

# The Office of Infrastructure Protection

National Protection and Programs Directorate  
Department of Homeland Security

Protective Security Coordination Division Overview

Name of Stakeholder

Date of Briefing



Homeland  
Security

# PSA Mission Areas

- Conduct Security Surveys, Gap Analysis, and Assessments
- Conduct Outreach Activities
- Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) Events
- Respond to Incidents
- Provide Improvised Explosive Device (IED) Awareness & Risk Mitigation Training



# Protective Security Advisor Locations

Protective Security Advisor (PSA) Locations - October 27, 2017

Region VIII				
NAME	PSA DISTRICT	TYPE	STATE	
Graf, Shawn	Denver	IPRD	CO	
Behrman, Scott A.	Salt Lake City	CPS	UT	
O'Keefe, Joseph J. "Joe"	Denver	PSA	CO	
Richards, Jamie	Denver	PSA	CO	
Middebrook, Randy	Helena	PSA	MT	
Ronsberg, Donald "Don"	Bismarck	PSA	ND	
Davis, Scott	Pierre	PSA	SD	
VACANT	Salt Lake City	PSA	UT	
Longfritz, Kenny	Cheyenne	PSA	WY	

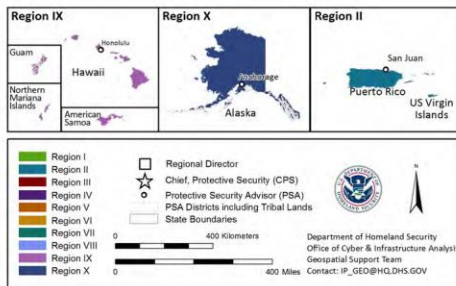
Region VII				
NAME	PSA DISTRICT	TYPE	STATE	
Kirk, Phil	Kansas City	IPRD	MO	
Gardner, Gregory B. "Greg"	Kansas City	CPS	MO	
Prizen, Philip "Phil"	Des Moines	PSA	IA	
Cranehan, Charles "Chuck"	Topeka	PSA	KS	
Macum, Seth	Kansas City	PSA	MO	
Goin, Rick	Jefferson City	PSA	MO	
Hollingwad, Gregory A. "Greg"	Omaha	PSA	NE	

Region V				
NAME	PSA DISTRICT	TYPE	STATE	
Jones, Alexander	Chicago	IPRD	IL	
Gleason, Edward J. "Ed"	Chicago	CPS	IL	
VACANT	Chicago	PSA	IL	
Pennell, Kevin	Springfield	PSA	IL	
DuShane, Charles "Chuck"	Chicago	PSA	IL	
Judge, Christopher "Chris"	Indianapolis	PSA	IN	
Baker, Michael "Mike"	Lansing	PSA	MI	
Lorson, Ernest "Ernie"	Detroit	PSA	MI	
Sanders, Glenn A.	Minneapolis	PSA	MN	
Christianson, Michael	Minneapolis	PSA	MN	
Shaw, Patrick M. "Pat"	Columbus	PSA	OH	
McMasters, Michael "Mike"	Cincinnati	PSA	OH	
Busch, John	Milwaukee	PSA	WI	

Region I				
NAME	PSA DISTRICT	TYPE	STATE	
McCann, Matthew	Boston	IPRD	MA	
VACANT	Boston	CPS	MA	
Pesce, Douglas J. "Doug"	New Haven	PSA	CT	
Wright, Jarrett	Boston	PSA	MA	
Donnelly, Timothy "Tim"	Boston	PSA	MA	
DeLong, William "Bill"	Portland	PSA	ME	
Climer, Jason	Manchester	PSA	NH	
Ullman, Erik	Providence	PSA	RI	
Palazzi, Gabe	Burlington	PSA	VT	

Region X				
NAME	PSA DISTRICT	TYPE	STATE	
Massey, Patrick	Seattle	IPRD	WA	
Holcomb, David "Dave"	Seattle	CPS	WA	
Wilder, Thomas "Tom"	Anchorage	PSA	AK	
Purpe, Eric	Boise	PSA	ID	
Jones, Chas	Portland	PSA	OR	
VACANT	Seattle	PSA	WA	
Richeson, Jonathan "Jon"	Auburn	PSA	WA	

Region IX				
NAME	PSA DISTRICT	TYPE	STATE	
Riccardi, Christine	Merito Park	IPRD	CA	
Calvillo, Frank	Sacramento	CPS	CA	
Figueras, Christine	Phoenix	PSA	AZ	
Schenkel, Keith	Phoenix	PSA	AZ	
Reidel, Chris	Sacramento	PSA	CA	
Michien, Richard S. "Scott"	Los Angeles	PSA	CA	
Wilson, Kelly	San Diego	PSA	CA	
Sierze, Richard D. "Rick"	Fresno	PSA	CA	
Castor, Edgar	San Francisco	PSA	CA	
Keith, Brian	Los Angeles	PSA	CA	
VACANT	San Jose	PSA	CA	
Cruz, James	Honolulu	PSA	HI	
Cordova, Gonzalo H. "Gonzalo"	Las Vegas	PSA	NV	



Region VI				
NAME	PSA DISTRICT	TYPE	STATE	
Nicholas, Steven "Steve"	Dallas	IPRD	TX	
Perriotti, Harvey	Dallas	CPS	TX	
Johnston, Chad	Little Rock	PSA	AR	
Constantin, Phil	New Orleans	PSA	LA	
McKee, Jeff	Baton Rouge	PSA	LA	
VACANT	Albuquerque	PSA	NM	
Moore, Glenn	Oklahoma City	PSA	OK	
Otten, Edwin	Austin	PSA	TX	
Hamilton, Charles "Buck"	El Paso	PSA	TX	
Macra, Michael "Mike"	Houston	PSA	TX	
Nurray, Jeff	Dallas	PSA	TX	
Gray, Bryan	Irving	PSA	TX	
Cary, Richard	Houston	PSA	TX	

Region IV				
NAME	PSA DISTRICT	TYPE	STATE	
Robinson, Donald "Don"	Atlanta	IPRD	GA	
Stallworth, Shawn	Atlanta	CPS	GA	
Toth, Kirk	Ivotile	PSA	AL	
VACANT	Birmingham	PSA	AL	
Frost, Matthew	Miami	PSA	FL	
Sasser, Billy	Tallahassee	PSA	FL	
Warren, Gary E.	Tallahassee	PSA	FL	
Gagnon, Ovia T. III "Ollie"	Tampa	PSA	FL	
Smith, Marty	Orlando	PSA	FL	
Thurmalie, Anthony	Atlanta	PSA	GA	
Matt, Dennis	Atlanta	PSA	GA	
Howard, Greg	Louisville	PSA	KY	
Fenn, James "Max"	Jackson	PSA	MS	
Asper, Darryl I.	Charlotte	PSA	NC	
Meislin, Robert	Raleigh	PSA	NC	
Jones, Keith	Columbia	PSA	SC	
Inns, Michael G.	Memphis	PSA	TN	
Coffey, Mark A.	Nashville	PSA	TN	

Region II				
NAME	PSA DISTRICT	TYPE	STATE	
VACANT	New York City	IPRD	NY	
Durkin, John	New York City	CPS	NY	
Smith, Andrew "Andy"	Newark	PSA	NJ	
Telab, Mohamed	Newark	PSA	NJ	
Tadrick, Joseph "Joe"	New York City	PSA	NY	
Peterson, Kevin	New York City	PSA	NY	
VACANT	New York City	PSA	NY	
Kreyer, Mark W.	Buffalo	PSA	NY	
Stenson, Albert F. "Al"	Albany	PSA	NY	
Gonzalez, Julio	San Juan	PSA	PR	

Region III				
NAME	PSA DISTRICT	TYPE	STATE	
Ryan, William J. "Bill"	Philadelphia	IPRD	PA	
Guest, John	Philadelphia	CPS	PA	
Finney, James "Jamie"	Washington	PSA	DC	
Wolf, Kyle	Washington	PSA	DC	
Greeson, Ken	Dover	PSA	DE	
Hanna, Raymond A. "Ray"	Baltimore	PSA	MD	
Johnston, David "Dave"	Baltimore	PSA	MD	
Winters, Robert E. "Bob"	Pittsburgh	PSA	PA	
Cratty, James	Harrisburg	PSA	PA	
VACANT	Philadelphia	PSA	PA	
VACANT	Norfolk	PSA	VA	
Mooney, Rob	Richmond	PSA	VA	
Ullom, Kenneth C.	Charleston	PSA	WV	

Headquarters				
NAME	PSA DISTRICT	TYPE	STATE	
Watson, Douglas	Arlington HQ	(A) FGB Branch Chief	VA	
Keene, Christopher "Chris"	Arlington HQ	Operations and Coordination Chief	VA	
VACANT	Arlington HQ	Current Operations	VA	
Genus, Daniel "Dan"	Arlington HQ	PSA	VA	
VACANT	Arlington HQ	PSA	VA	
VACANT	Arlington HQ	PSA	VA	
VACANT	Arlington HQ	PSA	VA	
VACANT	Arlington HQ	PSA	VA	



Homeland Security

Courtesy of DHS

# PSA Tools



Homeland  
Security

# Site Assistance Visit

- Establishes and enhances DHS's relationship with critical infrastructure owners and operators, informs them of the importance of their facilities, and reinforces the need for continued vigilance
- During a Site Assistance Visit (SAV), PSAs focus on coordination, outreach, training, and education
- SAVs are often followed by security surveys using the Infrastructure Survey Tool (IST) or delivery of other IP services



# Infrastructure Survey Tool

- The IST is a web-based vulnerability survey tool that applies weighted scores to identify infrastructure vulnerabilities and trends across sectors
- Facilitates the consistent collection of security information
  - Physical Security
  - Security Force
  - Security Management
  - Information Sharing
  - Protective Measures
  - Dependencies



# IST Deliverables

Table 2 Facility and SAA Vulnerabilities and Options for Consideration

Category	Vulnerability	Option(s) for Consideration
Security Management Profile	The facility's security plan is missing key elements.	<p>Update the security plan to include the following:</p> <ul style="list-style-type: none"> <li>• Illumination<sup>3</sup></li> <li>• Security force staffing<sup>4</sup></li> <li>• Security force training<sup>5</sup></li> <li>• Access control procedures for contractors</li> <li>• A security awareness training program that addresses internal disturbances (e.g., workplace violence) <ul style="list-style-type: none"> <li>– Develop a protocol to respond to workplace violence. Refer to the Federal Bureau of Investigation (FBI) Website for resources, such as the January 2011 <i>FBI Law Enforcement Bulletin: Workplace Violence Prevention</i>, available at <a href="http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/january2011/january_2011">http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/january2011/january_2011</a>.</li> <li>– Include policies and procedures to respond to workplace violence threats and incidents in the security plan.</li> <li>– Provide training on workplace violence to all personnel at initial hire and annually thereafter.</li> </ul> </li> <li>• A security awareness training program that addresses security communications policy or procedures</li> <li>• A security awareness training program that addresses information protection/operation security</li> <li>• A security awareness training program that addresses hostage situations</li> <li>• Liaison with response agencies</li> <li>• Exercising the plan</li> <li>• Plan maintenance (e.g., review and revision)</li> </ul>
Security Management Profile	Background checks are not conducted on contractors.	<ul style="list-style-type: none"> <li>• Require contracting companies to conduct background checks on their personnel who will work at the facility and to make such records available for audit.<sup>6</sup></li> </ul>



# IST Deliverables

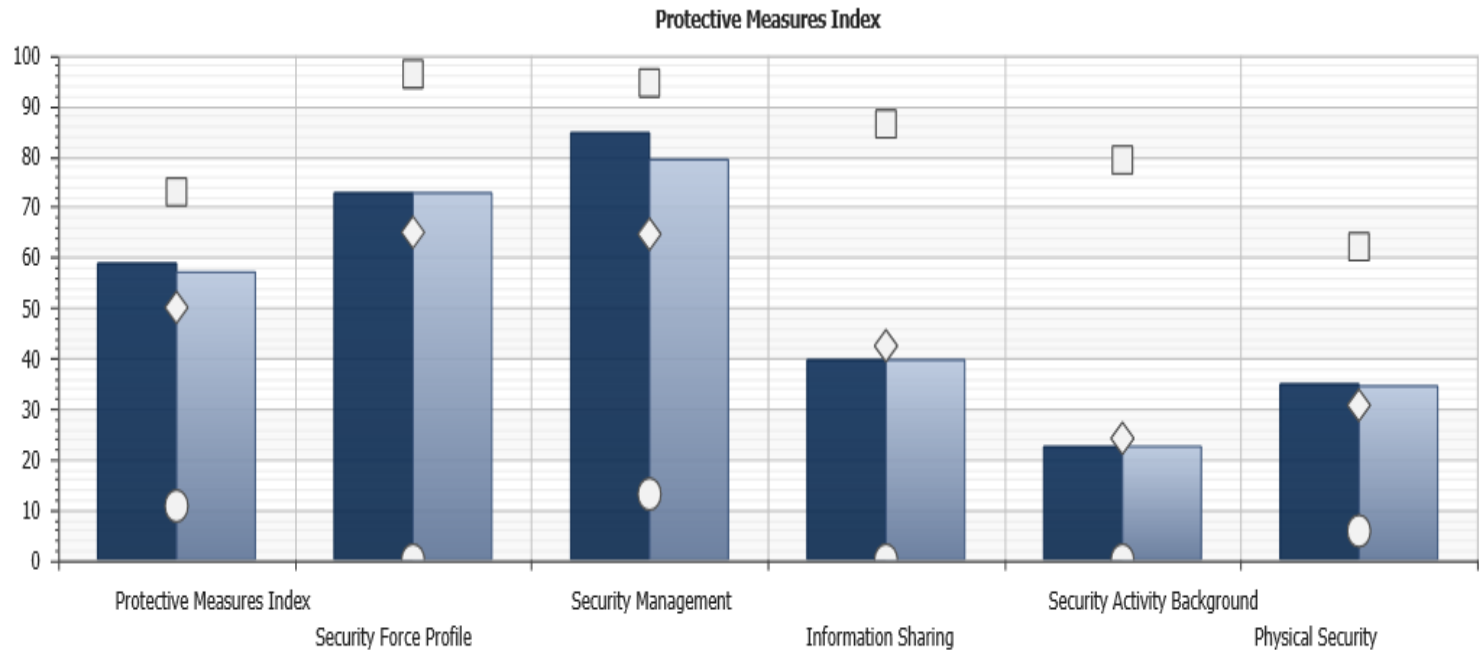
Overview	-
Facility Overview	
SAA Overview	
Security Force	+
Security Management	+
Information Sharing	+
Security Activity Background	+
Physical Security	+
Review	+

## Overview of PMI

Facility  Scenario  Index

**INSTRUCTIONS:** To view the details of any component on the chart below, click on the corresponding blue bars. To view the responses used to calculate the PMI, click on the side navigation menu options.

[Show Chart Data](#)



Homeland  
Security



# Protected Critical Infrastructure Information

- Established under the Critical Infrastructure Information Act of 2002
- Protects voluntarily submitted critical infrastructure information from:
  - Freedom of Information Act
  - State and local sunshine laws
  - Civil litigation proceedings
  - Regulatory usage
- Provides private sector with legal protections and “peace of mind.”

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION Requirements for Use	
Nondisclosure	
<p>This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq. (the “CII Act”), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the “Regulation”) and PCII Program requirements.</p> <p><b>By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.</b></p> <p><b>If you have not completed PCII user training, you are required to send a request to <a href="mailto:pcii-training@dhs.gov">pcii-training@dhs.gov</a> within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.</b></p>	
Access	<p>Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:</p> <ul style="list-style-type: none"> <li>Assigned to homeland security duties related to this critical infrastructure; and</li> <li>Demonstrate a valid need-to-know.</li> </ul> <p>The recipient must comply with the requirements stated in the CII Act and the Regulation.</p>
	<p><b>Storage:</b> When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. <b>Do not leave this document unattended.</b></p> <p><b>Transmission:</b> You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.</p> <p><b>Hand Delivery:</b> Authorized individuals may hand carry material as long as access to the material is controlled while in transit.</p> <p><b>Email:</b> Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. <b>Do not send PCII to personal, non-employment related email accounts.</b> Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment.</p> <p><b>Mail:</b> USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: <b>“POSTMASTER: DO NOT FORWARD. RETURN TO SENDER.”</b> Adhere to the aforementioned requirements for interoffice mail.</p> <p><b>Fax:</b> You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.</p> <p><b>Telephone:</b> You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.</p> <p><b>Reproduction:</b> Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.</p> <p><b>Destruction:</b> Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.</p>
Sanitized Products	<p>You may use PCII to create a work product. The product must not reveal any information that:</p> <ul style="list-style-type: none"> <li>Is proprietary, business sensitive, or trade secret;</li> <li>Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and</li> <li>Is otherwise not appropriately in the public domain.</li> </ul>
Derivative Products	<p>Mark any newly created document containing PCII with “Protected Critical Infrastructure Information” on the top and bottom of each page that contains PCII. Mark “(PCII)” beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Submission Identification Number(s) of the source document(s) must be included on the derivatively created document in the form of a footnote.</p> <p>For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.</p>
<p>Submission Identification Number: _____</p>	
<p><b>PROTECTED CRITICAL INFRASTRUCTURE INFORMATION</b></p>	



**Homeland  
Security**

*Courtesy of DHS*

# Infrastructure Visualization Platform

- Infrastructure Visualization Platform (IVP)
  - A data collection and presentation medium that supports critical infrastructure security, special event planning, and response operations by leveraging assessment data and other relevant materials
  - Integrates assessment data with immersive video, geospatial, and hypermedia data
  - Assists facility owners and operators, local law enforcement, and emergency response personnel to prepare for, respond to, and manage critical infrastructure, National Special Security Events (NSSEs), high-level special events, and contingency operations



# Active Shooter Preparedness Briefs

- DHS aims to enhance preparedness through a “whole community” approach by providing training products, and resources to a broad range of stakeholders on issues such as active shooter awareness, incident response, and workplace violence. In many cases there is no pattern or method to selection of victims by an active shooter, and these situations are, by their very nature, unpredictable and evolve quickly. DHS offers free courses, materials, and workshops to better prepare you to deal with an active shooter situation and to raise awareness of behaviors that represent pre-incident indicators and characteristics of active shooters.



# Infrastructure Protection Report Series



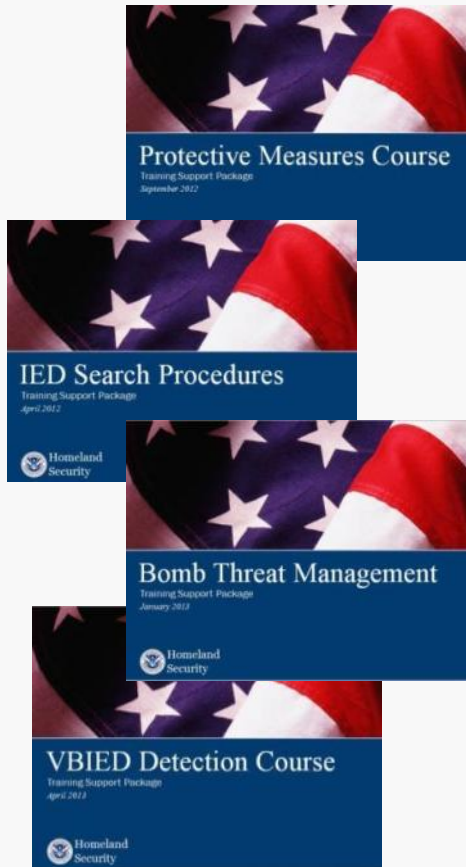
- Increase awareness of the infrastructure mission and build a baseline of security and resilience knowledge throughout the Nation
- Identify Common Vulnerabilities, Potential Indicators of Terrorist Activity, and associated Protective Measures, along with actions that can be undertaken to enhance resilience

*Courtesy of DHS*



**Homeland  
Security**

# Counter-IED Training & Awareness



*Courtesy of DHS OBP*

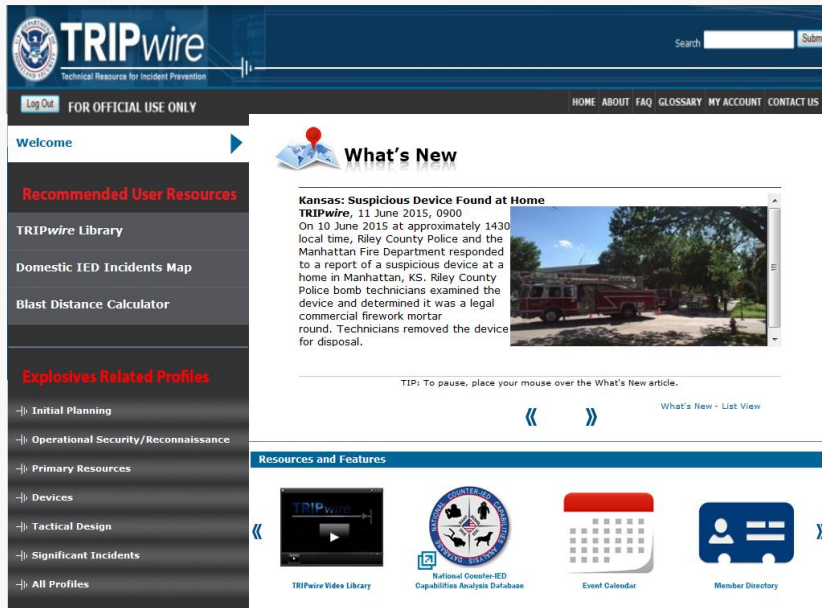
- Diverse curriculum of training designed to build counter-IED core capabilities, such as:
  - IED Counterterrorism Detection
  - Surveillance Detection
  - Bomb Threat Management
  - Vehicle-Borne IED (VBIED) Detection
  - Protective Measures
  - IED Search Procedures
- Increases knowledge and ability to detect, prevent, protect against, and respond to bombing threats



**Homeland  
Security**

# TRIPwire

## Technical Resource for Incident Prevention



*Courtesy of TRIPwire*

- Secure information sharing platform for IED incident information, evolving IED tactics, lessons learned, and counter-IED preparedness information
- Builds knowledge and preparedness capabilities, filling vital gaps in information sharing



Homeland  
Security



# Other Products and Services (cont.)

## Bomb Threat Guidance and Vehicle Inspection Guide



*Courtesy of DHS OBP*

- Bomb Threat Guidance provides a quick-reference for managing in-progress bomb threats for schools, businesses, and government facilities with information on police coordination, threat assessment, search, and evacuation versus shelter-in-place considerations
- Vehicle Inspection Guide assists Government and private sector security personnel in conducting vehicle inspection operations to prevent vehicle-borne IEDs



**Homeland  
Security**

# Cyber Support for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
  - United States Computer Emergency Readiness Team (US-CERT) Operations Center
  - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Operations Center
  - National Cybersecurity Assessment & Technical Services (NCATS)
- US-CERT
- Control Systems Security Program
- Cyber Exercise Program
- Cyber Security Evaluations Program
- Cyber Security Advisors







# Homeland Security

For more information, visit:  
[www.dhs.gov/critical-infrastructure](http://www.dhs.gov/critical-infrastructure)

Kyle Wolf

Protective Security Advisor

[Kyle.wolf@hq.dhs.gov](mailto:Kyle.wolf@hq.dhs.gov)



Homeland  
Security