LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

AUGUST 2023

ANTITERRORISM AWARENESS MONTH

This month, the LIS Solutions August Security Monthly Newsletter focuses on Antiterrorism (AT) Awareness Month in relation to the Center for Development of Security Excellence (CDSE) and the Defense Counterintelligence and Security Agency (DCSA) guidance.

To combat terrorism, it is our duty to utilize the required resources to train our employees, prevent future harm, and detect acts of terrorism. This month's newsletter aims to equip our employees with the ability to identify threats and report suspicious activity related to terrorism, ensuring the protection of American life, infrastructure, and prosperity against potential harm.

WHAT IS TERRORISM?

Per the FBI, there are two different terrorism definitions.

1. International Terrorism: regards to foreign (outside the USA) acts of violence that are committed by people, or groups of people, who are inspired by, or associated with, designated foreign terrorist organizations or nations.

2. Domestic Terrorism: regards to domestic (inside the USA) acts of violence that are committed by people, or groups of people, in relation to politics, religion, society, ethnicity, or environments.

FBI. (n.d.). Terrorism.
https://www.fbi.gov/investigate/terrorism

PREVENTING TERRORISM:

In order to prevent terrorism, it is critical for individuals to develop and maintain situational awareness. Adversaries aim to exploit complacency and societal norms, striking when least expected. It is essential to remain vigilant, as adversaries take advantage of people feeling too comfortable and secure.

Instead, we strongly recommend always being on alert and familiarizing yourself with your surroundings. Terrorist groups, whether foreign or domestic, target various locations such as schools, grocery stores, entertainment centers like movie theaters, and stadiums. Any threat from an adversary can occur anywhere and to anyone.

It is important to recognize suspicious behavior! Stay vigilant regarding activist groups and their protests. If you observe any signs of negativity escalating, prioritize moving to a safer environment and away from the threat. Immediately contact emergency services to report the incident. Additionally, we strongly advise against contributing, escalating, or associating with any acts of violence aimed at overthrowing the United States Government.

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

ANTI-TERRORISM IT CYBER SECURITY AND YOU

Terrorism can take many forms. Terrorist attacks aren't necessarily violent. They can be designed & used to disrupt commerce, travel, access to food, water, power, healthcare, or other basic needs of the public, government, or private industry.

Terrorism can be used by individuals, private groups including extremist religious groups, or foreign governments. Any attack against us, a government contractor, may not actually be aimed at us, but at our government clients.

A slogan to use, know, and live by in today's threats: ***"If you see something, say something."***

Terrorists, like thieves, may attempt to gain access to critical data via Phishing, attempts to hack your computer account, install viruses or other malware, etc.

Here is a brief review of our LIS IT Security Requirements: Portable equipment including laptops, data storage devices such as memory sticks, external hard drives, floppy, and Zip disks should not be left unattended. The data you work with is extremely confidential & must be kept secure. Like confidential documents, IT equipment must be kept secure at our office, a client's office, or on the job site. Your laptop should be either logged out or "locked" in Microsoft Windows whenever you are not actively using it. IT Equipment must be secured each night and should not be left unattended in our office outside of normal business hours. If you do not take it with you in the evening, it should be placed in a locked drawer or cabinet in your office.

The February LIS Security Newsletter also has excellent information and tips for security awareness: **https://www.lissol.com/_files/ugd/cde1f8_39304f75333e479cb55d236a5dccdd61.pdf**

Article to read at your leisure: Veteran.com Team. (2022a, December 23). Antiterrorism Awareness Month 2023. **https://veteran.com/antiterrorism-awareness-month/**

FORCE PROTECTION STANDARDS

FPCON Normal	This condition applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DOD installations and facilities.
FPCON Alpha	This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON Bravo measures. The measures in this force protection condition must be capable of being maintained indefinitely.
FPCON Bravo	This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this FPCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.
FPCON Charlie	This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is likely. Implementation of measures in this FPCON for more than a short period will probably create hardships and affect the peacetime activities of the unit and its personnel.
FPCON Delta	This condition applies in the immediate area where a terrorist attack occurred or when intelligence shows that a terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition.