FOOD DEFENSE AND BEYOND: IDENTIFYING & RESPONDING TO INSIDER THREATS

February, 2020
version 3

TABLE OF CONTENTS

Identifying and Responding to Insider Threats 3

Offender Characteristics 4

Behavioral Indicators 4

Violence Risk Assessment Tools 8

What Can You Do? 9

Supportive Programs 9

Policies 9

Proactive Program 10

Why Individuals May Not Report 11

Insider Threat Prevention 12

Concerns 14

Reporting an Incident 15

See Something, Say Something 16

Resources 17

References 18

IDENTIFYING AND RESPONDING TO INSIDER THREATS

Regardless of location, American citizens or businesses will continue to be targets for terrorists.[1] From an insider threat standpoint, this can be broadened to include criminally disposed or disgruntled employees who use their access to launch or enable attacks on persons, facilities, or resources. In many U.S. businesses and commercial settings, these resources include food and beverage products and supplies which are routinely assumed safe to consume.

Terrorists have demonstrated their willingness to employ non-traditional weapons to achieve their goals, and have long expressed interest in poisoning or adulterating ingestible items. Likewise, malicious insiders who for their own reasons wish to harm individuals, groups or their organizations as a whole.

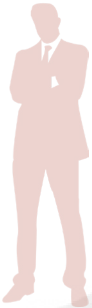
In some of these cases, there are observable human behavioral changes or warning signs which create opportunities to intervene. Universal training, awareness, and vigilance therefore offer the best hope of thwarting deliberate and potentially deadly contamination of food and beverages.

[1] Criminal and Epidemiological Investigation Handbook, Introduction: What is Bioterrorism?, 2011, page 6

OFFENDER CHARACTERISTICS

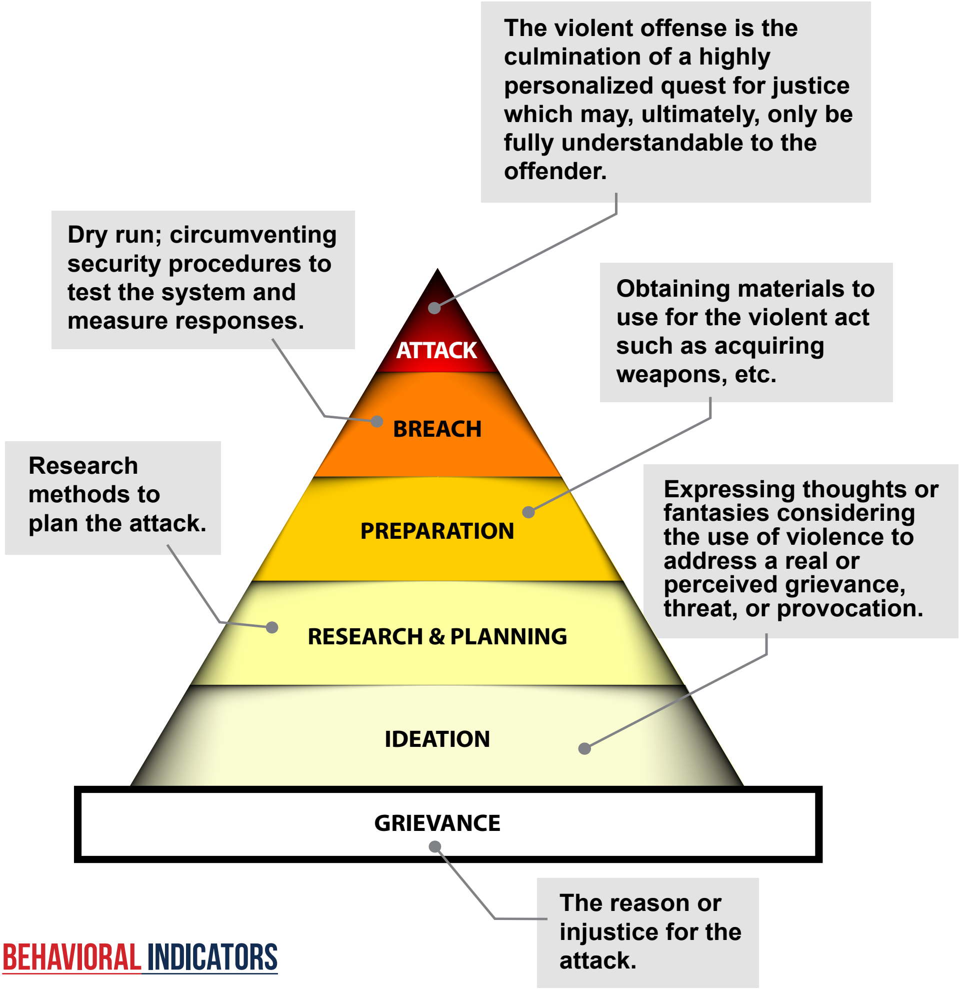
Despite common perceptions, violent or aggressive individuals do not typically just “snap”. Often, there are behavioral indicators which can be managed and (where mental illness is involved) successfully treated. In a work setting, manager and colleagues are well-situated to observe emerging or worsening problems in a person of concern, such as statements reflecting interest in terrorist groups or ideologies espousing violence; paranoid or irrational thinking; or increasingly hostile and antagonistic interpersonal behavior. Another potential indicator is animosity toward a particular demographic group, company or employer.

Grievances and targeted acts usually follow a progression that may be rapid or slow and may not be the same from person to person. A grievance could be against an individual, an institution, or other entity the person of concern feels slighted or wronged them. It may be nurtured and cultivated over a long period of time. Depending on the individual, it may be plainly evident to all around the person or kept hidden and private. For some individuals the motive to act out can be:



- Revenge for a perceived injury or grievance
- Quest for justice (as defined by the offender)
- Desire for notoriety or recognition
- Desire to solve a problem perceived to be unbearable
- Desire to kill or be killed

Perpetrators may research, plan and prepare with probing or breach of security measures. Time is on the side of the attacker as it may take weeks, months or even years to carry out the event. The following graphic illustrates a pathway to violence:


The violent offense is the culmination of a highly personalized quest for justice which may, ultimately, only be fully understandable to the offender.
Dry run; circumventing security procedures to test the system and measure responses.
Obtaining materials to use for the violent act such as acquiring weapons, etc.
ATTACK
BREACH
Research methods to plan the attack.
PREPARATION
Expressing thoughts or fantasies considering the use of violence to address a real or perceived grievance, threat, or provocation.
RESEARCH & PLANNING
IDEATION
GRIEVANCE
The reason or injustice for the attack.

BEHAVIORAL INDICATORS

The risk of violent, aggressive or sabotaging acts by an employee or other insider may be signaled by certain “concerning behaviors” that call for a closer look by the organization. There are however some common barriers to recognizing and reporting such concerns; for example, rationalizing warning behaviors as normal responses to stress; strategic avoidance of volatile individuals; or a perception that workplace security is solely management’s responsibility.

With any potential threat of terrorist activity or targeted violence, thoughtful and well-reasoned prevention plans can effectively mitigate risk. *If you see something, say something!* ®

Indicators of possible terrorist activity or other malicious acts can be either general or specific. The general indicators of potential insider threats include:

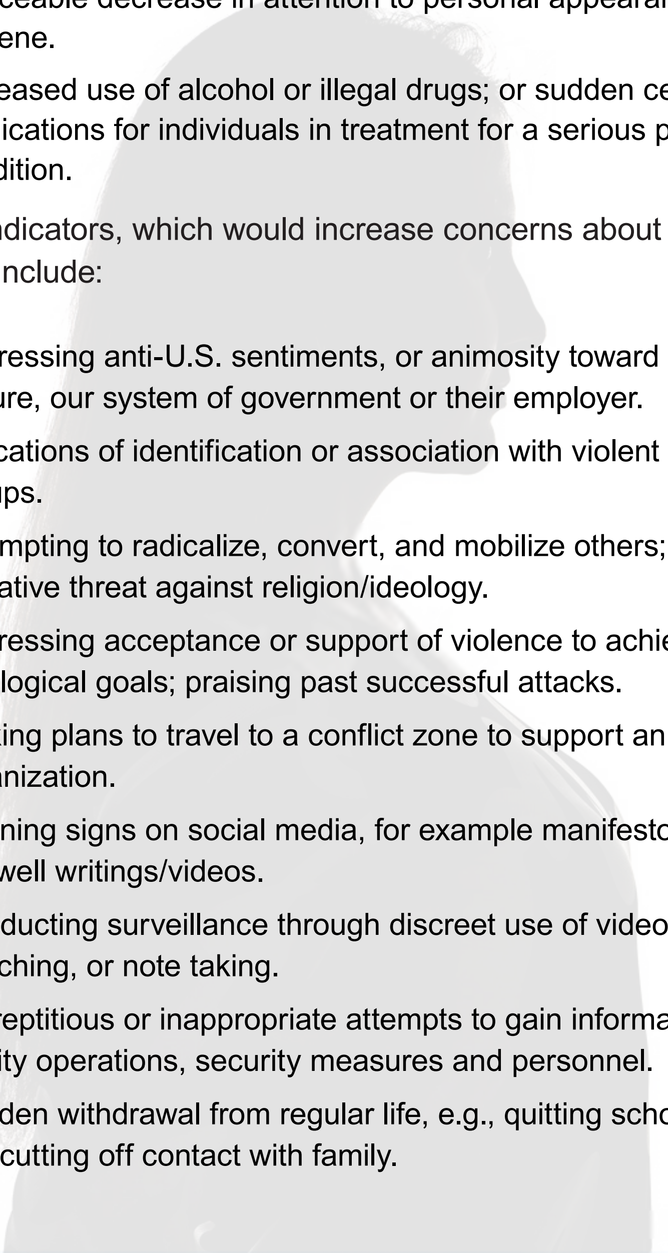
- Repeatedly violating rules, or angrily resisting normal changes in policies/procedures.
- Contempt and disrespect towards authority.
- Consistent blame of external factors for failure or disappointment - more concerning if the person seems vengeful.
- Persistent or escalating signs of disgruntlement, such as extreme carelessness, recklessness or antagonism toward others.
- Outrage or agitation over disciplinary, performance management or outside sanctions for misconduct.
- Threatening, aggressive or destructive behavior in the workplace or outside, with domestic abuse and related activity escalating this concern.
- Poor coping with significant losses or stressors, e.g., an unwanted breakup or divorce, loss of employment or professional reputation, legal or financial problems.
- Displays of emotional instability - explosive anger or otherwise disproportionate responses.
- Apparent depression, withdrawal, mood swings, or talk of suicide

– more concerning if the person also seems aggrieved.

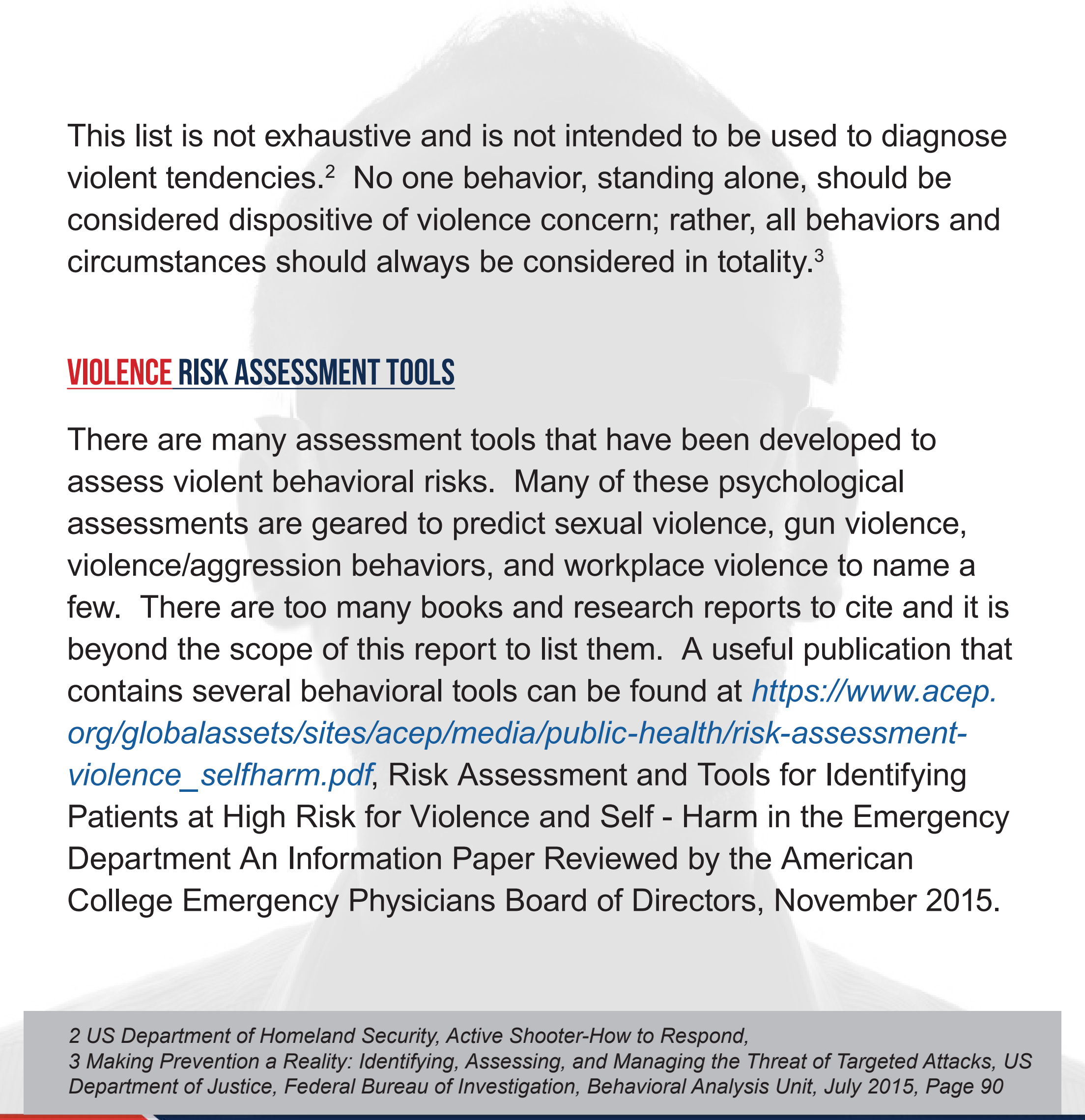
- Paranoid perceptions or accusations; hypersensitivity to criticism; refusal or inability to trust anyone.
- Noticeable decrease in attention to personal appearance and hygiene.
- Increased use of alcohol or illegal drugs; or sudden cessation of medications for individuals in treatment for a serious psychiatric condition.

Specific indicators, which would increase concerns about attack planning, include:

- Expressing anti-U.S. sentiments, or animosity toward American culture, our system of government or their employer.
- Indications of identification or association with violent extremist groups.
- Attempting to radicalize, convert, and mobilize others; promoting narrative threat against religion/ideology.
- Expressing acceptance or support of violence to achieve ideological goals; praising past successful attacks.
- Making plans to travel to a conflict zone to support an extremist organization.
- Warning signs on social media, for example manifestos or farewell writings/videos.
- Conducting surveillance through discreet use of video, camera, sketching, or note taking.
- Surreptitious or inappropriate attempts to gain information about facility operations, security measures and personnel.
- Sudden withdrawal from regular life, e.g., quitting school or one's job, cutting off contact with family.



- Unsolicited comments about firearms, explosives, contaminants or other means of attack.
- Apparent end of life preparations in the context of other concerning behavior, e.g., giving away possessions, writing a will, comments about “putting things in order”.



This list is not exhaustive and is not intended to be used to diagnose violent tendencies.[2] No one behavior, standing alone, should be considered dispositive of violence concern; rather, all behaviors and circumstances should always be considered in totality.[3]

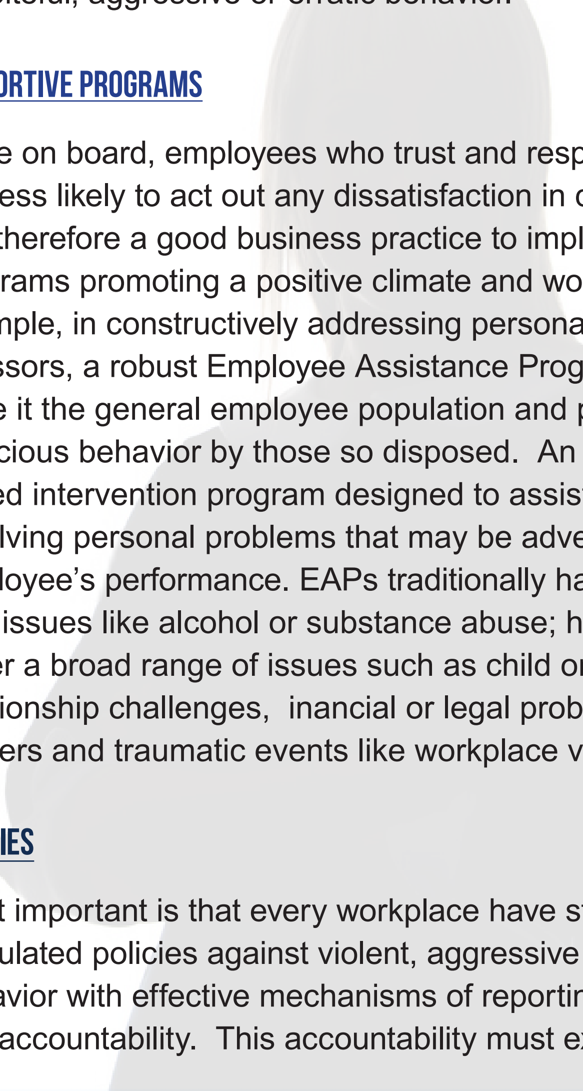
VIOLENCE RISK ASSESSMENT TOOLS

There are many assessment tools that have been developed to assess violent behavioral risks. Many of these psychological assessments are geared to predict sexual violence, gun violence, violence/aggression behaviors, and workplace violence to name a few. There are too many books and research reports to cite and it is beyond the scope of this report to list them. A useful publication that contains several behavioral tools can be found at *https://www.acep.org/globalassets/sites/acep/media/public-health/risk-assessment-violence_selfharm.pdf*, Risk Assessment and Tools for Identifying Patients at High Risk for Violence and Self - Harm in the Emergency Department An Information Paper Reviewed by the American College Emergency Physicians Board of Directors, November 2015.

2 US Department of Homeland Security, Active Shooter-How to Respond,
3 Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks, US Department of Justice, Federal Bureau of Investigation, Behavioral Analysis Unit, July 2015, Page 90

WHAT CAN YOU DO AS AN ORGANIZATION?

Certain individuals have negative “predispositions”, such as a volatile personality or a pattern of rule-breaking, which just make them poor employment candidates as well as potential insider threat risks. Recruitment, screening, and hiring processes should take this into account, being particularly careful about anyone with a history of spiteful, aggressive or erratic behavior.



SUPPORTIVE PROGRAMS

Once on board, employees who trust and respect the organization are less likely to act out any dissatisfaction in destructive ways. It is therefore a good business practice to implement supportive programs promoting a positive climate and work-life balance. For example, in constructively addressing personal and work-related stressors, a robust Employee Assistance Program (EAP) can benefit the general employee population and possibly decrease malicious behavior by those so disposed. An EAP is a work-based intervention program designed to assist employees in resolving personal problems that may be adversely affecting the employee’s performance. EAPs traditionally have assisted workers with issues like alcohol or substance abuse; however, most now cover a broad range of issues such as child or elder care, relationship challenges, financial or legal problems, wellness matters and traumatic events like workplace violence.

POLICIES

Most important is that every workplace have strong, clearly articulated policies against violent, aggressive or harassing behavior with effective mechanisms of reporting, investigation, and accountability. This accountability must extend to offending employees of all levels and statuses within the organization. Careful attention should also be given to protecting complainants, as well as responding (disciplinary, Human Resources (HR), EAP, occupational health) personnel from targeted violence or other retaliation.

PROACTIVE PROGRAM

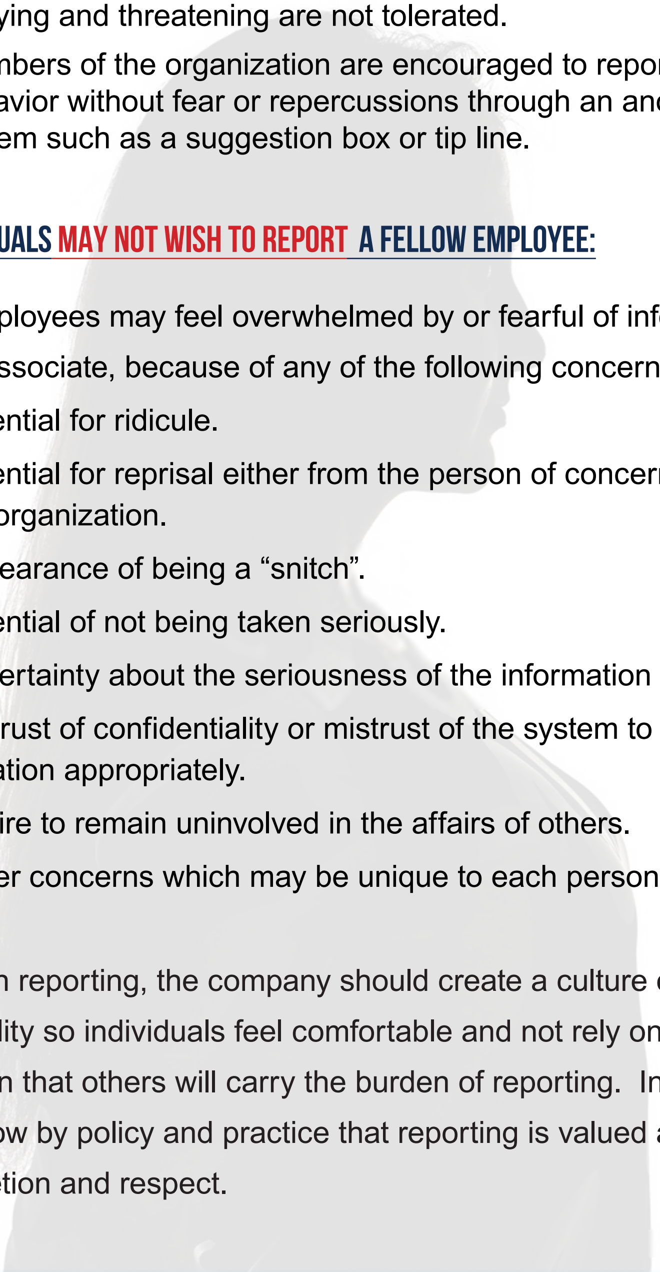
There is no “one right way” to address insider threat, as mitigation strategies and response options will depend on the individual organization, its size, culture, risk tolerance, and operating environment.[4] A proactive program might however include the following elements:

- Ensure that supervisors provide feedback about job performance in a timely and respectful manner, with clear guidance about how to improve where necessary.
- Promote a positive environment characterized by open communication and a proactive approach to conflict resolution.
- Provide alternate mechanisms for resolving disputes or for appeals when not satisfied with an initial attempt at resolution.
- Inform and consult employees about proposed company and process changes so that concerns can be anticipated and addressed before implementation.
- Incorporate regular team building activities to keep good morale.
- For employees of all levels, provide meaningful protection from workplace bullying, harassment and discrimination.

Additionally in effective programs:

- Everyone is treated with fairness and respect
- The organization communicates effectively
- Leaders set and enforce appropriate boundaries

[4] Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks, US Department of Justice, Federal Bureau of Investigation, Behavioral Analysis Unit, July 2015, Page 37



- Members of the organization are held accountable for their behavior.
- The organization fosters a nurturing environment.
- Bullying and threatening are not tolerated.
- Members of the organization are encouraged to report bad behavior without fear or repercussions through an anonymous system such as a suggestion box or tip line.

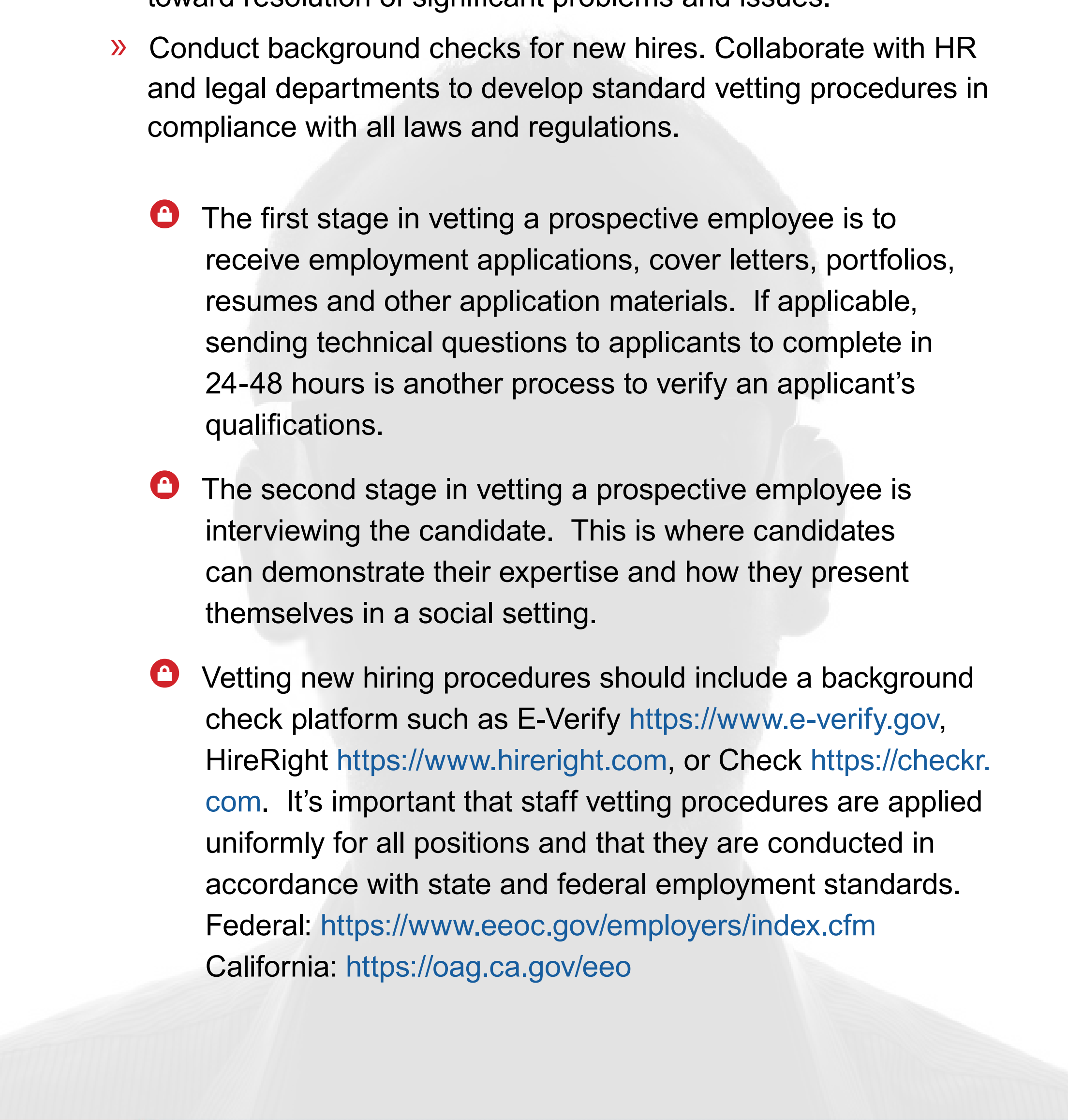
WHY INDIVIDUALS MAY NOT WISH TO REPORT A FELLOW EMPLOYEE:

Fellow employees may feel overwhelmed by or fearful of informing on a friend or associate, because of any of the following concerns:

- Potential for ridicule.
- Potential for reprisal either from the person of concern, or from the organization.
- Appearance of being a “snitch”.
- Potential of not being taken seriously.
- Uncertainty about the seriousness of the information or situation
- Mistrust of confidentiality or mistrust of the system to handle the situation appropriately.
- Desire to remain uninvolved in the affairs of others.
- Other concerns which may be unique to each person.

To assist in reporting, the company should create a culture of shared responsibility so individuals feel comfortable and not rely on the assumption that others will carry the burden of reporting. Individuals should know by policy and practice that reporting is valued and treated with discretion and respect.

SPECIFIC TO INSIDER THREAT PREVENTION:



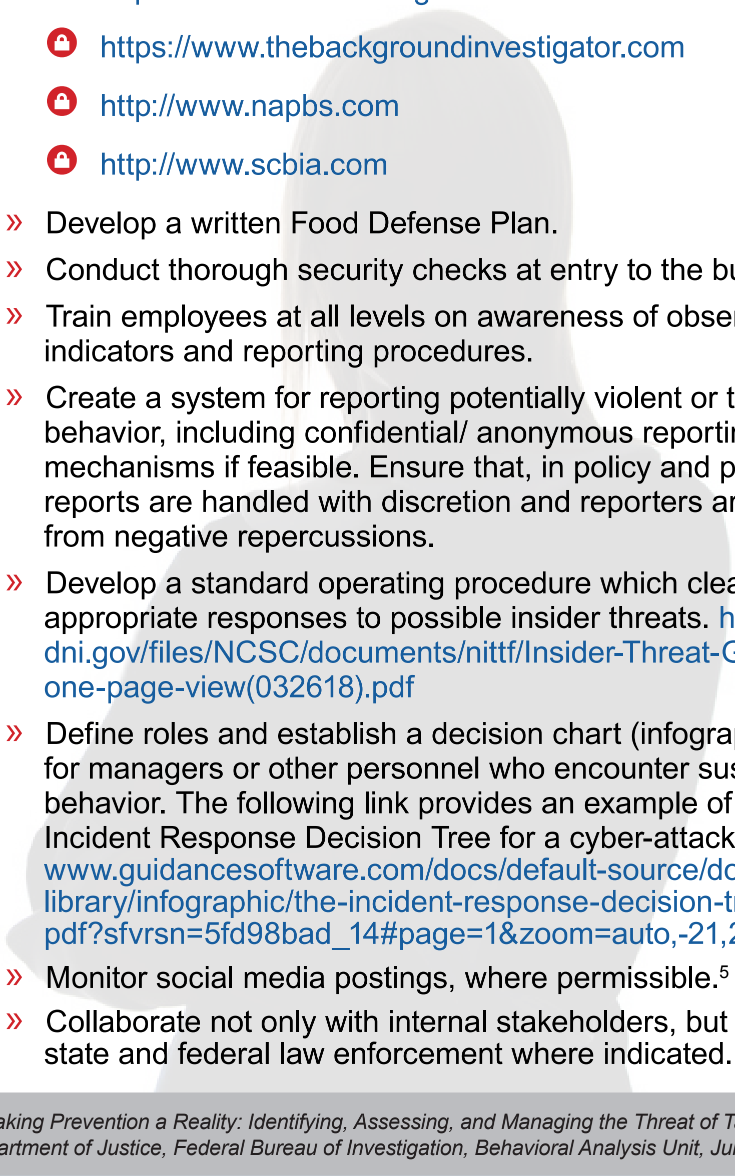
- Consider establishing a Food Safety/Food Defense Committee or designate a Food Safety and Defense Manager to address employee concerns. This ensures a unified and multi-disciplinary partnership, reflecting a commitment to engage employees toward resolution of significant problems and issues.
- Conduct background checks for new hires. Collaborate with HR and legal departments to develop standard vetting procedures in compliance with all laws and regulations.

  - The first stage in vetting a prospective employee is to receive employment applications, cover letters, portfolios, resumes and other application materials. If applicable, sending technical questions to applicants to complete in 24-48 hours is another process to verify an applicant’s qualifications.

  - The second stage in vetting a prospective employee is interviewing the candidate. This is where candidates can demonstrate their expertise and how they present themselves in a social setting.

  - Vetting new hiring procedures should include a background check platform such as E-Verify https://www.e-verify.gov, HireRight https://www.hireright.com, or Check https://checkr.com. It’s important that staff vetting procedures are applied uniformly for all positions and that they are conducted in accordance with state and federal employment standards.
    Federal: https://www.eeoc.gov/employers/index.cfm
    California: https://oag.ca.gov/eeo

Below is a list of organizations that can provide recommendations of companies or individuals who can conduct background checks. They can also provide guidance on background check laws and regulations:



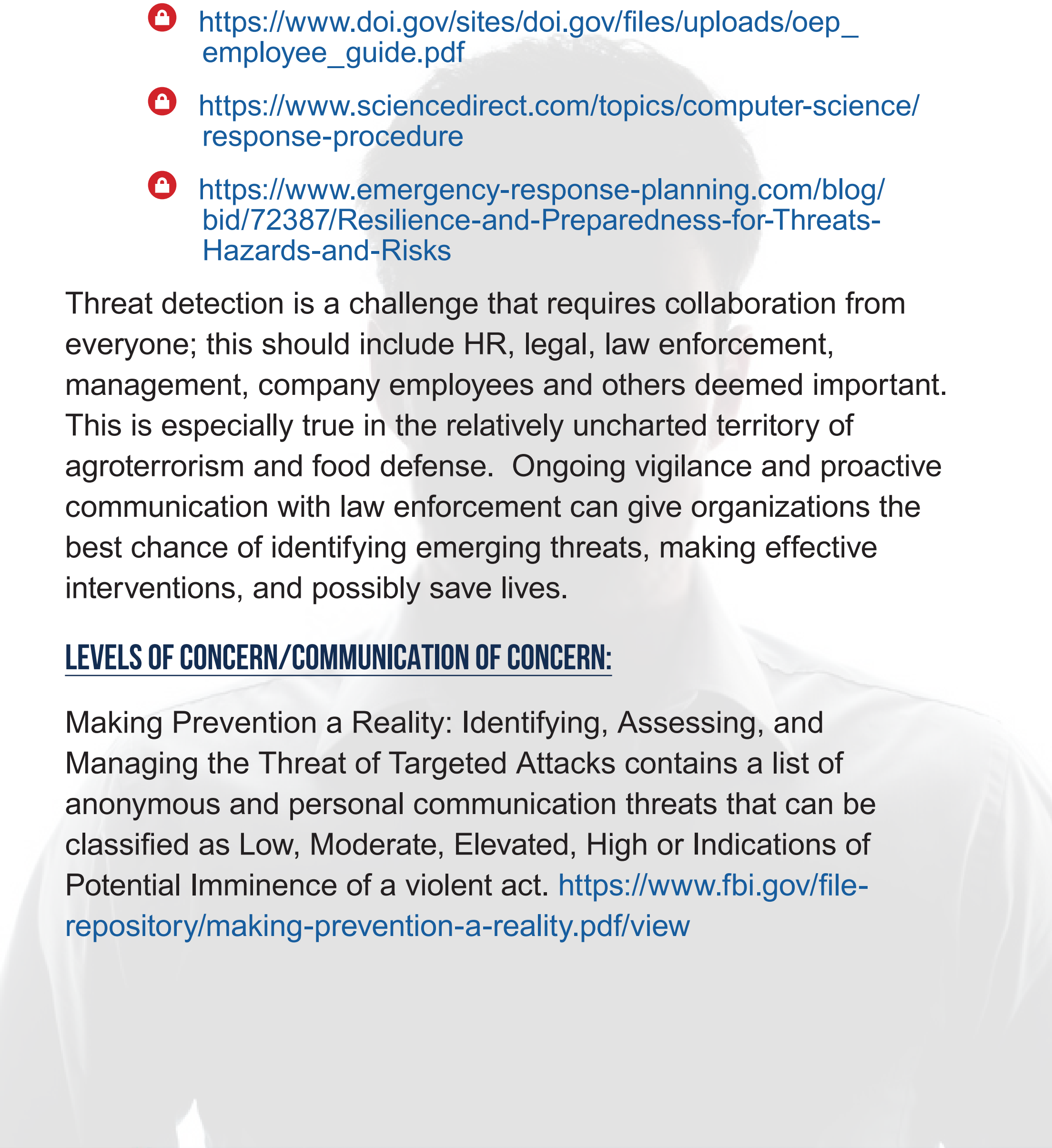
- https://www.acbi.net
- http://www.nalionline.org
- https://www.thebackgroundinvestigator.com
- http://www.napbs.com
- http://www.scbia.com

- Develop a written Food Defense Plan.
- Conduct thorough security checks at entry to the building.
- Train employees at all levels on awareness of observable indicators and reporting procedures.
- Create a system for reporting potentially violent or threatening behavior, including confidential/ anonymous reporting mechanisms if feasible. Ensure that, in policy and practice, reports are handled with discretion and reporters are protected from negative repercussions.
- Develop a standard operating procedure which clearly outlines appropriate responses to possible insider threats. https://www.dni.gov/files/NCSC/documents/nittf/Insider-Threat-Guide-2017-one-page-view(032618).pdf
- Define roles and establish a decision chart (infographic) for managers or other personnel who encounter suspicious behavior. The following link provides an example of an Incident Response Decision Tree for a cyber-attack. https://www.guidancesoftware.com/docs/default-source/document-library/infographic/the-incident-response-decision-tree.pdf?sfvrsn=5fd98bad_14#page=1&zoom=auto,-21,2603
- Monitor social media postings, where permissible.[5]
- Collaborate not only with internal stakeholders, but also local, state and federal law enforcement where indicated.

[5] Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks, US Department of Justice, Federal Bureau of Investigation, Behavioral Analysis Unit, July 2015, Page 38

» Develop a written Occupant Emergency Plan. See the links below for suggestion son developing an OEP plan:

- https://www.cdc.gov/niosh/docs/2004-101/emrgact/emrgact.pdf
- https://www.hsdl.org/?view&did=4512
- https://www.doi.gov/sites/doi.gov/files/uploads/oep_employee_guide.pdf
- https://www.sciencedirect.com/topics/computer-science/response-procedure
- https://www.emergency-response-planning.com/blog/bid/72387/Resilience-and-Preparedness-for-Threats-Hazards-and-Risks



Threat detection is a challenge that requires collaboration from everyone; this should include HR, legal, law enforcement, management, company employees and others deemed important. This is especially true in the relatively uncharted territory of agroterrorism and food defense. Ongoing vigilance and proactive communication with law enforcement can give organizations the best chance of identifying emerging threats, making effective interventions, and possibly save lives.

LEVELS OF CONCERN/COMMUNICATION OF CONCERN:

Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks contains a list of anonymous and personal communication threats that can be classified as Low, Moderate, Elevated, High or Indications of Potential Imminence of a violent act. https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

WHEN TO FILE AN INCIDENT REPORT

When the following behaviors are observed:

ESPOUSING VIOLENCE

A desire to commit and act to harm individuals or a company's products

SURVEILLANCE

Exhibiting an unusual interest in taking pictures or asking probing questions about security procedures

BREACH OR TESTING SECURITY RESPONSE

Researching methods or assessing gaps in security procedures

THEFT OR LOSS PREVENTION

Stealing items such as uniforms, badges belonging to facility

MATERIAL ACQUISITION

Accumulating materials or items to use in the attack

RECRUITING

Enlisting others to participate

SABOTAGE

Destroying property or products

WEAPONS COLLECTION

Collecting firearms, explosives, chemical or toxins

INTELLECTUAL PROPERTY

Theft of trade secrets or proprietary information

**This list is not exhaustive and is not intended to be used to diagnose violent tendencies. No one behavior, standing alone, should be considered dispositive of violence concern; rather, all behaviors and circumstances should always be considered in totality.*

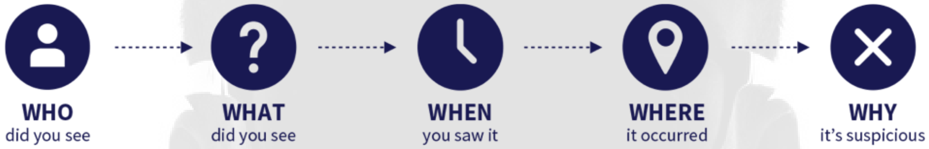
IF YOU SEE SOMETHING SUSPICIOUS, SAY SOMETHING®

Report suspicious activity to company personnel, law enforcement or 9-1-1 in case of emergency:

http://www.dhs.gov/see-something-say-something

HOW TO REPORT SUSPICIOUS ACTIVITY

Public safety and security is everyone's responsibility. If you see suspicious activity, report it to local law enforcement or a person of authority using the "5W's":



WHO did you see → **WHAT** did you see → **WHEN** you saw it → **WHERE** it occurred → **WHY** it's suspicious

RESOURCES

Websites:

- » http://www.dhs.gov/topic/countering-violent-extremism
- » http://securityawareness.usalearning.gov/itawareness
- » http://www.dhs.gov/active-shooter-preparedness
- » https://www.leo.gov
- » https://www.dhs.gov

Articles of Interest:

- » *National Insider Threat Task Force - Protect Your Organization from the Inside Out: Government Best Practices – 2016*
- » *National Risk Estimate: Insider Threat – Homeland Security – March 2014*
- » *National Cybersecurity and Communications Integration Center – March 1, 2014*
- » *Joint Intelligence Bulletin – August 31, 2016*

- Blum, D. (2013, September 1). A window on the world of homicidal poisoners. Los Angeles Times online, http://articles.latimes.com/2013/sep/01/opinion/la-oe-blum-poison-20130901.

- Bureau of Justice Statistics (2011, November). Homicide trends in the United States, 1980-2008. Washington D.C.: U.S. Department of Justice.

- Federation of American Scientists (2011). Case studies in agricultural biosecurity: Agroterrorism and food safety. At: https://fas.org/biosecurity/education/dualuse-agriculture/1.-agroterrorism-and-foodsafety/index.html.

- Gray, Richard, “Food Chain at Risk of Being Poisoned by Terrorist Groups,” Sunday Telegraph (London), June 4, 2011.

- New America (2017). In depth: Terrorism in America after 9/11. At: www.newamerica.org/in-depth/terrorism-in-america/who are the terrorists/.

- Shaw, E. and Sellers, L. (2015, June). Application of the critical-path method to evaluate insider risks. Studies in Intelligence, 59 (2), 41-48.

- Trestrail, J.H. (2007, 2nd Ed.). Criminal poisoning: Investigational guide for law enforcement, toxicologists, forensic scientists, and attorneys. Totowa, NJ: Humana Press.

UC DAVIS WIFSS

Western Institute for Food Safety & Security

USDA

cdfa
CALIFORNIA DEPARTMENT OF
FOOD & AGRICULTURE

UCDAVIS

WIFSS
Western Institute for
Food Safety & Security