



NJOHSP

INFRASTRUCTURE PROTECTION RESOURCE SHEET

ELECTRIC INFRASTRUCTURE

Electric infrastructure is necessary for the generation, transmission, and distribution of electricity. Disruptions to normal functionality will directly impact consumers of electric service. The reliance upon electrical service and the cascading impacts of disruption make the energy grid a potential terrorist target.

Physical Threats of Most Concern Include:

- Small-arms attacks
- Improvised explosive devices
- Vehicles approaching the facility unimpeded at high speeds
- Cyber attack causing physical disruptions or damage

Potential Indicators of Terrorist Activity Include:

- Individuals wearing bulky clothing that may be used to conceal weapons or explosives
- Suspicious or illegally parked vehicles
- Unattended packages that could contain explosives
- Persons attempting to gain unauthorized entry to restricted areas
- Individuals wearing official uniforms or accessing authorized areas without official credentials
- Damage to restricted areas, perimeter lighting, security cameras, doors, locks, or other security devices

Potential Indicators of Terrorist Surveillance Include:

- Persons loitering in the same area over multiple days with no reasonable explanation
- Employees being questioned about venue operations or security measures
- Unfamiliar employees, contract workers, or unannounced maintenance activities in the vicinity
- Photography or videography focused on security features, including cameras, security personnel, gates, and barriers

Protective Measures Include:

- Restricting unauthorized access through the use of locked entrances and exits, fencing, and other impediments to pedestrians and vehicles
- Employing perimeter alarm systems that dispatch personnel or law enforcement to investigate forced intrusions, signs of surveillance, and other disturbances
- Safeguarding vulnerable equipment with projectile barriers
- Posting adequate signage throughout the facility to warn potential intruders of trespassing and the dangers of electrical infrastructure
- Ensuring lighting around the facility, which provides optimal visibility for security cameras
- Providing mandatory cybersecurity training for employees
- Maintaining a separate network for industrial control systems that is not connected to the Internet
- Managing the authentication of Internet users through multi-factor authentication, reducing user privileges, and implementing secure password policies
- Participating in cybersecurity information-sharing platforms such as the Cybersecurity Risk Information Sharing Program from the US Department of Energy, and the [New Jersey Cybersecurity and Communications Integration Cell \(NJCCIC\)](#)