The Partnership Bulletin

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

September 14, 2018 **Volume 4, Issue 12**

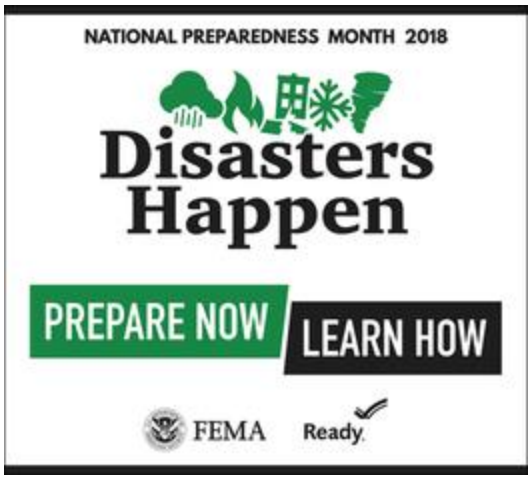
The Partnership Bulletin, designed for widest distribution, provides a snapshot of upcoming training and exercise opportunities, critical infrastructure events, and key announcements. To receive this Bulletin directly or to share upcoming events or articles, please send your request or submission to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

- September is National Preparedness Month
- Get Ready: October is National Cybersecurity Awareness Month
- National Terrorism Advisory System Bulletin Reissue
- Cyber Community Joint Council Webinar Series
- 2019 Public-Private Analytic Exchange Program Participant Application Information
- New Electronic Submission Portal for Protected Critical Infrastructure Information
- Presentations Now Available: 2018 DHSChemSecurityTalks
- New DHS Ammonia (Anhydrous) Flyer
- Phishing: Don't Be Phooled! Resources
- New Insider Threat Mitigation Website
- Critical Infrastructure Cyber Community Voluntary Program (C3VP) Events, Updates, and Resources
- Risk Management Process and Facility Security Committee Training
- Chemical Sector Monthly Unclassified Threat Calls
- Corporate Security Symposia Dates
- Training/Resources

September is National Preparedness Month



"Disasters Happen. Prepare Now. Learn How." That is the theme this September for National Preparedness Month, an opportunity to remind families, friends, and communities to get ready for disasters and emergencies before they strike. Thinking ahead can save lives, so DHS is working to create a "culture of preparedness" nationwide that requires all Americans to prioritize preparedness efforts in their daily lives. Take the time to evaluate your preparedness and learn how to protect your family so that if disaster strikes, you are ready.

National Preparedness Month is divided into four weeks. Each week DHS will publish recommended steps you can take to ensure you are prepared:

- Week 1: Sept. 1-8, Make and Practice Your Plan
- Week 2: Sept. 9-15, Learn Life Saving Skills
- Week 3: Sept. 16-22, Check Your Insurance Coverage
- Week 4: Sept. 23-29, Save For an Emergency

There are a number of resources available to help you implement the steps recommended for each week of National Preparedness Month. You can begin to boost your level of preparedness by taking small steps, such as discussing an emergency communications plan with your family over dinner, installing carbon monoxide detectors, reviewing your insurance coverage, or starting an emergency savings fund. To prepare, you can:

- Make a Family Emergency Communication Plan: Have all members of your household keep a fillable plan card in their wallet, purse or backpack.
- Get to know your neighbors: check with each other before and after a disaster and include neighbors in your emergency plan.
- Sign up for emergency alerts to receive life-saving information from your state and local officials.
- Learn your evacuation zone and have an evacuation plan.
- Have regular household meetings to review and practice your plan.

In addition to utilizing these resources, consider taking part in the National Day of Action on September 15th. This is an opportunity for individuals, organizations, and businesses to take an action, such as learning a life-saving skill or participating in an exercise or drill, to increase preparedness. Visit www.ready.gov/september for more information and resources. And if you have the ability to help others, please consider joining a Community Emergency Response Team (CERT).

With these resources and training, you can be a lifeline for your family and fellow citizens.

Get Ready: October is National Cybersecurity Awareness Month

Securing the internet is a shared responsibility. Visit Stay Safe Online and view this infographic to learn how to get involved in National Cybersecurity Awareness Month (NCSAM) this October.

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/.

National Terrorism Advisory System Bulletin Reissue

Secretary of Homeland Security Kirstjen M. Nielsen reissued the National Terrorism Advisory System (NTAS) Bulletin on September 14, 2018 pertaining to the terror threat to the U.S. homeland. 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.

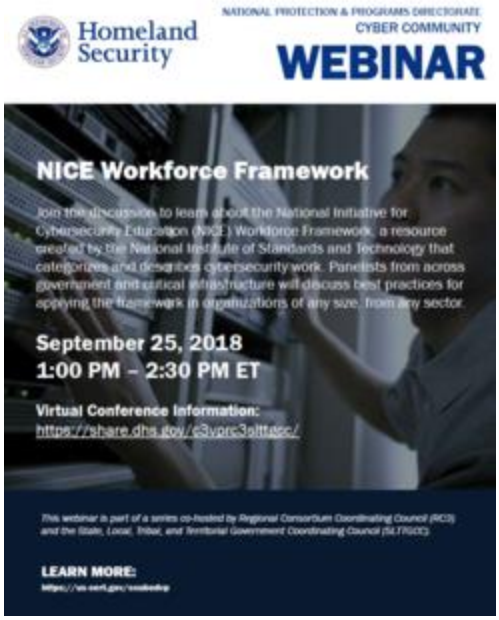
Cyber Community Joint Council Webinar Series

On September 25, join DHS for the next webinar in its series with the Regional Consortium Coordinating Council and the State, Local, Tribal, and Territorial Government Coordinating Council—this time spotlighting the National Initiative for Cybersecurity Education (NICE) Workforce Framework, a resource created by the National Institute of Standards and Technology (NIST) that categorizes and describes cybersecurity work.

Experts from DHS and NIST will provide background on the NICE Workforce Framework, as well as suggest best practices and resources to help attendees use the Workforce Framework within their own organizations.

- **Date:** September 25, 2018
- **Time:** 1:00 p.m–2:30 p.m. ET
- **Link:** https://share.dhs.gov/c3vprc3slttgcc/

Registration information is forthcoming and will be posted online. View the event flyer here. For more information or questions, contact CCubedVP@hq.dhs.gov.



2019 Public-Private Analytic Exchange Program Participant Application Information

DHS and the Office of the Director of National Intelligence invite analysts who are U.S. citizens to apply for the 2019 Public-Private Analytic Exchange Program (AEP). Applicants from all industries are encouraged to apply, but should have an interest and/or demonstrated expertise in at least one of the 2019 topics detailed below. Applicants are welcome to express an interest in **up to three** of the 2019 topics, but each selected program participant will only be assigned to one team. Applications from first-time participants will be given priority consideration over previous AEP participants. Selected applicants will be notified of their selection in November 2018 and will be expected to attend a kick-off meeting in Washington, D.C. on January 24, 2019.

About the Program:

AEP enables intelligence community analysts and private sector partners to gain a greater understanding of how their disparate, yet complementary, roles can work in tandem to ensure mission success. Participants work on topic-focused teams over six months to create joint analytic products of interest to both the private sector and the U.S. Government. The program begins with a kick-off event in January 2019 and concludes with a summit in July 2019.

The 2019 AEP program topic areas are:

- Best Practices in Vetting Prospective and Current Employees
- Combatting Targeted Disinformation Campaigns
- Counterterrorism Futures
- E-Commerce: Illicit Use of Reshipping Services
- Geopolitical Impact on Cyber Threats from Nation-State Actors
- Identifying Risks to Vehicle Technology Advancements
- Industrial Internet of Things Interconnections

- Strategies to Address Physical Supply Chain Risks

Application Information:

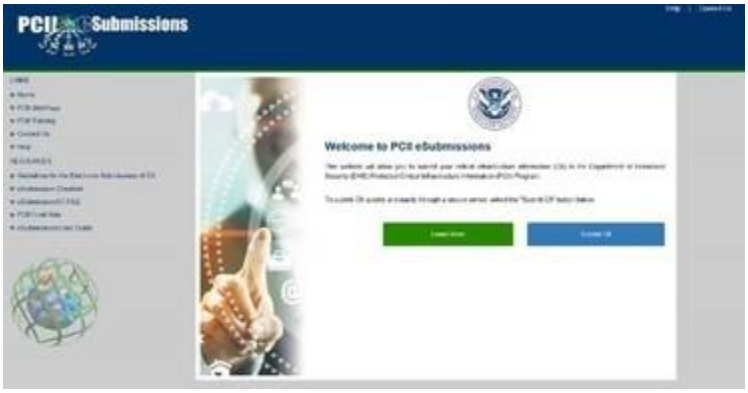
The AEP application consists of three items: the application form, a copy of the applicant's resume or CV, and a supervisor endorsement form submitted by the applicant's supervisor. Both forms can be found online at: https://www.dhs.gov/publication/aep-application-information. Applicants should return the completed application form, along with a resume or CV, and have their supervisors submit the completed supervisor endorsement form to aepsubmissions@hq.dhs.gov no later than **September 28, 2018**.

Please note that by applying you are agreeing/validating:

1. To provide verification of your U.S. citizenship.
2. That your employer supports your participation in the program. If your employment status changes during the program, you must notify the program.
3. That you will make every effort to attend, in-person, the program kick-off and concluding summit in the Washington, D.C. area. **You or your employer will be responsible for the expenses of these two travel engagements.**
4. That you will make every effort to participate in a research trip should your team decide to conduct research.
5. That the U.S. government is under no obligation to fund your travel for program activities; however, limited funds are available for the research trips.

Based upon high demand for participation in AEP, the application window will be open from September 5 – 28th, 2018, or until 500 applications are received. Please contact aep@hq.dhs.gov or 202-447-3873 with any questions. For reference, prior year deliverables can be found here: www.dhs.gov/aep-deliverables

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 prior to accessing the e-Subs webpage that the owner/operator provided an E&C statement.

Upon submission, the CII automatically receives not only the legal protection as provisioned in the CII Act, but 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.

Watch for other DHSChemSecurityTalks in 2020. For more information on events or any questions, contact DHSChemSecurityTalks@hq.dhs.gov.

New DHS Ammonia (Anhydrous) Flyer

DHS published a flyer that can be used by chemical facilities when shipping, selling, or distributing ammonia (anhydrous). Ammonia (anhydrous) is a CFATS Chemical of Interest (COI), and this flyer can be used to notify customers that they may need to report their chemical holdings to DHS.

Facilities are **not** required to share this flyer, but may choose to use it to assist their customers and partners to understand their regulatory obligations. It can be found on the Knowledge Center, and can be downloaded and reproduced by stakeholders as needed.

For more information, contact CFATS@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.

New Insider Threat Mitigation Website

DHS recently released a new website on Insider Threat Mitigation. The website provides information on establishing an insider threat mitigation program, protecting critical assets, recognizing and reporting suspicious

behavior, and how to assess and respond to insider threats. Readers also have access to insider threat mitigation resources and trainings in the form of videos, publications, and on-line training.

For more information, visit the new website or contact InTmitigation@hq.dhs.gov.

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

Preview: Awareness Briefings on Protecting Network Devices

On the heels of its successful Ransomware and Russian Activity webinars, DHS is continuing its Awareness Briefing program in October 2018 with a series of webinars on Protecting Network Devices.

Join experts from the National Cybersecurity and Communications Integration Center who will discuss best practices for protecting network devices in organizations of all types and sizes.

Watch this bulletin and the website for briefing dates and registration information.

Election Security Training

A new course is now LIVE on the Federal Virtual Training Environment (FedVTE): The Election Official as an IT Manager. This course introduces election officials to the knowledge and skills necessary to function as an information technology (IT) manager. Included is a review of election systems, election night reporting, and interconnected election systems vulnerabilities and liabilities. In addition, the course includes a review of resources available to the election community from DHS.

FedVTE provides free online cybersecurity training to U.S. government employees, federal contractors, and veterans.

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.

- September 25, 2018 – Denver, CO
- September 27, 2018 – Laguna Niguel, CA
- October 2, 2018 – National Capitol Region
- 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."

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.

- **Date:** 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 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

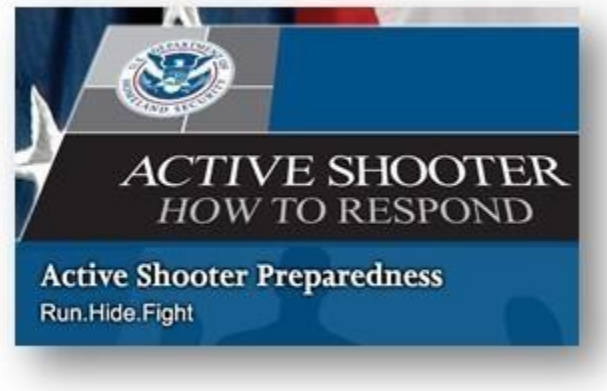
Region IX

- 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

- Saint Michael, ND, Tuesday, October 2
- Denver, CO, Thursday, October 4
- Westminster, CO, Thursday, October 4

Region IX

- 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 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 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 IV

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

- Wednesday, September 26

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

Region V

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

- Tuesday, October 30

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 IV

Anniston AL – Michael Aguilar, 866-213-9547

- Monday, September 24

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

- Tuesday, September 25

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 IV

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

- Monday, September 24

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

- Thursday, September 27

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, October 23

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

- Tuesday, October 23

Region III

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

- Tuesday, October 2

Region IV

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

- Tuesday, September 25

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 I

Providence, RI – Erik Ulmen, erik.ulmen@hq.dhs.gov

- Tuesday, October 2
- Wednesday, October 3

Region V

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

- Wednesday, October 31

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:

- Wednesday, September 26, 2018
- Thursday, September 27, 2018
- Thursday, October 11, 2018
- Tuesday, October 16, 2018
- Thursday, October 18, 2018
- Thursday, October 25, 2018
- Tuesday, October 30, 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, September 25, 2018
- Thursday, September 27, 2018
- Wednesday, October 10, 2018
- Wednesday, October 17, 2018
- Wednesday, October 24, 2018
- Wednesday, October 31, 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:

- Wednesday, September 26, 2018
- Tuesday, October 9, 2018
- Wednesday, October 17, 2018
- Thursday, October 18, 2018
- Tuesday, October 23, 2018
- Wednesday, October 31, 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, September 26, 2018
- Wednesday, October 10, 2018

- Thursday, October 11, 2018
- Tuesday, October 16, 2018
- Wednesday, October 24, 2018
- Thursday, October 25, 2018
- Tuesday, October 30, 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:

- Tuesday, September 25, 2018
- Tuesday, October 9, 2018
- Thursday, October 11, 2018
- Tuesday, October 16, 2018
- Thursday, October 18, 2018
- Tuesday, October 23, 2018
- Thursday, October 25, 2018
- Tuesday, October 30, 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, NC, Thursday, November 15, 2018

Region V

- Glenview, IL, Friday, September 21, 2018
- Oak Forest, IL, Wednesday, October 11, 2018

Missed the last one? Read the August 31, 2018 issue.