Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 17 — Issue 44 | November 2, 2017

Truck ramming attacks appeal in their simplicity and success

Vehicle ramming attacks against westerners are likely to continue due to how simple it is to plan and carry them out, how successful these attacks are, and how difficult it is to predict or detect the planning process. So far, major cities are the primary targets both here and abroad due to the enticing population density, but any area where people congregate is at risk. Mitigation strategies to consider:

- Restrict vehicle access in "pedestrian only" areas and install physical barriers.
- Train personnel on active shooter response, suspicious activity reporting (SAR), and improvised explosive devices (IED) and vehicular IED awareness and recognition.
- Increase patrols at special events and install temporary physical barriers.

Several ramming attacks used rented trucks, and this process may be one of the only points to spot and report suspicious activity. The Transportation Security Administration trifold "Safeguarding American's Transportation System" (PDF, 1 MB) can help first responders educate businesses on SAR recognition and reporting. The TSA video training series "First Observer Plus" also works toward this goal.

(Source: TSA)

SOP guidance and a new final standard for sUAS operations

There is a limited amount of official or proposed guidance on small unmanned aircraft system (sUAS, or "drones") programs currently, and two newly available documents for public safety departments may be helpful.

"Standard Operating Policy (SOP) Guidance for Law Enforcement Use of Small Unmanned Aircraft Systems (sUAS)" is a new template SOP available from the Justice Technology Information Center (JUSTNET). To obtain a copy of the template, send an email to asknlectc@justnet.org from a legitimate government agency/law enforcement agency email address (no Yahoo, Gmail, etc.).

This SOP policy guidance is suggested for law enforcement agencies to use as a general template for developing and enhancing their internal sUAS programs. It should not be construed as the concise final program guidance for any agency, only an example agencies can base their own unique sUAS program on.

The Public Safety Aviation Accreditation Commission (PSAAC) and the Airborne Law Enforcement Association (ALEA) released the final version of standards for sUAS use by public safety agencies. The new sUAS standard has five sections: administration, flight operations, safety, training and maintenance, and discusses tactical, legal and ethical uses of sUAS. Those interested in obtaining a copy of the sUAS standard should contact the PSAAC at jdigiovanna@psaac.com or ALEA at dschwartzbach@alea.org.

(Source: JUSTNET and PSAAC)

Training and resources for cybersecurity professionals

A key risk to our economy and security is the shortage of cybersecurity professionals to protect our extensive networks. Growing the next generation of a skilled cybersecurity workforce – along with training those already in the workforce – is crucial to building

Highlights

Truck ramming attacks appeal in their simplicity and success

SOP guidance and a new final standard for sUAS operations

Training and resources for cybersecurity professionals

Assisting victims of violent crime

U.S. Fire Administration

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.

stronger defenses. Begin or develop your cybersecurity career by checking out the National Initiative for Cybersecurity Education (NICE) Framework, which provides information on the knowledge, skills and abilities employers value. Follow this up with a visit to Cyber Seek, an interactive website offering tools and data supporting cybersecurity duties.

Once you know the desired skills, take advantage of free training with the Federal Virtual Training Environment, available to all state, local, tribal, and territorial (SLTT) government employees, veterans and government contractors. Texas A&M's Engineering Extension Service offers cybersecurity courses in addition to those related to fire and emergency services, law enforcement, infrastructure safety and incident response.

For those working with Industrial Control Systems (ICS), the ICS Computer Emergency Response Team's Virtual Learning Portal offers several hours of basic information. Many universities also offer free courses through their online learning portal or edX. The Code Academy also offers free instruction in several popular coding languages.

We should all stay current with the cybersecurity environment. United States citizens who pass a basic background check can join the FBI's InfraGard program to receive information direct from the FBI. In addition, the Multi-State Information Sharing and Analysis Center (MS-ISAC) is the focal point for cyber threat prevention, protection, response and recovery for SLTT governments. Individuals can register with the MS-ISAC to receive some information (e.g., patch advisories and webcasts), while all SLTT governments can join for full access to MS-ISAC products.

(Source: MS-ISAC)

Assisting victims of violent crime

Communities affected by mass violence or terrorism must pick up the pieces and heal. Often they are expected to carry on as though nothing happened, yet this is difficult as these violent acts change communities and their collective sense of safety. Jurisdictions are putting more resources and time into victim assistance programs as the overarching benefits are better documented.

The Office of Victims of Crime Training and Technical Assistance Center's (OVC TTAC) free webinar "Mass Violence Communications" on Tuesday, November 7 from 10-11:30 a.m. Eastern, assists jurisdictions preparing to help community members after mass violence. Effective communications during or after violent incidents decreases anxiety, provides support, helps sustain order and reduces the impact of misinformation.

The webinar's target audience is those who are responsible for planning and responding to incidents of mass violence and terrorism, including law enforcement leaders, emergency management officials, healthcare providers and other community leaders or mental health providers.

This webinar is part of the OVC TTAC "Helping Victims of Mass Violence and Terrorism: Planning, Response, Recovery, and Resources Toolkit" training series. Visit the OVC website for a list of crime victim resources by state such as regional networks, victim rights legal programs, statistics reports and victim notification systems.

(Source: Office of Victims of Crime)

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI office and also the State or Major Urban Area Fusion Center.

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201,** or by email at **nicc@dhs.gov.**

The U.S. Fire Administration maintains the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC). For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.