



NJOHSP

INFRASTRUCTURE PROTECTION RESOURCE SHEET

COMMUNICATIONS

Communications infrastructure, including wireless, wireline, satellite, cable, and broadcasting systems, plays a vital role in routine business and government operations. Nearly all infrastructure sectors depend in some way upon communications infrastructure, and a disruption would cause cascading impacts throughout the state.

Threats of Most Concern to Communications Infrastructure Include:

- Small-arms attacks on infrastructure
- Improvised explosive devices
- Cyber attacks to routing and switching software and user applications

Potential Indicators of Terrorist Activity Include:

- Suspicious or illegally parked vehicles near communications infrastructure such as fiber-optic cables
- Unattended packages that could contain explosives
- Damage to gates, doors, locks, or security systems
- Individuals wearing official uniforms or being in authorized areas without official credentials

Potential Indicators of Terrorist Surveillance Include:

- Individuals loitering or unattended vehicles near communications buildings, towers and switches over multiple days with no reasonable explanation
- Employees being questioned about entrance restrictions for personnel and visitors, communications system operations, and security measures
- Unfamiliar employees, contract workers, or unannounced maintenance activities
- Individuals photographing, recording, or otherwise focusing on security features, including security cameras, security personnel, gates, and barriers

Protective Measures Include:

- Implement credential standards to control access to secure areas
- Develop and exercise security and emergency response plans
- Incorporate security awareness and response procedures into employee training
- Establish regular communication with local law enforcement and emergency management officials
- Monitor access to facilities and restricted areas with cameras
- Establish and document key control procedures for tracking, collection, and loss
- Develop procedures for monitoring, detecting, and reporting cyber incidents
- Encourage employees to report any threats or suspicious activity

Incident Response

Alert law enforcement immediately by calling 9-1-1

Connect.

Visit njohsp.gov to connect with NJOHSP, find resources available, and maintain awareness of threat information.

Prepare.

Visit njohsp.gov/resources to learn about planning resources for your organization.

Train.

Visit njohsp.gov/programs to learn about training and exercises for your organization.

Report Suspicious Activity.

Dial 1-866-4-SAFE-NJ or e-mail tips@njohsp.gov to report suspicious activity in New Jersey.

Visit njohsp.gov/report to learn more about suspicious activity reporting.