Homeland Security

The Partnership Bulletin

From the National Protection and Programs Directorate / Office of Infrastructure Protection

August 17, 2018 **Volume 4, Issue 10**

The Partnership Bulletin, designed for widest distribution, provides a snapshot of upcoming training and exercise opportunities, critical infrastructure events, and key announcements. To receive this Bulletin directly or to share upcoming events or articles, please send your request or submission to partnershipbulletin@hq.dhs.gov.

Help the Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP) make The Partnership Bulletin better. Please tell us what you think.

In This Issue

DHS National Cybersecurity Summit Highlights

On Tuesday, July 31, the Department of Homeland Security (DHS) hosted the first-of-its-kind National Cybersecurity Summit in New York City, bringing together industry partners and top federal officials with the goal of laying out a vision for a collective defense strategy to protect our nation’s critical infrastructure. The summit brought together Vice President Mike Pence, Secretary Kirstjen M. Nielsen, Secretary of Energy Rick Perry, Federal Bureau of Investigation Director Christopher Wray, and Commander, U.S. Cyber Command and Director, National Security Agency General Paul M. Nakasone, DHS Under Secretary Chris Krebs, U.S. Secret Service Director

Randolph Alles, and DHS Assistant Secretary Jeanette Manfra, alongside top CEOs from across industry including the telecom, financial, and energy sectors.

“We are not waiting for the next intrusion before we act,” said DHS Secretary Kirstjen Nielsen. “We are taking a clear-eyed look at the threat and taking action—and notably—collective action to combat them.”

Throughout the Summit, DHS and its government and industry partners agreed on a series of concrete steps to better understand what is truly critical and work together to reduce strategic risk.

Secretary Nielsen announced the creation of the National Risk Management Center, which will coordinate national efforts to protect the nation’s critical infrastructure.

The National Risk Management Center will create a cross-cutting risk management approach across the federal government and our private sector partners through three lines of effort:

- Identifying and prioritizing strategic risks to national critical functions;
- Integrating government and industry activities on the development of risk management strategies; and
- Synchronizing operational risk management activities across industry and government.

The National Risk Management Center advances the ongoing work of DHS and government and private sector partners to move collaborative efforts beyond information sharing and develop a common understanding of risk and joint action plans to ensure our nation’s most critical services and functions continue uninterrupted in a constantly evolving threat environment. The Center will work closely with the National Cybersecurity and Communications Integration Center (NCCIC), which will remain DHS’s central hub for cyber operations focused on threat indicator sharing, technical analysis and assessment services, and incident response. The two centers will work hand-in-hand to ensure effective coordination between strategic risk management and tactical operations.

The Department also unveiled the formation of the Information and Communications (ICT) Supply Chain Risk Management Task Force, which will be comprised of subject matter experts from industry and government. The Task Force will be housed in the Center and will examine and develop recommendations for actions to address key strategic challenges to identifying and managing risk associated with the global information and communications technology supply chain and related third-party risk. The Task Force is intended to focus on potential near- and long-term solutions to manage strategic risks through policy initiatives and opportunities for innovative public-private partnership.

Secretary Nielsen also discussed DHS’ ongoing commitment to improving the nation’s cybersecurity posture through the timely sharing of actionable cyber threat indicators via the free Automated Information Sharing (AIS) program. DHS has prioritized working with industry to identify improvements to AIS and will roll out an updated platform in the fall with upgraded capabilities to improve our collective defense. These improvements are based on feedback received from industry and will include additional context and improved feedback mechanisms to be more relevant and meaningful to users.

In his closing keynote address, Vice President Pence highlighted the Administration’s focus on cybersecurity and the critical role this summit played in moving forward with these efforts. Vice President Pence also called on the U.S. Senate to enact legislation to create the Cybersecurity and Infrastructure Security Agency before the end of the year.

At the summit, a diverse group of more than twenty CEOs from some of the largest companies in the world and senior-most government officials convened specifically to discuss cybersecurity and critical infrastructure risk management. They were joined by hundreds of others from across a wide range of industries. The Department will continue to lead the federal government’s efforts for an integrated, cross-sector approach to protect our nation’s critical infrastructure from the growing cyber threat.

Watch the DHS National Cybersecurity Summit here: https://www.dhs.gov/national-cybersecurity-summit.

Ready Business Hurricane Toolkit

Many parts of the United States, including Atlantic and Gulf of Mexico coastal areas, Hawaii, parts of the Southwest, Puerto Rico, the Pacific Coast, and the U.S. Virgin Islands and territories in the Pacific may be directly affected by heavy rains, strong winds, wind-driven rain, coastal and inland floods, tornadoes, and coastal storm surges resulting from tropical storms and hurricanes. The Ready Business Hurricane Toolkit helps leaders take action to protect employees and customers, and help ensure business continuity.

The Toolkit outlines how to identify your risk, how to develop a preparedness and mitigation plan, best practices for taking action, and resources for hurricane preparedness. The Toolkit is available in English and in Spanish.

For more business preparedness resources, go to https://www.ready.gov/business.

Federal Emergency Management Agency Releases the 2017 Hurricane After-Action Report

The Federal Emergency Management Agency (FEMA) released the 2017 Hurricane Season FEMA After-Action Report. The report examines the agency's performance during the record breaking season. Last year, hurricanes Harvey, Irma, and Maria devastated the nation at a time when FEMA was already supporting 692 federally declared disasters. During response to the three catastrophic hurricanes, FEMA also responded to the historic wildfires in California. The report captures transformative insights from a historic hurricane season that will help FEMA, the emergency management community, and the nation chart the path into the future. The report identified 18 key findings across five focus areas and offered targeted recommendations for FEMA improvements, as well as broader lessons for partners throughout the emergency management community.

The agency has already taken immediate actions based on the findings from the After-Action Report including updated hurricane plans, annexes, and procedures for states and territories; increased planning factors for the Caribbean and disaster supplies; and updated high priority national-level contracts, including the National Evacuation Contract, Caribbean Transportation Contract, and National Ambulance Contract. FEMA has also tested its response and initial recovery capabilities in the National Level Exercise (NLE) 2018, which occurred in May and focused on areas identified from real-world continuous improvement findings in this report.

Hurricanes Harvey, Irma, and Maria caused a combined $265 billion in damage and each ranked among the top five costliest hurricanes on record. As a result, FEMA coordinated large deployments of federal personnel, both before and after the storms' landfalls, to support response and initial recovery efforts across 270,000 square miles. In total, the hurricanes and wildfires affected more than 47 million people—almost 15 percent of the nation's population. FEMA registered nearly 4.8 million households for assistance.

FEMA has incorporated many of the findings from this report into its 2018-2022 Strategic Plan, which will guide implementation of long-term goals to build a more prepared and resilient nation. For a copy of the full After-Action Report, go to https://www.fema.gov/media-library/assets/documents/167249.

Software and Supply Chain Assurance Fall 2018 Forum

Cyber risk has become a topic of core strategic concern for business and government leaders worldwide and is an essential component of an enterprise risk management strategy. The Software and Supply Chain Assurance Forum (SSCA) provides a venue for government, industry, and academic participants from around the world to share their knowledge and expertise regarding software and supply chain risks, effective practices and mitigation strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved.

The Fall Forum will feature speakers on:

- Multiyear Plan for Energy Cybersecurity with a focus on supply chain vulnerabilities and risks.
- Enhanced Supply Chain Risk Management Reliability Standards (NERC CIP): The Rule, Approach, and Process used for developing the standard.
- Industry experiences with implementing NERC CIP.

The effort is co-led by the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Department of Defense (DoD), and the Government Services Agency (GSA). Participants represent a diverse group of career professionals including government officials, chief information security officers, academics with cybersecurity and supply chain specialties, system administrators, engineers, consultants, vendors, software developers, managers, analysts, IT and cybersecurity specialists, and many more fields.

Additional information about the SSCA Forum and upcoming event will be posted at http://csrc.nist.gov/scrm/ssca/. The event is FREE and open to the public, but registration is required. Registration ends for non-US citizens on September 12, 2018 and for US citizens and green card holders on September 19, 2018.

- **Dates:** September 26-27, 2018
- **Location:** MITRE-1, 7525 Colshire Drive, McLean, VA 22102
- **Registration:** http://www.mitre.org/ssca
- **Agenda:**

For additional information and questions, contact Beatrix.Boyens@hq.dhs.gov.

Region VIII Infrastructure Resilience Conference

Salt Lake County Emergency Management, the Utah Department of Public Safety, and Region VIII of the U.S. Department of Homeland Security (DHS) will sponsor the **2018 Region VIII Infrastructure Resilience Conference in Salt Lake City** on September 12, 2018 for emergency managers, utility owners, first responders, security professionals, and private sector stakeholders. This no-cost, all-day conference will convene national experts from DHS and emergency managers from hurricane-affected counties and states to brief on experiences and best practices. Discussion topics include emergency reentry after disaster planning, cybersecurity recommendations, unmanned aircraft systems (UAS) and counter-UAS best practices and guidance, business emergency operations center lessons learned from 2017 hurricane states, and soft target venues.

- **Date:** Wednesday, September 12, 2018
- **Time:** 8:30 a.m. – 4:30 p.m. MDT
- **Location:** Salt Palace Convention Center, 100 South West Temple, Salt Lake City, UT 84104

- **Registration:** Click here

For additional information, contact dorothy.miller1@hq.dhs.gov.

EARTH EX 2018 Registration Open

One of the largest cross-sector critical lifeline sector exercises in 2018, EARTH EX 2018 provides stakeholders the opportunity to exercise their plans and policies in response to true Black Sky hazards that threaten our modern society in a direct and complex manner. Take the opportunity to learn, share information, and improve plans to become more resilient. EARTH EX is a no-cost, four-hour tabletop exercise over three advancing phases with flexible start times.

- **Date:** Wednesday, August 22, 2018
- **Registration:** Click here

For more information or questions, contact earthex@eiscouncil.org.

Critical Infrastructure Cyber Community Voluntary Program (C3VP) Events, Updates, and Resources

Industrial Control Systems Joint Working Group (ICSJWG) 2018 Fall Meeting

The 2018 Fall ICSJWG Meeting in Cincinnati (OH) will provide a forum for all control systems stakeholders to gather and exchange ideas about critical issues in industrial control systems cybersecurity. This meeting will foster an opportunity for stakeholders to interface with peers, network with industry leaders, and stay abreast of the latest initiatives impacting security for industrial control systems and critical infrastructure. The Fall Meeting will include three full days of interactions and discussions in the form of keynote speakers, practical demonstrations, presentations, and panels. The Vendor Expo will return, as will the popular "Ask Me Anything" session by National Cybersecurity and Communications Integration Center leadership.

- **Date**: August 28-30, 2018
- **Location**: Hilton Cincinnati Netherland Plaza, 35 West 5th Street, Cincinnati, Ohio

Registration is now open. For additional information about the Fall Meeting or the ICSJWG, visit the ICSJWG Webpage or contact ICSJWG.Communications@hq.dhs.gov.

DHS Campus Resilience Program Exercise Starter Kits

The DHS Office of Academic Engagement (OAE) recently released three Exercise Starter Kits for the academic community as part of the Campus Resilience (CR) Program. The CR Program Exercise Starter Kits are a set of tools and resources for institutions of higher education to self-conduct a tabletop exercise. The kits reinforce an institution’s specific emergency plans, protocols, and procedures, while also testing and strengthening an institution’s preparedness, response, and recovery capabilities. The CR Program Exercise Starter Kits are currently available in three scenarios, including Cyber Breach. For more information, please read the press release, one-pager, or visit www.dhs.gov/academicresilience. To request one of the Exercise Starter Kits, please use this link.

Risk Management Process and Facility Security Committee Training

During Phase One of the National Compliance Advisory Initiative, the DHS Interagency Security Committee (ISC) provided awareness training across the country. Now building off of that foundation, Phase Two provides a half day, instructor-led training course covering the Risk Management Process and the roles and responsibilities of the Facility Security Committee. The course is offered at no cost to Federal employees and state and local employees with a Federal sponsor. The training is available on a first-come, first-served basis.

- August 21, 2018 – Lincoln, NE
- September 25, 2018 – Denver, CO
- September 27, 2018 – Laguna Niguel, CA
- October 2, 2018 – National Capitol Region
- October 16, 2018 – San Francisco, CA
- October 18, 2018 – Santa Ana, CA
- December 4, 2018 – Seattle, WA
- December 6, 2018 – Portland, OR

RSVP to ISC@hq.dhs.gov and include name, title, organization, armed/unarmed, and desired training location, with the subject line "ISC-NCAI training."

Chemical Sector Monthly Unclassified Threat Calls

DHS NPPD/IP, serving as the Chemical Sector-Specific Agency, conducts a monthly unclassified threat call in coordination with DHS NPPD Office of Cybersecurity and Communications (CS&C), DHS Office of Intelligence and Analysis (I&A), Office of The Director of Intelligence, Federal Bureau of Investigation (FBI), and more. The call is intended to provide unclassified threat information to chemical sector partners and those in associated sectors. The call is held every fourth Thursday of each month.

- **Dates:** August 23 and September 27
- **Time:** 11:00 a.m. EDT
- **Dial-In:** 1-855-852-7677
- **PIN:** 999998362769
- **Link:** **https://share.dhs.gov/chemthreatcall/**

For more information about the Chemical Sector Monthly Classified Threat Call contact chemssa@hq.dhs.gov.

Corporate Security Symposia Dates

The DHS I&A Private Sector Outreach Program, in coordination with FBI, hosts regional Corporate Security Symposia around the country to discuss and inform public and private sector audiences on the most challenging security issues our Nation faces today.

The Corporate Security Symposia focus on topics that are critical to security within the public and private sectors. Events feature public and private subject matter experts (SMEs), who provide insight on a variety of issues such as cybersecurity, infrastructure protection, communications, global intelligence, border security, and counterintelligence. Several Fortune 500 companies, including Sony, the Walt Disney Company, Gulfstream, and Microsoft, have hosted past Corporate Security Symposia.

Region IV

- Nashville, TN, Thursday, August 23 Register Here

To register or for more information please contact I&APrivateSector@hq.dhs.gov.

Training/Resources

DHS offers a wide array of training programs and resources, at no cost, to government and private sector partners. Web-based training, classroom courses, and associated training materials provide government officials and critical infrastructure owners and operators with the knowledge and skills needed to implement critical infrastructure security and resilience activities. For further information, visit the DHS Critical Infrastructure Training website or the Critical Infrastructure Resources website.

Active Shooter Program Resources

NPPD/IP's Active Shooter Preparedness Program remains committed to developing resources that help the critical infrastructure community mitigate the potential impacts associated with the evolving threat environment. Visit the Active Shooter Preparedness webpage to access a variety of new products ranging from an active shooter preparedness fact sheet and Pathway to Violence informational poster to translated materials.

More Active Shooter Preparedness Resources:

- **Recovering From An Active Shooter Incident Fact Sheet:** provides high level considerations for the short and long-term phases of recovery following an incident.
- **Active Shooter Recovery Guide:** provides detailed information on actions organizations should consider to reconstitute services more effectively and ensure the wellness of their employees and visitors.
- **Active Shooter Emergency Action Plan Video**: A great resource for individuals unable to attend an in-person workshop or those who would like a refresher. This dynamic 90-minute video describes the fundamental concepts of developing an emergency action plan for an active shooter scenario by leveraging the perspectives of survivors, first responders, and SMEs.
- **Active Shooter Emergency Action Plan Trailer**: This one-minute video provides a brief overview of the components of the Active Shooter Emergency Action Plan video.
- **Options for Consideration**: Replacing the previously available resource, this seven minute video demonstrates possible actions individuals can take if confronted with an active shooter; it provides updated information that includes considerations for individuals with disabilities and incorporation of technology into security practices.

Additional Resources

- A recently developed Vehicle Ramming Attack Mitigation video provides information to assist with mitigating the evolving threat corresponding to vehicle ramming incidents with insightful technical analysis from public and private sector SMEs. It leverages real-world events and provides recommendations aimed at protecting organizations and individuals against a potential vehicle ramming incident.
- **Understanding the Insider Threat Video:** uses security and behavior experts to discuss how insider threats manifest in a variety of ways including terrorism, workplace violence, and breaches of cybersecurity.
- **Unmanned Aircraft Systems (UAS) Video:** contains information on critical infrastructure challenges associated with the UAS threat, counter UAS security practices, actions to consider for risk mitigation, and provides messages of facility and organizational preparedness related to UAS incidents

For questions, please contact ASworkshop@hq.dhs.gov.

Active Shooter Preparedness Workshop Dates

Active Shooter Preparedness Workshops are conducted across the Nation to provide participants with information that helps mitigate the impacts of an active shooter incident. These workshops—which include case studies, visual media content, and facilitated dialogue in breakout sessions—allow participants to begin developing an emergency action plan for their respective organizations.

Below is the tentative schedule of upcoming workshops. For additional information regarding the upcoming schedule, please contact ASworkshop@hq.dhs.gov.

Region I

- Augusta, ME, Wednesday, August 22

Region II

- Atlantic City, NJ, Monday, October 15
- New York City, NY, Wednesday, October 17
- White Plains, NY, Friday, October 19

Region V

- Bloomington, MN, Monday, August 20
- Detroit, MI, Tuesday, September 11

Region VI

- Camden, AR, Tuesday, August 28
- Oklahoma City, OK, Thursday, August 30

Region VII

- Wichita, KS, Wednesday, September 5

Region VIII

- Saint Michael, ND, Tuesday, October 2

- Denver, CO, Thursday, October 4
- Westminster, CO, Thursday, October 4

Region IX

- Las Vegas, NV, Thursday, September 13
- Phoenix, AZ, Wednesday, November 7

Region X

- University Place, WA, Thursday, September 27

Office for Bombing Prevention Training Courses

Independent Studies:

These web-based courses are self-paced and designed for a broad audience to provide general awareness-level, counter-improvised explosive device (IED) information to general public and private sector partners to enhance awareness and response to IED threats. They are offered free-of-charge.

Homemade Explosives and Precursor Chemicals Awareness for Public Safety (AWR-349)

This one-hour, awareness-level, computer-based course, available through TRIPwire, educates law enforcement, firefighters, emergency medical technicians, and other public safety personnel about homemade explosives (HME), the precursor chemicals that are used to manufacture HME, and actions to take if HME precursor chemicals or equipment are thought to be present during a routine service call.

Improvised Explosive Device Awareness and Safety Procedures (AWR-341)

This one-hour, awareness-level, computer-based course, available on TRIPwire, provides foundational knowledge concerning IED and proper safety precautions and procedures for reacting and responding to unattended and suspicious items.

Direct Delivery In-Person Training:

Coordinated through DHS Protective Security Advisors (PSA), State Homeland Security Officials, and training offices, Office of Bombing Prevention courses educate Federal, state, local, tribal, and territorial participants—such as municipal officials and emergency managers, state and local law enforcement and other emergency services, critical infrastructure owners and operators, and security staff—on strategies to prevent, protect against, respond to, and mitigate bombing incidents. Unless otherwise indicated, all courses are instructor-led and designed for small groups of 25 participants.

Bombing Prevention Awareness Course (AWR-348)

This one-day awareness course provides an overview of bombing prevention topics. Course topics include IED and HME awareness, explosive effects mitigation, protective measures awareness, suspicious behaviors and items, and an introduction to the terrorist attack cycle for bombing events. This course is designed for public and private sector critical infrastructure owners and operators interested in or required to have a basic awareness of bombing prevention measures, public safety personnel, emergency managers, law enforcement, and special event security personnel can also benefit from the course. Upcoming scheduled courses are as follows:

Region IV

Anniston, AL – Michael Aguilar, 866-213-9547

- Monday, September 10
- Thursday, September 13

Region X

Boise, ID – Eric Puype, eric.puype@hq.dhs.gov

- Wednesday, August 29

IED Search Procedures Course (PER-339)

This one-day, performance-based course introduces participants to basic, low-risk search protocols and allows participants to practice an IED search of a facility, an area, and a route in order to reduce vulnerability and mitigate the effects of IED attacks. This course is designed for public and private facility owners and operators and security staff that may be tasked with search duties during a bomb threat incident.

Region III

Pittsburgh, PA – Robert E. Winters, Robert.e.winters@hq.dhs.gov

- Friday, September 9

Region IV

Mobile, AL – Kirk Toth, kirk.toth@hq.dhs.gov

- Wednesday, September 26

Bomb Threat Management Planning Course (MGT-451)

This one-day, management-level course introduces participants to the DHS risk management process and the development of a bomb threat management (BTM) plan. During the course, participants will learn how to apply specific portions of the risk management process and BTM procedures against mock BTM plans. This course is designed for public and private sector emergency management representatives, critical infrastructure owners and operators, and law enforcement officials.

Region II

Mahwah, NJ – Andrew Smith, Andrew.smith@hq.dhs.gov

- Thursday, September 13

Region III

Pittsburgh, PA – Robert E. Winters, Robert.e.winters@hq.dhs.gov

- Thursday, September 6

Region IV

Anniston AL – Michael Aguilar, 866-213-9547

- Monday, September 24

Mobile, AL – Kirk Toth, kirk.toth@hq.dhs.gov

- Tuesday, September 25

Protective Measures Course (PER-336)

This one-day, performance-based course provides participants with a basic understanding of how to identify risks and vulnerabilities to a facility, determine additional security needs for a special event or public gathering, and identify and apply physical and procedural protective measures to mitigate the threat of an IED or vehicle-borne IED (VBIED). This course is designed for public and private sector security personnel at the executive, management, and operations level. Public safety workers, emergency managers, law enforcement, and special event security personnel can also benefit from the course. Upcoming scheduled courses are as follows:

Region II

Mahwah, NJ – Andrew Smith, andrew.smith@hq.dhs.gov

- Wednesday, September 12

Region III

Pittsburg, PA – Robert E. Winters, robert.e.winters@hq.dhs.gov

- Wednesday, September 5

Region IV

Anniston, AL – Michael Aguilar, 866-213-9547

- Thursday, September 13
- Monday, September 17
- Monday, September 24

Mobile, AL – Kirk Toth, kirk.toth@hq.dhs.gov

- Thursday, September 27

Region X

Boise, ID – Eric Puype, eric.puype@hq.dhs.gov

- Tuesday, August 28

Surveillance Detection for Law Enforcement and Security Professionals (PER-346)

This three-day, performance-based course provides instruction on how to detect hostile surveillance by exploring surveillance techniques, tactics, and procedures from an adversary's perspective. These skills enhance counter-IED capabilities of law enforcement and security professionals to detect, prevent, protect against, and respond to IED threats. This course incorporates multiple hands-on exercises and culminates in a field exercise that includes role players. This course is designed for law enforcement and public and private sector security staff. Upcoming scheduled courses are as follows:

Region II

Trenton, NJ – Andrew Smith, andrew.smith@hq.dhs.gov

- Tuesday, September 18

Region IV

Birmingham, AL – Greg Carden, greg.carden@hq.dhs.gov

- Wednesday, September 5

Huntsville, AL – Greg Carden, greg.carden@hq.dhs.gov

- Tuesday, September 18

Louisville, KY – Greg Carden, greg.carden@hq.dhs.gov

- Tuesday, September 25

Region V

West Allis, WI – John Busch, john.busch@hq.dhs.gov

- Wednesday, September 12

Region VI

Rockwall, TX – Jeff Murray, Jeffrey.murray@hq.dhs.gov

- Tuesday, August 28

Vehicle-Borne Improvised Explosive Device (VBIED) Detection Course (PER-312)

This one-day, performance-based course provides participants with the knowledge and skills to recognize the VBIED threat and identify VBIED components and devices, methods for reacting to improvised explosive devices, and procedures for inspecting vehicles to detect VBIEDs. This course is designed for first responders, public safety officers, security officers, and law enforcement officers tasked with inspecting vehicles for explosive threats, hazards, or prohibited items.

Region X

Boise, ID – Eric Puype, eric.puype@hq.dhs.gov

- Thursday, August 30

Virtual Instructor Led Training (VILT):

These web-based courses provide general awareness-level, counter-IED information to a broad audience via an online virtual training experience with a live instructor, using Adobe Connect through the Homeland Security Information Network. These courses are designed for small group instruction of 15 to 25 participants.

A FEMA Student ID (FEMA SID) is required to participate in all VILT OBP course offerings. To obtain a FEMA SID, visit FEMA's website to apply. To view the VILT training schedule and register for a course, please visit the VILT website.

Homemade Explosive (HME) and Precursor Awareness (AWR-338)

This one-hour awareness course provides a basic understanding on HMEs and common precursor materials. Participants will define HMEs, explain the considerations perpetrators have when evaluating whether or not to use HMEs as the explosive for an attack, and identify common precursor chemicals and materials used to make HMEs. This course is designed for public and private sector individuals who are interested in or required to have a basic awareness of homemade explosives and precursor chemicals. Upcoming scheduled courses are as follows:

- Wednesday, August 22, 2018
- Thursday, August 30, 2018
- Wednesday, September 5, 2018
- Wednesday, September 12, 2018
- Tuesday, September 18, 2018
- Thursday, September 20, 2018
- Wednesday, September 26, 2018
- Thursday, September 27, 2018

Improvised Explosive Device (IED) Construction and Classification Course (AWR-333)

This one-hour awareness course provides participants with a basic understanding of the function, components, construction, and classification of IEDs. It is designed for public and private sector individuals who are interested in or required to have a basic awareness of IED construction and classification. Upcoming scheduled courses are as follows:

- Tuesday, August 21, 2018
- Wednesday, August 22, 2018
- Thursday, August 23, 2018
- Tuesday, August 28, 2018
- Thursday, August 30, 2018
- Wednesday, September 5, 2018
- Thursday, September 6, 2018
- Tuesday, September 11 2018
- Thursday, September 13, 2018
- Wednesday, September 19, 2018
- Tuesday, September 25, 2018

- Thursday, September 27, 2018

Improvised Explosive Device (IED) Explosive Effects Mitigation Course (AWR-337)

This one-hour awareness course introduces participants to the effects of detonations and details the difference between blast, thermal/incendiary, and fragmentation effects and the destructive consequences of each on various targets. It also describes security measures and best practices that can help prevent or mitigate explosive effects. This course is designed for public and private sector individuals who are interested in or required to have a basic awareness of how to mitigate the explosive effects of IEDs. Upcoming scheduled courses are as follows:

- Tuesday, August 21, 2018
- Thursday, August 23, 2018
- Wednesday, August 29, 2018
- Tuesday, September 4, 2018
- Tuesday, September 11, 2018
- Thursday, September 13, 2018
- Wednesday, September 19, 2018
- Thursday, September 20, 2018
- Wednesday, September 26, 2018

Introduction to the Terrorist Attack Cycle Course (AWR-334)

This one-hour awareness course introduces a conceptual model of common steps that terrorists take in planning and executing terrorist attacks. It enhances participants' awareness and capability to prevent, protect against, respond to, and mitigate attacks that use IEDs against people, critical infrastructure, and other soft targets. This course is designed for public and private sector individuals who have a responsibility for critical infrastructure protection and those who are interested in or required to have a basic awareness of terrorist operations and bomb prevention. Upcoming scheduled courses are as follows:

- Wednesday, August 29, 2018
- Tuesday, September 4, 2018
- Thursday, September 6, 2018
- Wednesday, September 12, 2018
- Tuesday, September 18, 2018
- Thursday, September 20, 2018
- Wednesday, September 26, 2018

Response to Suspicious Behaviors and Items Course (AWR-335)

This one-hour awareness course serves as an overview of appropriate responses to suspicious behaviors and items by differentiating normal and abnormal behaviors and highlighting appropriate responses to potential terrorist or criminal activity. It also discusses the differences between unattended and suspicious items, and the responses for each situation. This course is designed for managers and employees of stores that sell homemade explosive precursors, facility managers, public and private sector emergency management representatives, security professionals, and law enforcement. Upcoming scheduled courses are as follows:

- Wednesday, August 22, 2018
- Tuesday, August 28, 2018
- Thursday, August 30, 2018
- Wednesday, September 5, 2018
- Thursday, September 13, 2018

- Tuesday, September 25, 2018

Physical and Cybersecurity for Critical Infrastructure Training Course

The Texas A&M Engineering Extension Service (TEEX) is offering a course for practitioners managing physical and cybersecurity. The course is the result of a partnership between TEEX, NPPD IP, NPPD Office of Cybersecurity and Communications, and the FEMA National Training and Education Division. The course, MGT 452 – Physical and Cybersecurity for Critical Infrastructure, encourages collaborative efforts among individuals and organizations responsible for both physical and cybersecurity toward development of integrated risk management strategies that lead to enhanced capabilities necessary for the protection of our Nation’s critical infrastructure.

Participants will identify physical and cybersecurity concerns impacting overall infrastructure security posture, examine integrated physical and cybersecurity incidents and the evolving risks and impacts they pose to critical infrastructure, and explore resources that can be applied to improve security within an organization, business, or government entity. The target audience is critical infrastructure owners and operators and individuals responsible for physical and/or cybersecurity within their organization, including Federal, State, local, regional, tribal, and territorial government officials, and owners and operators of small businesses and nonprofit organizations. This instructor-led course is eight hours in length and offers 0.8 continuing education units. For more information, contact nerrtc@teex.tamu.edu.

Register Today!

Region V

- Oak Forest, IL, Wednesday, October 11, 2018

Missed the last one? Read the July 27, 2018 issue.

Privacy Policy

GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.

Please do not reply to this message. This message originates from a mail delivery service and the account is unattended for replies/responses.

Subscriber Preferences | Unsubscribe

Homeland Security

U.S. Department of Homeland Security · Washington, DC 20528 · 800-439-1420