Suspicious Activity Reporting
Indicators and Behaviors

Behaviors	Descriptions
Potential Criminal or Noncriminal Activities Requiring Additional Information During Investigation	
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.
Testing of Security	Interactions with or challenges to installations, personnel, or systems that reveal physical personnel or cybersecurity capabilities.
Recruiting	Building operations teams and contacts, personnel data, banking data, or travel data.
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc. All reporting on photography should be done within the totality of the circumstances.
Observation/ Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g., engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
Materials Acquisition/Storage	Acquisition of unusual quantities of precursor materials such as cell phones, pagers, fuel, and timers, such that a reasonable person would suspect possible criminal activity.
Acquisition of Expertise	Attempts to obtain or conduct training in security concepts (military weapons or tactics) or other unusual capabilities that would arouse suspicion in a reasonable person.
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector) with regard to their personnel, facilities, systems, or functions.
Defined Criminal Activity and Potential Terrorism Nexus Activity	
Breach/Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g., police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification to misrepresent one's affiliation to cover possible illicit activity.
Theft/Loss/ Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents [classified or unclassified] which are proprietary to the facility).
Sabotage/ Tampering/ Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Cyberattack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/ infrastructure.
Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious or posing a threat to people or property. May or may not be in violation of Federal Aviation Regulations.