Homeland Security

The Partnership Bulletin

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

October 1, 2018 **Volume 4, Issue 13**

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

National Cyber Strategy Released

NATIONAL CYBER STRATEGY

of the United States of America

SEPTEMBER 2018

The critical infrastructure that Americans rely on is threatened every day by nation-states, cyber criminals and hackers seeking to wreak havoc, disrupt commerce, and even undermine our democratic institutions. The National Cyber Strategy—the first in fifteen years—strengthens the government's commitment to work in partnership with industry to combat those threats and secure our critical infrastructure.

The National Cyber Strategy, along with the U.S. Department of Homeland Security (DHS) Cybersecurity Strategy released in early 2018, will guide the department's cybersecurity activities in a number of areas, including securing federal networks and information systems, managing risk to the nation's critical infrastructure, and combatting cybercrime. With respect to securing federal networks, for example, DHS has used its authorities to ensure agencies are updating and patching systems, strengthening their email security, and removing Kaspersky antivirus products from their systems. To strengthen critical infrastructure security and resilience, DHS works across government and industry to share timely and actionable information as well as provide training and incident response support. Working with the private sector, the department's newly launched National Risk Management Center is working collaboratively to break down silos, identify and prioritize national critical functions, provide a more holistic picture of the risk environment within and across sectors, and develop joint solutions to manage risk.

The new strategy also identifies several important steps that will further enable DHS to successfully combat cybercrime. Transnational criminal groups are employing increasingly sophisticated digital tools and techniques to enable their illegal activities online, and the strategy calls for DHS and the broader law enforcement community to continue to develop new and more effective legal tools to investigate and prosecute these criminal actors. It also notes the need for electronic surveillance and computer crime laws to be updated to keep pace with the rapidly evolving environment.

Cybersecurity is a shared responsibility, and DHS will continue to stand with its partners, in government and industry, to raise the collective defense against cyber threats to the Nation's security, prosperity, and way of life.

To read the National Cyber Strategy, go to https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

2018 Joint National Priorities Released

DHS Secretary Kirstjen M. Nielsen recently signed off on the 2018 Joint National Priorities (JNPs)—a critical infrastructure protection doctrine developed jointly by government and industry intended to guide the strategic focus of the public-private critical infrastructure partnership outlined in the National Infrastructure Protection Plan (NIPP). The JNPs were developed with industry and government, and the themes they encapsulate reinforce the collective defense model DHS and its National Risk Management Center (NRMC) are looking to promote.

New priorities include reducing risk to national critical functions in addressing risks and corrective actions at a system-wide level, as well as the increased interconnectedness of critical infrastructure systems and resources to ensure that critical operations can be executed, even in the face of evolving threats. The new priorities will also improve efforts to leverage partnerships and evaluate how partnerships and sharing agreements can be used to bolster operational capabilities.

The collaborative, cross-sector efforts of the critical infrastructure community have yielded many accomplishments and success stories during the past four years. These success stories highlight the importance of these various activities and the updated Priorities emphasize the importance of building on those advances to continue improving the security and resilience of the Nation’s critical infrastructure in the face of a complex risk environment.

For more information on the 2018 JNPs, please visit www.dhs.gov/publication/joint-national-priorities.

October is National Cybersecurity Awareness Month

October is the 15th annual National Cybersecurity Awareness Month (NCSAM), a time when Americans are encouraged to reflect on their personal use of the internet and smart phone behaviors. In addition, it is a time when DHS stresses the importance of cybersecurity and ensures collaboration with partners at all levels to manage cyber risks that may affect a single infrastructure asset or impact multiple interconnected resources. Securing the Internet is a shared responsibility. Visit Stay Safe Online and view this infographic to learn how to get involved in NCSAM.

NCSAM will be broken down into weekly cybersecurity themes:

- Week 1: Oct. 1-5, Make your Home a Haven for Online Safety
- Week 2: Oct. 8-12, Millions of Rewarding Jobs: Educating for a Career in Cybersecurity
- Week 3: Oct. 15-19, It’s Everyone’s Job to Ensure Online Safety at Work
- Week 4: Oct. 22-26, Safeguarding the Nation’s Critical Infrastructure

In addition, DHS will be promoting four key messages throughout the month:

- Strengthen the Nation’s Cybersecurity Ecosystem
- Cybersecurity is a Cross-Cutting, Cross-Sector Challenge, So We Must Tackle It Together
- Increase and Strengthen the Cybersecurity Workforce Across All Sectors
- Secure Critical Infrastructure from Cyber Threats

Participate throughout the month in live events and on social media:

- Use the #CyberAware hashtag.
- View live segments with experts each week on Facebook, and follow Twitter for the latest news and resources.
- Join the #ChatSTC Twitter chat each Thursday in October at 3:00 p.m. ET.

Organizations can register as a Champion to take action in support of NCSAM. Sign up on https://staysafeonline.org/ncsam/.

2018 National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge Update

In July 2018, the DHS National Protection and Programs Directorate (NPPD), NRMC, announced this year’s NIPP Security and Resilience Challenge, in partnership with the National Institute for Hometown Security (NIHS). The goal of the Challenge is to fill gaps in risk management, resilience, and cyber and physical security, and has the unique capability to identify and enable funding opportunities to ready or near-ready-for-use initiatives. This is the third year that the Office of Infrastructure Protection has managed the Challenge, and this year's Challenge includes $2.5 million in funding.

This summer, NIHS and DHS received 35 Challenge submissions that spanned all critical infrastructure sectors and geographic regions. From those 35, an independent review panel of Federal and industry experts selected 10 projects to proceed to a contract negotiation stage. Each of these submissions proposed solutions that would fill specific critical infrastructure security and resilience capability gaps, continuing to build on the successes of previous Challenge projects. NIHS is in the process of notifying submitters of their status, and it will negotiate subsequent contracts. Submissions not selected for advancement are catalogued for possible future funding opportunities.

In November 2018, NPPD/NRMC plans to host a full day briefing from both the awardees from the FY17 Challenge and the selected FY18 Challenge submissions where presenters will share updates on their projects.

A factsheet is available for a summary of selected documents.

National Terrorism Advisory Bulletin Reissue

DHS Secretary Kirstjen M. Nielsen reissued the National Terrorism Advisory System (NTAS) Bulletin on September 14, 2018. After carefully considering the current threat environment, as well as input from the Department's intelligence and law enforcement partners, Secretary Nielsen determined it is necessary to extend the NTAS Bulletin at this time.

Terrorist groups continue to inspire, enable and direct their followers to spread chaos using homemade weapons and by striking soft targets and crowded places. They also remain focused on conducting more sophisticated attacks using conventional weapons as well as new technologies and tactics. DHS is committed to staying a step ahead of our enemies, and an informed and vigilant public remains one of the Department's greatest assets in protecting the homeland.

This marks the seventh iteration of the Bulletin on the homegrown terrorism threat since the first Bulletin was released in December 2015.

You can read the new NTAS Bulletin here.

New Electronic Submission Portal for Protected Critical Infrastructure Information

DHS recently released a Protected Critical Infrastructure Information (PCII) electronic submissions (e-Subs) portal. The e-Subs portal allows a private owner/operator or a state, local, tribal, or territorial (SLTT) government official to voluntarily share critical infrastructure information with the Federal government for homeland security purposes.

Each step of the submission process is designed with clear instructions and guidance to walk users through the submission process. A key requirement is to submit information with an Express and Certification (E&C) statement. These documents "express" that the information is voluntarily submitted to the Federal government in expectation of protection from disclosure in accordance with the Critical Infrastructure Information (CII) Act of 2002 and “certify” the information is not customarily in the public domain. Once the questions are answered and the critical infrastructure information and the E&C statements are uploaded, the PCII Program Office starts the validation process. Government employees sponsoring a submission must ensure that the owner/operator provided an E&C statement prior to accessing the e-Subs webpage.

Upon submission, the CII automatically receives not only the legal protection as provisioned in the CII Act, but also information security while in the validation process. If validated as PCII, the information is marked and securely stored by DHS. If not validated as PCII, the submission is returned to the submitter or, if requested, destroyed.

Access the PCII e-Subs portal by going to http://pciims.dhs.gov/eSubmissions/.

Interested entities can inquire about e-Subs, submission format, and request additional information by contacting the PCII Program Office at PCII-Assist@hq.dhs.gov or by going to the PCII e-Subs information website.

Presentations Now Available: 2018 DHSChemSecurityTalks

Presentations from the 2018 DHSChemSecurityTalks EAST, MID, and WEST events held in Philadelphia, PA; Chicago, IL; and Oakland, CA are now available. If you missed the events, you can still learn about the Chemical Facility Anti-Terrorism Program (CFATS), how to take a holistic approach to facility security plans, and the voluntary and regulatory resources available for owners, operators, and stakeholders.

For more information on events or any questions, contact DHSChemSecurityTalks@hq.dhs.gov.

Phishing: Don't Be Phooled! Resources

DHS and the Office of the Director of National Intelligence, as part of their Public-Private Analytic Exchange Program, produced and released a white paper and fact sheet on phishing. The documents were created for the Healthcare and Public Health Sector, but the vast majority of the information is applicable to other sectors as well. The white paper goes into detail about what phishing is, what techniques are used, and how to mitigate phishing attacks. The fact sheet is a collection of tips and best practices for organizations to prevent phishing attacks.

Access the white paper here and the fact sheet here.

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

Awareness Briefing Recording: Combating Ransomware

The recording of the June 2018 Awareness Briefing on Combating Ransomware is now live.

In the last few years, organizations around the world have lost tens of millions of dollars to ransomware – a type of malware that threatens to publish, destroy, or perpetually block access to a victim's data it unless a ransom is paid.

In light of this threat, DHS hosted an awareness briefing to help organizations understand and combat ransomware. Panelists from the NCCIC and the Multi-State Information Sharing and Analysis Center (MS-ISAC) discussed recent malware variants, emerging trends, incident response tips, and best practices to help protect organizations from being compromised.

View information on all past webinars here: https://www.us-cert.gov/ccubedvp/past-events.

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.

- October 15, 2018 – Oakland, CA
- 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."

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 II

- New York, NY, Tuesday, October 16, 2018, Register Here

Region III

- Norfolk, VA, Wednesday, April 3, 2019

Region IV

- Louisville, KY, Thursday, November 1, 2018, Register Here

- Biloxi, MS, Wednesday, March 20, 2019

Region VI

- Bentonville, AR, Wednesday, August 14, 2019

Region IX

- Los Angeles, CA, Thursday, December 6, 2018, 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 II

- Atlantic City, NJ, Monday, October 15
- New York City, NY, Wednesday, October 16
- White Plains, NY, Friday, October 19

Region VIII

- Rapid City, SD, November 13

Region IX

- Phoenix, AZ, Wednesday, November 7

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 II

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

- Tuesday, October 30

Region III

Springfield, VA – Kyle Wolf, kyle.wolf@hq.dhs.gov

- Wednesday, October 17

Region IV

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

- Monday, October 15
- Monday, October 22
- Thursday, November 8

Research Triangle Park, NC – Robert Mielish, Robert.Mielish@hq.dhs.gov

- Wednesday, November 14

Region VII

Mayetta, KS – Charles Clanahan, charles.clanahan@hq.dhs.gov

- Wednesday, October 10

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. Upcoming scheduled courses are as follows:

Region II

New York, NY – Kevin Peterson, kevin.peterson@hq.dhs.gov

- Tuesday, November 13

Region III

Philadelphia, PA – Richard Turzanski, Richard.Turzanski@hq.dhs.gov

- Sunday, November 18

Region V

Indianapolis, IN – Christopher Judge, christopher.judge@hq.dhs.gov

- Tuesday, October 30
- Thursday, November 1

Evansville, IN – Christopher Judge, christopher.judge@hq.dhs.gov

- Monday, November 5
- Wednesday, November 7

Region VII

Mayetta, KS – Charles Clanahan, charles.clanahan@hq.dhs.gov

- Friday, October 12

Region X

Tacoma, WV – Jonathan Richeson, jonathan.richeson@hq.dhs.gov

- Tuesday, October 16

Seattle, WA – Jonathan Richeson, jonathan.richeson@hq.dhs.gov

- Thursday, October 18

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. Upcoming scheduled courses are as follows:

Region III

Philadelphia, PA - Richard.Turzanski@hq.dhs.gov

- Tuesday, November 6

Region IV

Research Triangle Park, NC – Robert Mielish, Robert.Mielish@hq.dhs.gov

- Tuesday, November 13

Region VII

Mayetta, KS – Charles Clanahan, charles.clanahan@hq.dhs.gov

- Thursday, October 11

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 III

Rockville, MD – Kyle Wolf, kyle.wolf@hq.dhs.gov

- Tuesday, October 16

Region IV

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

- Wednesday, October 17
- Monday, October 29
- Monday, November 5

Research Triangle Park – Robert Mielish, Robert.Mielish@hq.dhs.gov

- Thursday, November 15

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

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

- Tuesday, October 23

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

- Tuesday, November 13

Region X

Tacoma, WA – Jonathan Richeson, jonathan.richeson@hq.dhs.gov

- Thursday, October 11

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. Upcoming scheduled courses are as follows:

Region II

Westhampton, NJ – Andrew Smith, Andrew.Smith@hq.dhs.gov

- Friday, November 2

West Point, NY – Michael Gray, mgray@usmint.treas.gov

- Tuesday, November 6
- Thursday, November 8

- Saturday, November 10

Region III

Philadelphia, PA – Richard Turzanski, Richard.Turzanski@hq.dhs.gov

- Wednesday, November 7

Region V

Indianapolis, IN – Christopher Judge, christopher.judge@hq.dhs.gov

- Wednesday, October 31
- Friday, November 2

Evansville, IN – Christopher Judge, christopher.judge@hq.dhs.gov

- Tuesday, November 6
- Thursday, November 8

Region X

Tacoma, WA – Jonathan Richeson, jonathan.richeson@hq.dhs.gov

- Monday, October 15

Seattle, WA – Jonathan Richeson, jonathan.richeson@hq.dhs.gov

- Wednesday, October 17

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:

- Thursday, October 11, 2018
- Tuesday, October 16, 2018

- Thursday, October 18, 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:

- Wednesday, October 10, 2018
- Wednesday, October 17, 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, October 9, 2018
- Wednesday, October 17, 2018
- Thursday, October 18, 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, October 10, 2018
- Thursday, October 11, 2018
- Tuesday, October 16, 2018

Protective Measures Awareness (AWR-340)

This one hour course introduces participants to identifying and filling facility security gaps. It provides a basic understanding on risks, risk management, and the three rings of security: physical protective measures, procedural/technical protective measures, and intelligence protective measures. Upcoming scheduled courses are as follows:

- Tuesday, October 9
- Monday, October 10
- Monday, October 17
- Sunday, October 23
- Wednesday, October 24
- Wednesday, October 31
- Tuesday, November 6

- Wednesday, November 7

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:

- Tuesday, October 9, 2018
- Thursday, October 11, 2018
- Tuesday, October 16, 2018
- Thursday, October 18, 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 IV

- North Charleston, SC, Thursday, November 15, 2018

Region V

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

Missed the last one? Read the September 14, 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