U.S. Department of Homeland Security

Protective Security Coordination Division
Office of Infrastructure Protection

Infrastructure Protection Report Series

Restaurants

Hundreds of thousands of restaurants throughout the Nation serve more than 70 billion meals annually, bringing in revenue of more than $440 billion, employing more than 12 million people, and accounting for 4% of the US gross domestic product. Restaurants are open-access, limited egress congregation points and have been successfully targeted by terrorists on numerous occasions in the past.

Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to restaurants include:

- Small arms attack
- Improvised explosive devices (IEDs)
- Vehicle-borne improvised explosive devices (VBIEDs)
- Arson or incendiary attack
- Chemical or biological attack
- Intentional food contamination

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons in restaurants wearing unusually bulky clothing that might conceal suicide explosives or weapons
- Suspicious or illegally parked vehicles near the restaurant or where crowds gather
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Evidence of unauthorized access to heating, ventilation, and air-conditioning (HVAC) areas; indications of unusual substances near air intakes

Indicators of potential surveillance by terrorists include:

- Persons discovered with restaurant photos or diagrams with facilities highlighted
- Persons parking, standing, or loitering in the same area over a multiple-day period with no reasonable explanation
- Persons using or carrying video/camera/observation equipment over an extended period
- Restaurant personnel being questioned off-site about restaurant operations or security measures
- Restaurant employees changing working behavior or working more irregular hours without explanation
- Persons observed or reported to be observing restaurant deliveries, food preparation, and storage
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unfamiliar employees (e.g., cleaning crews), or other contract workers
- Restricted areas left unsecured
- Threats from unidentified sources
- Unusual or unannounced maintenance activities in the vicinity of the restaurant
- Sudden losses or thefts of surveillance equipment or hazardous material (e.g., cleaning/disinfection)
- Suspicious behavior of patrons asking about food supplies, preparation, and storage

Common Vulnerabilities

The following are key common vulnerabilities of restaurants:

- Unrestricted public access
- Limited to no in-place physical security measures or guard force
- Unrestricted access by food suppliers, vendors, and maintenance workers
- Limited employee background checks
- Unrestricted access to peripheral areas, such as parking lots

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for restaurants include:

- **Planning and Preparedness**
  - Develop a comprehensive security plan and emergency response plan
  - Conduct regular exercises of the plan
  - Maintain constant awareness of current threat condition and available intelligence information
  - Develop policies and procedures for dealing with hoaxes and false alarms

- **Personnel**
  - Conduct background checks on restaurant employees
  - Incorporate food security awareness and appropriate response procedures for security situations into employee training programs

- **Access Control**
  - Provide appropriate signs to restrict access to nonpublic and restricted areas (food preparation/storage areas, cleaning/sanitizing material)
  - Identify and control access by employees, vendors, delivery personnel, visitors, and contractors
  - Install and regularly test access control systems and intrusion detection systems in sensitive areas
  - Remove any vehicles that have been parked for an unusual length of time

- **Barriers**
  - Provide adequate locks, doors, and other barriers for designated areas
  - Minimize, to the extent practical, places in public areas that an intruder could remain unseen after work hours
  - Provide adequate interior and exterior lighting, including emergency lighting, where appropriate, to facilitate detection of suspicious or unusual activity

- **Communications and Notification**
  - Install, maintain, and regularly test the facility security and emergency communications system
  - Develop redundancy in the equipment, power supply, and means used to contact security officials
  - Communicate threat level information to restaurant employees
  - Take any threatening or malicious telephone call or bomb threat seriously
  - Encourage employees and the public to report any threat situation or suspicious activities

- **Monitoring, Surveillance, Inspection**
  - Install closed-circuit television (CCTV) systems, intruder detection systems, and lighting to cover key areas, including parking lots
  - Monitor and restrict the type of personal items allowed in nonpublic areas of the facility; prevent staff from bringing personal items (e.g., lunch containers, purses) into nonpublic food preparation or storage areas.
  - Train security personnel to watch for suspicious or unattended vehicles near facilities; watch for abandoned parcels, suitcases, backpacks, and packages and any unusual activities; and monitor delivery of food and supplies
  - Regularly inspect and monitor food supply, display, and storage areas, trash bins, parking lots

- **Infrastructure Interdependencies**
  - Provide adequate security and backup for critical utility services (e.g., electricity, natural gas, water)

- **Cyber Security**
  - Implement and review, if applicable, computer-based operational systems
  - Eliminate, if applicable, any information from restaurant Web site that might provide security information to adversaries
  - Establish, if applicable, a system that allows food supply computer transactions to be traced

WARNING

This document is **FOR OFFICIAL USE ONLY (FOUO).** It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

At a minimum when unattended, this document is to be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza or locked area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

For more information about this document contact:
Protective Security Coordination Division
(IPassessments@dhs.gov or FOBanalysts@dhs.gov)