

Contact PaCIC Critical Infrastructure/ Key Resources Unit

Phone

(855) 772-7768

Facsimile

(717) 772-6917

Email

sp-protectpa@pa.gov

Mail

Pennsylvania State Police
PaCIC - CI/KR Unit
1800 Elmerton Avenue
Harrisburg, Pennsylvania 17110

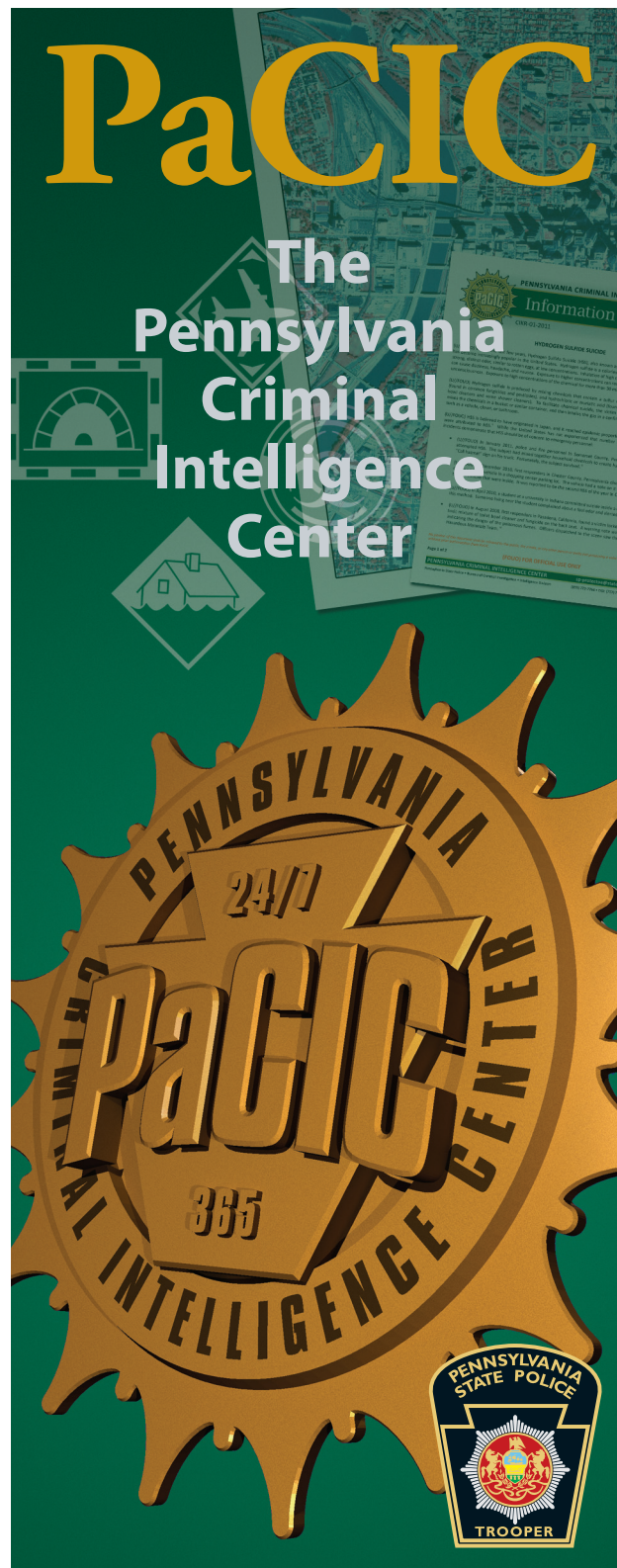


If you wish to report tips associated with terrorism, please call/email:

Terrorism Tip Line

(888) 292-1919

sp-intelligence@pa.gov



PaCIC and the CI/KR Mission

The Pennsylvania Criminal Intelligence Center (PaCIC) was originally created by the Pennsylvania State Police to enhance the crime prevention and investigation capabilities of local, state, and federal law enforcement agencies. PaCIC provides 24 hours a day, seven days per week access to its most powerful weapon—information.

Recently the need was recognized to increase information sharing between criminal justice agencies and the owners and operators of critical infrastructure and key resources throughout Pennsylvania with whom we share the fundamental responsibility of safeguarding our communities. Critical Infrastructure / Key Resources (CI/KR) are the assets, systems, and networks, whether physical or virtual, so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. A group of Intelligence Analysts at PaCIC are specifically tasked with monitoring potential threats to the various CI/KR sectors throughout Pennsylvania and keeping the owners and operators informed so they can better protect the Commonwealth's infrastructure, environment, and citizens from future threats.

Critical Infrastructure/ Key Resources Sectors

Homeland Security Presidential Directive - 7 established United States policy for enhancing critical infrastructure protection by establishing a framework for the Department of Homeland Security's partners to identify, prioritize, and protect the CI/KR in their communities from terrorist attacks. It defined 18 vital sectors that could, if attacked, significantly disrupt the functioning of government, businesses, and daily life and produce cascading effects felt far beyond the targeted sector and physical location of the incident. Since many of the sectors are intertwined, effects in one sector are many times felt in another.

Agriculture & Food farms, firms, and facilities that feed and clothe the American public

Banking & Finance banks, thrifts, credit unions, insurers, securities brokers/dealers, investment companies, and certain financial utilities

Chemical basic, specialty, and agricultural chemicals, plus pharmaceuticals and consumer products

Commercial Facilities public assemblies, sports leagues, gaming, lodging, outdoor events, entertainment and media, real estate, and retail

Communications provides voice services using terrestrial, satellite, and wireless transmission systems

Critical Manufacturing primary metal; machinery; electrical equipment, appliance, and component; and transportation equipment

Dams dams, navigation locks, levees, hurricane barriers, mine tailings, and other water retention facilities

Defense Industrial Base facilities performing research and development, design, production, delivery, and maintenance of military weapons systems, subsystems, components, or parts

Emergency Services first responder disciplines

Energy includes electricity, petroleum, and natural gas

Government Facilities buildings owned or leased by federal, state, territorial, local, or tribal governments

Healthcare & Public Health hospitals, clinics, and other aspects of public health

Information Technology hardware, software, and IT systems and services

National Monuments & Icons monuments and historical landmarks widely recognized or memorialized

Nuclear Reactors, Materials, & Waste all fields dealing with nuclear material including power plants, research, medical, and disposal

Postal & Shipping automated processing facilities; local delivery units; collection, acceptance, and retail operations; and mail transport vehicles

Transportation Systems aviation, highway, maritime transportation systems, mass transit, pipeline systems, and railways

Water drinking water and wastewater utilities

Reporting Suspicious Activity Indicators and Behaviors

Your impressions and assessment based on your professional experience are extremely valuable and should help guide you in determining if a fact pattern or set of circumstances is unusual. In addition to reporting suspicious activity to your local police department, you are encouraged to contact the Pennsylvania Criminal Intelligence Center's Terrorism Tip Line at (888) 292-1919. This will enhance statewide situational awareness and can potentially aid in the prevention of future terrorist acts through early identification and intervention.

Behaviors Potential Criminal or Noncriminal Activities Requiring Additional Information During Investigation	Descriptions
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.

Information to Gather

- Date and time
- Description of incident
- Number of individuals involved
- Contact information of reporting individual and witnesses
- Description of individuals and/or vehicles involved
- Why is it suspicious?

PaCIC Information Bulletins

To assist critical infrastructure owners and operators in Pennsylvania, Intelligence Analysts prepare and disseminate Information Bulletins on known risks and potential threats to critical infrastructure and key resources, as well as provide information regarding emerging trends or patterns that may impact various sectors.



Protection Partnership

In order to build this new partnership and obtain maximum benefit from this effort, an open dialogue between trained PaCIC analysts and our partners is essential. Critical infrastructure partners are encouraged to contact the CI/KR analysts at PaCIC to discuss emerging threats, share concerns, or simply provide feedback. The CI/KR analysts can be reached via email at sp-protectpa@pa.gov or by calling **(855) 772-7768**. Suspicious activity can be reported to PaCIC 24 hours a day, seven days a week, by calling **(888) 292-1919** or via email at sp-intelligence@pa.gov.

Getting Started

If you are interested in receiving future CI/KR products, please email sp-protectpa@pa.gov to request a registration form. Once this form has been returned to the CI/KR analysts at PaCIC, you will begin receiving alerts and briefs relevant to your sector.

Terrorism Tip Line

(888) 292-1919

sp-intelligence@pa.gov