FIRSTRESPONDER'STOOLBOX

TERRORIST INSIDER THREAT

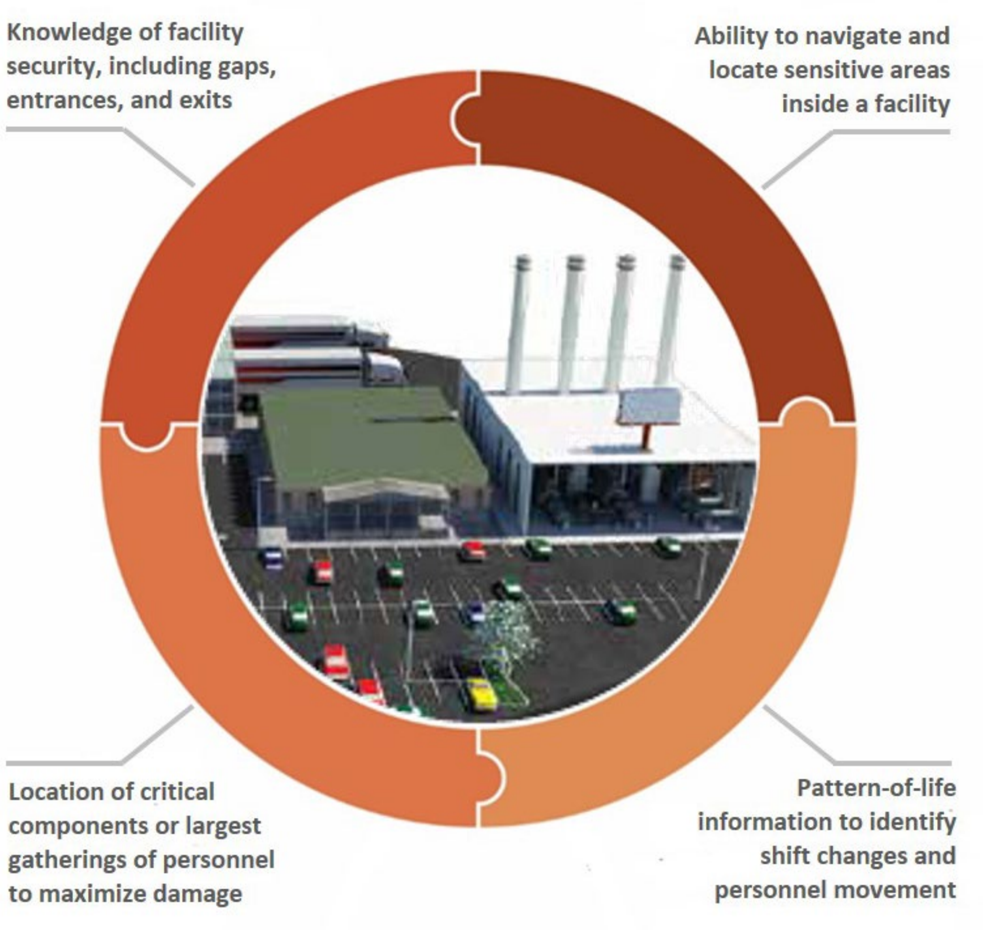
Insider threats continuously evolve and are a constant security vulnerability. Terrorists have used insiders to facilitate and conduct attacks and view them as valuable assets for obtaining information, gaining access, exploiting vulnerabilities, and challenging security countermeasures. An insider can enable an attack that would otherwise be difficult or unachievable without his or her access and knowledge or increase the severity or impact of an attack. Insider threats may involve one or more witting or unwitting individuals who are exploited for access to a target to carry out, facilitate, or enable terrorist activity. Complacent personnel may be vulnerable to exploitation and pose a security risk. Once within the organization an insider may be difficult to detect, which is why it is critical to develop and implement comprehensive protective measures, such as initial applicant and recurring employee screening, vetting, and training. Insiders pose threats to critical systems, networks, facilities, or operations by means including espionage, physical and intellectual property theft, sabotage, security compromise, and workplace violence.

- In December 2019, a Royal Saudi Air Force officer undergoing flight training at Naval Air Station Pensacola, Florida, shot US military members in a classroom, killing three and injuring eight. The perpetrator was radicalized in 2015 and communicated with AQAP until the night before the shooting.
- In February 2016, an explosion occurred shortly after takeoff onboard a commercial aircraft in Somalia. Two airport workers allegedly gave an explosive device concealed in a laptop to a third man, who died when the laptop exploded. Al-Shabaab claimed responsibility for the attack.
- In December 2013, authorities arrested an avionics technician in Wichita, Kansas, for attempted use of a weapon of mass destruction at an airport. The technician, who had a Secure Identification Display Area badge, armed what he believed to be an explosive device and tried to open a security access gate. He had performed preoperational surveillance, photographed gate access points, and researched flight schedules.

INDICATORS OF INSIDER THREAT ACTIVITY:

- Irregular work hours without authorization
- Unexpected or unexplained absences
- Unnecessary copying or printing of material, especially if it is proprietary or classified
- Unusual interest in gaining information outside the scope of their responsibility
- Consistently seeking to forge friendships to gain information from coworkers while off duty
- Improper use of information technology systems or repeated attempts to access restricted information
- Repeated attempts to enter restricted areas without proper credentials
- Off-duty presence on the property, possibly accompanied by unknown or unauthorized individuals
- Acquisition of unexpected wealth
- Unusual foreign travel
- Patterns of inaccurate statements or excuses for irregular behavior
- Threats made by disgruntled employees
- Signs of vulnerability—such as drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health, or hostile behavior—should trigger concern and a higher degree of oversight

KEY ELEMENTS TO SAFEGUARD AGAINST FACILITY ATTACKS: Studies of insider terrorist attacks show that attackers attempt to gain information in four areas:


Knowledge of facility security, including gaps, entrances, and exits
Ability to navigate and locate sensitive areas inside a facility
Location of critical components or largest gatherings of personnel to maximize damage
Pattern-of-life information to identify shift changes and personnel movement

SCOPE: An *insider* is a current or former employee or person with regular access to a facility who provides terrorists information or materials. Insiders may or may not actively participate in the attack. This product provides awareness on insider threats to public safety personnel, local government officials, critical infrastructure staff, and private-sector security partners and on how to identify insiders, starting with screening and vetting.

CONSIDERATIONS: PLACEMENT, ACCESS, and **POSITION** will determine the actions of an insider and the possible threat posed.

- **HIRING PROCESS:** Terrorists have used the employee application and hiring process to gain access to a target. In addition, existing employees may be co-opted for a variety of reasons, including disgruntlement, money, and being sympathetic to a cause or ideology. Consider the following possible protective and preventive measures:
  - Conduct comprehensive background checks and vetting of prospective employees, contractors, and support staff during the hiring process
  - Periodically reevaluate personnel on the suitability of their current level of access
  - Provide insider threat training to those involved in the hiring, evaluation, and human resources processes
- **CREDENTIALS:** Approved credentials ensure a level of trust, training, safety awareness, vetting, and access to sensitive areas. Some Federal credentials may allow unsupervised or unescorted access to critical infrastructure, such as the Transportation Worker Identification Credential and state-issued Commercial Driver's License (CDL) with hazardous materials endorsements. Credentials have varying application, vetting, and renewal requirements. Consider the following practices:
  - Enforce requirements to obtain and maintain access credentials
  - Promptly report and investigate potential illicit use or loss of credentials
  - Perform ID checks of each and every individual entering a facility

NOTICE: This is a Joint Counterterrorism Assessment Team (JCAT) publication. JCAT is a collaboration by the NCTC, DHS and FBI to improve information sharing among federal, state, local, tribal, territorial governments and private sector partners, in the interest of enhancing public safety. This product is **NOT** in response to a specific threat against the United States. It provides general awareness of, considerations for, and additional resources related to terrorist tactics, techniques and procedures, whether domestic or overseas. Consider the enclosed information within existing laws, regulations, authorities, agreements, policies or procedures. For additional information, contact us at JCAT@NCTC.GOV. **This document is best printed on 11x17.**

AUTHORED BY NCTC, DHS, FBI
2 SEPTEMBER 2020

TERRORIST INSIDER THREAT (*continued*)

NOTE: Employees may be vulnerable to elicitation during what may seem to be innocuous conversations with the public. This is called social engineering, which highlights the importance of operational and personal security and reporting as key elements of insider threat training.

- **ACCESS TO INFORMATION:** Seemingly innocuous information can be beneficial to terrorists— including knowledge of equipment, facilities, operations, and security procedures and familiarity with accesses, training, or weapons. Terrorists have used this information to assess a target, circumvent security, and gain access to restricted areas. Terrorists may target individuals on or off duty to gain this information. Consider the following practices:
    - Emphasize the importance of maintaining situational awareness and vigilance for insider threats, including outside the workplace
    - Openly and clearly communicate current threats and security challenges to increase chances of detection and prevention
    - Provide insider threat training and education, including indicators of suspicious behavior, proper reporting mechanisms, personal security practices, and technical vulnerabilities

- **ACCESS TO SPECIALIZED AREAS AND EQUIPMENT:** An employee's position can provide terrorists access to particular areas and equipment in a facility. Certain employee privileges or insufficient security regulations may allow employees to circumvent security checkpoints, which attack plotters could deem advantageous. Consider the following security measures:
    - Restrict credentials based on need to access secure or sensitive areas, and routinely audit access-control records
    - Collect equipment—such as uniforms, badges, personal protective equipment, keys—when employment ends and when issuing new equipment
    - Establish procedures for reporting lost or stolen items
    - Vary security screening and vehicle inspections by including unpredictable and unannounced activities
    - Monitor remote network accesses
    - Monitor sensitive areas for suspicious patterns of physical access

- **GENERAL:**
    - Establish organizational policies and procedures to deter and detect insider threats
    - Conduct regular insider threat awareness training
    - Establish an insider threat reporting mechanism
    - Perform spot security checks of all interior and exterior areas

SCREENING AND VETTING: Comprehensive screening and vetting of prospective employees can mitigate the threat of an insider. Background checks have complex privacy laws, which vary by jurisdiction and state on how to compile and safeguard the results of such searches. Employers should consult their state and local regulations. Suspicious results in any category may not be indicative of terrorism. The following list will assist in performing checks and is not exhaustive:

- **IDENTITY**
    - Document review:
        - □ Driver's license
        - □ Passport
        - □ Birth certificate
        - □ Military ID
        - □ School ID
    - Home address:
        - □ Utility bill
        - □ Mortgage or rent bill
        - □ Previous addresses
    - Social Security:
        - □ www.ssa.gov
        - □ www.ssa.gov/foia (to request information on already assigned SSNs)
        - □ https://classic.ntis.gov/products/ssa-dmf (Death Master File)

INDUSTRIAL SABOTAGE: While not terrorism related, in February 2019, one American and one Chinese national were indicted on seven counts of theft of trade secrets and one count of wire fraud. They were accused of a premeditated theft and transfer of trade secrets worth more than $100 million for setting up a Chinese company to compete with the US companies from which the trade secrets were stolen.

- **PERSONAL HISTORY**
    - References:
        - □ Personal
        - □ Professional
    - Motor vehicle: Contact your local department of motor vehicles
    - Credit, payment and loan history: Credit bureaus
    - Military record: www.archives.gov/facilities/mo/st_louis/military/personnel_records.html
    - Criminal history:
        - □ Federal: https://pacer.uscourts.gov
        - □ State: State law enforcement organization
        - □ County: County or local law enforcement organization
        - □ INTERPOL: www.interpol.int
        - □ National Crime Information Center: https://www.fbi.gov/services/cjis/ncic
        - □ National Sex Offender Public Website: www.nsopw.gov
        - □ Fingerprints: https://www.fbi.gov/services/cjis/identity-history-summary-checks or https://www.edo.cjis.gov
    - Incarceration records:
        - □ Federal Bureau of Prisons: https://www.bop.gov
        - □ National Institute of Corrections: https://nicic.gov/
        - □ State and local department of probation
        - □ State and local department of corrections
        - □ Municipal jail

- **REGULATORY**
    - Office of Foreign Assets Control: https://www.treasury.gov/about/organizational-structure/offices/pages/office-of-foreign-assets-control.aspx
    - GSA System for Award Management: https://www.sam.gov
    - Health and Human Services Office IG: https://www.oig.hhs.gov/fraud/index.asp
    - National Practitioner Data Bank: www.npdb.hrsa.gov
    - US Food and Drug Administration:
        - □ Bioresearch Monitoring Program (BIMO): www.fda.gov/science-research/clinical-trials-and-human-subject-protection/bioresearch-monitoring-program-bimo
        - □ FDA Debarment List: www.fda.gov/ora/compliance_ref/debar/default.htm
    - CDL: https://www.fmcsa.dot.gov/registration/commercial-drivers-license/employee-notification-services-state

OTHER RESOURCES

- **THE INSIDER THREAT BROCHURE:** https://www.dni.gov/files/NCSC/documents/products/Insider_Threat_Brochure.pdf
- **NATIONAL INSIDER THREAT TASK FORCE (NITTF):** https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
- **NATIONWIDE SUSPICIOUS ACTIVITY REPORTING (SAR) INITIATIVE:** https://nsi.ncirc.gov/
- **DHS SUSPICIOUS ACTIVITY REPORTING PROGRAM:** https://www.dhs.gov/see-something-say-something
- **HVE MOBILIZATION INDICATORS 2019:** https://www.dni.gov/files/NCTC/documents/news_documents/NCTC-FBI-DHS-HVE-Mobilization-Indicators-Booklet-2019.pdf

NOTICE: This is a Joint Counterterrorism Assessment Team (JCAT) publication. JCAT is a collaboration by the NCTC, DHS and FBI to improve information sharing among federal, state, local, tribal, territorial governments and private sector partners, in the interest of enhancing public safety. This product is **NOT** in response to a specific threat against the United States. It provides general awareness of, considerations for, and additional resources related to terrorist tactics, techniques and procedures, whether domestic or overseas. Consider the enclosed information within existing laws, regulations, authorities, agreements, policies or procedures. For additional information, contact us at JCAT@NCTC.GOV. **This document is best printed on 11x17.**

AUTHORED BY NCTC, DHS, FBI
2 SEPTEMBER 2020

JOINT
COUNTERTERRORISM
ASSESSMENT
TEAM

JCAT

PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE: □ LE □ FIRE □ EMS □ HEALTH □ ANALYSIS □ PRIVATE SECTOR DATE:

PRODUCT TITLE: NCTC-FBI-DHS (U) First Responder's Toolbox - Terrorist Insider Threat.pdf

POOR ○ ○ ○ ○ ● GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT