremists' desire to target a specific critical infrastructure sector or site.

- Unscheduled one-way travel to physically surveil a critical infrastructure site. This could include repeated drive-by surveillance from unusual vehicles, such as cars with new or out-of-town license plates.

FINANCIAL
Moving or acquiring money or resources to prepare for or conduct violence

6 Disposing of meaningful personal assets or belongings in an unusual manner, particularly with a sense of urgency or without regard for personal financial gain

23 Sending or receiving unexplained financial resources or equipment to/ from violent extremists

Potential Examples:

- Significant loans or accrual of debt in pursuit of courses or training outside of current area of employment to develop unexplained sector-specific expertise.

- Sudden large cash withdrawals or articulating the need to amass large sums of cash, especially in conjunction with other indications of interest in violent extremist activities.

- Sending multiple cash transfers or withdrawals, often in amounts below the cash reporting threshold, to avoid alerting banking authorities to potentially suspicious activities.

- Funds deposited to or withdrawn from a cryptocurrency address with direct or indirect links to known violent extremists, which could include connections to darknet marketplaces, mixing or tumbling services, questionable gambling websites, ransomware, or theft reports.
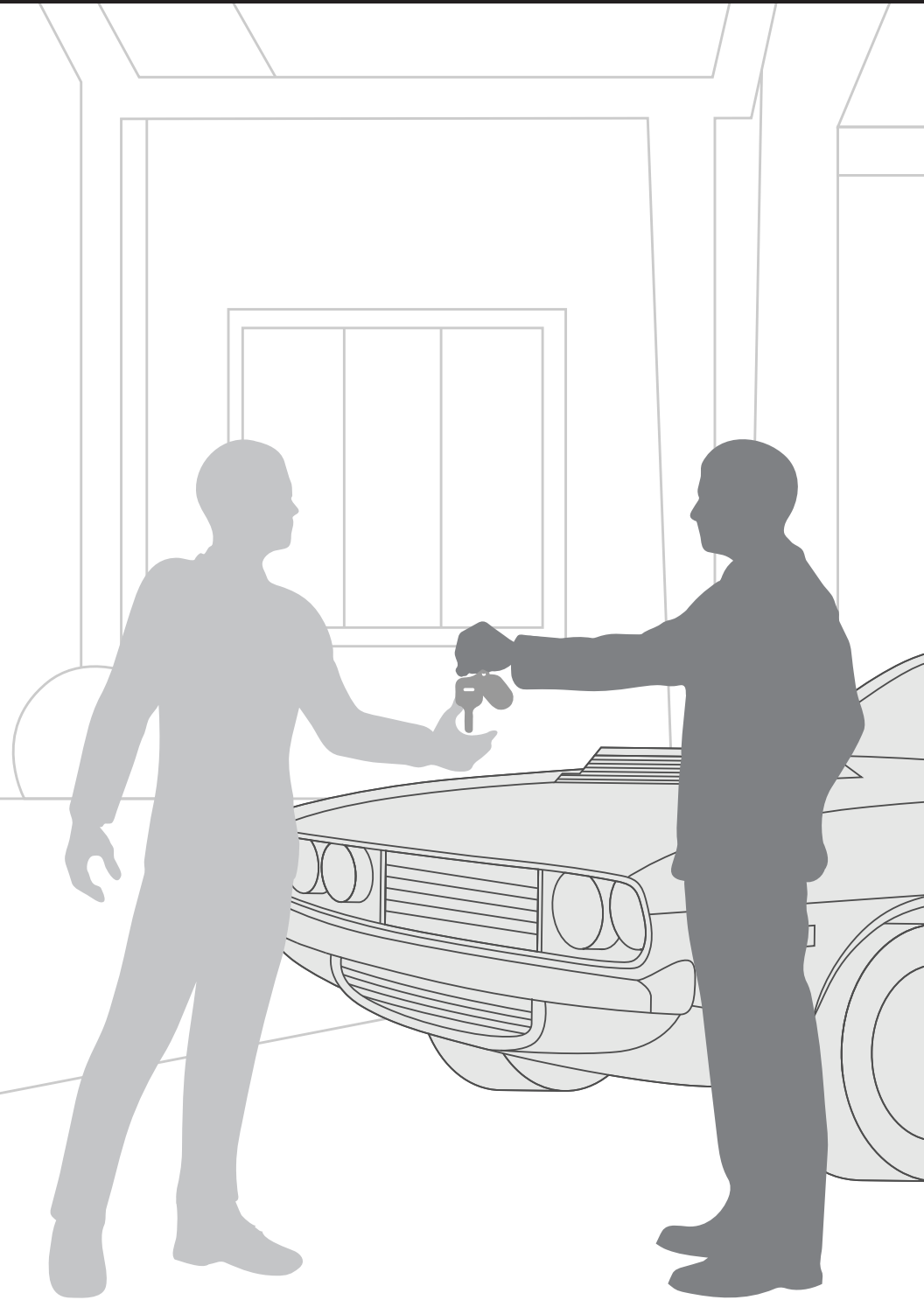
IDEOLOGICAL

Developing or communicating the mentality or justification that could lead to the commission of a violent act

● Mobilization   ■ Preparation   ⬡ Motivation

12 Seeking or claiming religious, political, or ideological justification or validation for a planned violent act

32 Producing, promoting, or extensively consuming violent extremist content online or in person, including violent extremist videos, narratives, media, and messaging for suspected criminal purposes

33 Posing with weapons and imagery associated with violent extremism in photos or videos, especially if paired with threats, or expressing interest in carrying out violence against an ideological target for suspected criminal purposes

36 Praising, or researching to emulate, past successful or attempted violent extremist attacks or attackers

37 Demonstrating increasing or extreme adherence to conspiracy theories as a justification of violence against ideological targets

40 Rejecting nonviolent voices in favor of violent extremist ideologues

41 Changing vocabulary, style of speech, or behavior to reflect a hardened point of view or new sense of purpose associated with violent extremist causes, particularly after a catalyzing event

Potential Examples:

- Posting violent extremist iconography glamorizing or venerating past attackers who have specifically targeted critical infrastructure.

- Producing or repeatedly sharing stories highly critical of a specific sector or publicly naming specific individuals within that industry as responsible for a perceived wrongdoing as a justification for violence.

- Downloading or disseminating violent extremist messaging that emphasizes infrastructure attacks or vulnerabilities.

SECTOR-SPECIFIC REFERENCE AID

This section highlights sector-specific facility personnel who are most likely to observe suspicious in-person activities, such as attempts to surveil or breach a critical infrastructure site. In addition, industry intelligence and security personnel in all sectors would be positioned to observe many of the examples listed below, as well as any potentially concerning online activity, given their role in monitoring social media and other digital spaces for sector threats.

CHEMICAL

SRMA DHS

Potential Observers Manufacturing plant personnel; disposal, storage, or warehouse staff; distributors transporting chemicals to/from manufacturing plants or warehouses.

Potential Examples
- Repeated attempts to obtain, demonstrate suspicious interest in, or try to steal commercial explosives or toxic industrial chemicals (TICs).
- Employee or outsider trying to gain unauthorized access to a restricted area—such as a chemical storage room—or someone doing so without going through proper procedures.
- Individuals seeking to purchase chemical materials who cannot answer basic questions on material use or provide an explanation for current use, safety, or handling.
- Requests for samples, particularly large samples, of hazardous materials by new or unknown parties.
- Unexplained, unapproved, or new delivery location for sensitive materials to an existing customer, or a reluctance to provide information on the location of end use.
- Efforts to hide and prevent the tracking of purchases of TICs or explosive precursor chemicals, such as purchases that are spread across multiple stores in a chain.
- Unusual interest in the purchase or possession of potential dispersal materials, including tubing, pumps, sprayers, drop mechanisms, or modified UAS.

COMMERCIAL SERVICES

SRMA DHS

Potential Observers Media production facility staff; commercial and tribal casino operators and staff; hotel and motel staff; amusement park and other outdoor venue and event staff; arena, convention center, and stadium staff; mall, shopping center, and retail staff.

Potential Examples
- Unusual interest in building or facility security or access points, including main, alternate, and emergency entrances and exits; weapons screening points; and access controls, such as alarms, barriers, doors, gates, or locks.
- Seemingly purposeful attempts to mask one's identity in the vicinity of cameras or to use entrances and exits that avoid the lobby, cameras, and staff.
- Significant changes in physical appearance or attempts to disguise appearance between repeated visits to a particular site or venue.

COMMUNICATIONS

SRMA DHS

Potential Observers Broadcast, cable, satellite, wireless, or wireline service providers or technicians.

Potential Examples
- Threatening violence, either in person or online, toward specific communications targets (e.g., 5G towers) based on increasing or extreme adherence to conspiracy theories that justifies such violent acts.
- Visible signs of trespassing, tampering, or vandalism in conjunction with the presence of suspicious or unusual items near structures. Such items could include bottles of liquid, empty or used packaging or materials that could disguise incendiary devices or explosives, or hidden sharp objects (e.g., razor blades or needles) that are located where they could injure employees.

CRITICAL MANUFACTURING

SRMA DHS

Potential Observers Electrical equipment, machinery, or primary metals manufacturers, processors, and transporters.

Potential Examples
- Repeated reports of manufacturing or processing facility personnel being asked questions about the facility while off-site or after their normal workday.
- Damage to facility's perimeter fence, gate, perimeter lighting, close-circuit televisions, or other security devices.
- Unauthorized individuals seen inside the facility or individuals not following basic facility protocols, such as wearing an ID card or hard hat.
- Abnormal interest in truck and delivery schedules, especially for key manufacturing components.

DAMS

SRMA DHS

Potential Observers Private- and public-sector dam, levee, and navigation lock owners and operators; dam safety officers.

Potential Examples
- An unauthorized individual getting close to or entering a dam exclusion zone.
- Airborne vehicles—such as small planes, helicopters, or remotely controlled aircraft—that appear to be using a crossing pattern or other suspicious means to survey the property or facility.
- Unusual or repeated gathering of information about a dam, its operations, or protective measures through unusual means, such as repeated efforts to take notes, draw maps, or draw structures of the facility.

DEFENSE INDUSTRIAL BASE

SRMA DOD

Potential Observers DOD employees and contractors.

Potential Examples
- Creating, joining, or implying membership or association—either in person or online—with a foreign terrorist organization or violent extremist network with the intent to mobilize to or incite violence.
- Unusual attempts by outsiders to elicit information about facility security, or attempts by base or company personnel to repeatedly seek access to sensitive information that is beyond the scope of their work.

EMERGENCY SERVICES

SRMA DHS

Potential Observers Law enforcement, fire and rescue, emergency medical, emergency management, and public works officers and support staff.

Potential Examples
- Making prank or hoax emergency calls, pulling fire alarms, or calling in repeated bomb threats to provoke and gauge responses by fire, rescue, emergency medical service, or law enforcement officers.
- Professing intent to harm or explicitly threatening violence—either in person or online—against law enforcement if confronted or encountered.

ENERGY

SRMA DOE

Potential Observers Electric utility service providers, operators, and technicians; oil and natural gas operators and transporters.

Potential Examples
- Unusual online searches, sharing, or downloading material identifying potential points of failure in pipeline networks, electricity distribution and transmission networks, or industrial control systems.
- Unusual, repeated, or prolonged visits to substations, especially when combined with efforts to photograph or record the site.
- Unusual vehicle traffic activity along known pipeline/feeder routes, particularly in remote areas.
- Recovered UAS, overflying or deflated mylar balloons, or other metal or metallic objects—particularly modified with ropes or copper wire—near electric substations.

FINANCIAL SERVICES

SRMA Treasury

Potential Observers Operators or moderators of online marketplaces, e-commerce websites, or financial services; employees at financial institutions or exchanges; remittance service providers.

Potential Examples
- Use of obfuscation techniques, such as sending or receiving directly from third-party mixing or gambling services, layering transactions (e.g., moving funds to a series of wallets to obscure the origin), and transfers less than reporting thresholds (similar to structured cash transactions).
- Large amounts of cash from unexplained sources or deposits or other financial activity inconsistent with known (or claimed) sources of income.
- The excessive use of informal banking, value transfer, or remittance systems to transfer funds abroad to people in countries with inadequate or non-existent formal financial systems.

FOOD AND AGRICULTURE

SRMAs USDA; HHS

Potential Observers Farmers and agricultural workers, including seasonal employees; agricultural equipment sales employees, distributors, and technicians; veterinarians; employees at animal feed production, distribution, and sales facilities; agrochemical company and agricultural cooperatives personnel; food manufacturers, food processor facility staff, storage facility staff, and warehouse staff; food inspectors; restaurateurs and food service and staff; federal and state foresters and logging industry personnel.

Potential Examples
- Intentionally killing or poisoning farm animals—excluding protocols for disease control or public health—or intentionally letting farm animals escape.
- Unusual interest in acquisition of vaccines or medications for a crop or livestock disease.
- Unusual interest in acquiring or possession of site or facility specific maps, or maps of agricultural asset concentrations.
- Unusual interest in travel to regions where an infectious disease event or pest event is occurring or has recently taken place.
- Gathering information on operational security protocols, including physical security and biosecurity, at food and agricultural harvesting, production, and distribution sites (e.g., animal feedlots, food processors, or cold storage distribution centers).
- Individuals loitering or discreetly using cameras or video recorders near food processing or production facilities, restaurants, or institutional food service establishments in a suspicious manner.
- Employees unwilling to maintain or participate in record keeping practices, seeking to bring personal items into production areas, or removing company provided protective gear from facility premises without prior authorization.

GOVERNMENT FACILITIES

SRMAs	DHS; GSA
Potential Observers	Federal, state, local, tribal, and territorial government employees, including teachers and school administrative and support staff.
Potential Examples	• Increasingly using lexicon that reflects antigovernment violent extremist grievances or narratives, especially justifying violence against government targets. • Repeated attempts to visit or intrude upon restricted or access-controlled facilities. • Threatening violence against a government target, especially in response to a flashpoint event regarding a particular political or legislative issue.

HEALTHCARE AND PUBLIC HEALTH

SRMA	HHS
Potential Observers	Hospital and other direct patient care medical and support staff; health information technology company staff; laboratory, blood and pharmaceutical organization staff.
Potential Examples	• Posting vaccine or medical misinformation or disinformation, especially when highlighting specific company or health provider locational information to incite individuals to violence. • Inciting or espousing violence against a medical worker, public health official, or health care facility in support of an ideological goal—for example, threatening abortion or pro-life clinics. • Factory-sealed medical or pharmaceutical products that appear to have been tampered with or opened. • Showing unusual interest in a healthcare or public health facility, such as observation through binoculars, taking notes or photographs, or drawing maps of the facility.

INFORMATION TECHNOLOGY

SRMA	DHS
Potential Observers	Hardware, software, and information technology systems and service providers.
Potential Examples	• Unexplained persons near facility with observation equipment—such as high-magnification lenses or night-vision devices—or with detailed facility diagrams. • Searching for, viewing, or downloading material to gain functional expertise on sensitive information technology systems and services while attempting to obfuscate network activity.

NUCLEAR REACTORS, MATERIALS, AND WASTE

SRMA	DHS
Potential Observers	Nuclear power plant personnel and transporters; research and test reactor university and national lab staff; nuclear reactor fuel production and enrichment facility personnel.
Potential Examples	• Unauthorized or suspicious attempt to divert, delay, or reroute shipments of nuclear materials or waste. • Delivery or receipt of materials outside of normal operating hours and procedures. • Probing site security or attempts to surreptitiously surveil a facility.

TRANSPORTATION SYSTEMS

SRMAs	DHS; DOT
Potential Observers	Airport and heliport personnel; flight school instructors; transit bus, metro or subway, passenger and freight rail personnel; vehicle rental personnel; port, terminal, and cruise operators and staff.
Potential Examples	• Seeking unauthorized access to aviation, rail, or mass transit facilities, including to serve or pose as a pilot, conductor, or driver. • Training/probing on how to operate various transportation nodes without consideration to normal safety issues; for example, unusual interest in how to fly a plane but not how to land it. • Strong desire to handle particular items of luggage or strongly refusing assistance with numerous or heavy luggage. • Observed difficulty in explaining the planned use of a vehicle rental or observed difficulty in operating a vehicle, indicating a lack of familiarity, prior use, or experience. • The theft or disappearance of transportation safety and operational equipment and tools, including radios, identification badges, uniforms, or track tools that could enable an attack or are needed to prevent an attack.

WATER AND WASTEWATER SYSTEMS

SRMA	EPA
Potential Observers	Water and wastewater utility owners and operators.
Potential Examples	• Posting or downloading violent extremist messaging or scientific research of chemical or biological means to contaminate the water supply. • Attempting surveillance or unauthorized entry—in person or via cyber intrusion—into a water or wastewater treatment or processing plant, or sewer infrastructure.

WWW.FBI.GOV   WWW.NCTC.GOV   WWW.DHS.GOV

Individuals are strongly encouraged to contact their local FBI office by telephone or submit an online tip to the FBI at https://tips.fbi.gov if, based on these indicators and the situational context, they suspect an individual is mobilizing to violence.

In case of an emergency, please call 9-1-1.

Link to Booklet

2022 | 16804

2024-04989