

The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Protective Security Coordination Division

Protective Security Advisor Program and DHS Services

9/6/2018



Homeland
Security

Protective Security Advisors

- PSAs are non-regulatory, field-deployed personnel who serve as critical infrastructure security and resilience advisors
- Link State, local, tribal, and territorial (SLTT) and private sector partners to DHS resources and services
 - Coordinate vulnerability assessments, training, and other DHS products and services
 - Share information in steady state, during special events and incidents
 - Assist facility owners and operators with obtaining security clearances
- During contingency events, PSAs support the response, recovery, and reconstitution efforts
 - Man state and local emergency operations centers
 - Serve as pre-designated Infrastructure Liaisons (IL) at Joint Field Offices



Protective Security Advisor Locations

Protective Security Advisor (PSA) Locations - July 21, 2015

Region VII				
STATE	CITY	NAME		TYPE
UT	Salt Lake City	Bahouth, Scott A.		RD
CO	Denver	O'Keefe, Joseph J.		PSA
CO	Denver	VACANT		PSA
MT	Helena	Middlebrook, Randy		PSA
ND	Bismarck	Rosenberg, Donald		PSA
SD		VACANT		PSA
UT	Salt Lake City	Lay, Rash		PSA
WY	Cheyenne	Loughlin, Kenny		PSA

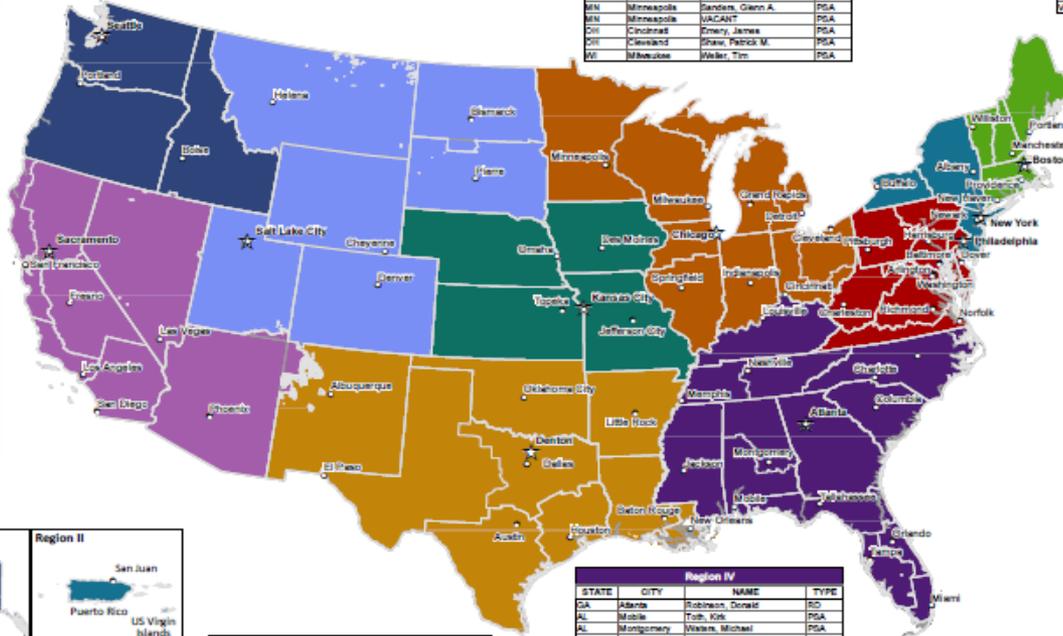
Region VII				
STATE	CITY	NAME		TYPE
MO	Kansas City	Sardner, Gregory S.		RD
IA	Des Moines	Peters, Philip "Phil"		PSA
KS	Topeka	Santhan, Charles		PSA
MO	Jefferson City	Sotha, Rick		PSA
MO	Kansas City	VACANT		PSA
NE	Omaha	Hollingshead, Gregory A.		PSA

Region V				
STATE	CITY	NAME		TYPE
IL	Chicago	Gleason, Edward J.		RD
IL	Chicago	Bauch, John		PSA
IL	Chicago	Dulhane, Chuck		PSA
IL	Springfield	Pennell, Kevin		PSA
IN	Indianapolis	Finney, James		PSA
MI	Grand Rapids	VACANT		PSA
MI	Grand Rapids	VACANT		PSA
MI	Minneapolis	Sanders, Glenn A.		PSA
MI	Minneapolis	VACANT		PSA
OH	Cincinnati	Finney, James		PSA
OH	Cincinnati	Shaw, Patrick M.		PSA
WI	Madison	Waller, Tim		PSA

Region I				
STATE	CITY	NAME		TYPE
MA	Boston	Erskine, Donald "Don"		RD
CT	New Haven	Paceo, Douglas J.		PSA
MA	Boston	Connelly, Timothy		PSA
MA	Boston	Richmond, Albert		PSA
ME	Portland	DeLong, William		PSA
NH	Manchester	Palmer, Ronald		PSA
RI	Providence	VACANT		PSA
VT	Williston	Palazzi, Gabe		PSA

Region X				
STATE	CITY	NAME		TYPE
WA	Seattle	Hunsinger, Dennis		RD
AK	Anchorage	Burgess, Thomas J.		PSA
ID	Boise	Paype, Eric		PSA
OR	Portland	Collins, Glen S.		PSA
WA	Seattle	Holcomb, Dave		PSA
WA	Seattle	VACANT		PSA

Region IX				
STATE	CITY	NAME		TYPE
CA	Sacramento	Dakilo, Frank		RD
AZ	Phoenix	Piquero, Christina		PSA
AZ	Phoenix	VACANT		PSA
CA	San Francisco	Caster, Edgar		PSA
CA	Los Angeles	Kalsh, Brian		PSA
CA	Los Angeles	Mitchem, Richard S.		PSA
CA	Sacramento	Rindel, Chris		PSA
CA	Fresno	Starks, Richard D.		PSA
CA	San Diego	Wilson, Kelly		PSA
CA	San Francisco	VACANT		PSA
HI	Honolulu	VACANT		PSA
NV	Las Vegas	Condrvo, Gonzalo H.		PSA



■ Region I
■ Region II
■ Region III
■ Region IV
■ Region V
■ Region VI
■ Region VII
■ Region VIII
■ Region IX
■ Region X
■ Region XI

★ Regional Director & PSA
★ Protective Security Advisor (PSA)
★ PSA Clients including Tribal Lands
— State Boundaries

Department of Homeland Security
 Office of Infrastructure Protection (IP)
 IP Geographic Support Team
 Contact: IP_GSD@HQ.DHS.GOV

Region VI				
STATE	CITY	NAME		TYPE
TX	Denton	Nicholas, Steve		RD
AR	Little Rock	VACANT		PSA
LA	New Orleans	Conestable, Phil		PSA
LA	Baton Rouge	Madley, Jeff		PSA
NM	Albuquerque	Murray, Jeff		PSA
OK	Oklahoma City	Moore, Glenn		PSA
TX	Houston	Cuddeker, Scott E.		PSA
TX	El Paso	Hamilton, Charles		PSA
TX	Houston	Maucha, Mike		PSA
TX	Austin	McPherson, Ronald A.		PSA
TX	Dallas	Parmer, Harvey		PSA
TX	Dallas	VACANT		PSA

Region IV				
STATE	CITY	NAME		TYPE
GA	Atlanta	Robinson, Donald		RD
AL	Mobile	Toth, Kim		PSA
MS	Montgomery	Waters, Michael		PSA
FL	Tampa	Gagnon, Ovide T. III		PSA
FL	Tallahassee	Gesser, Sily		PSA
FL	Orlando	Smith, Mary		PSA
FL	Miami	Waters, Gary E.		PSA
FL	Miami	VACANT		PSA
GA	Atlanta	VACANT		PSA
GA	Atlanta	VACANT		PSA
NY	Louisville	Howard, Greg		PSA
MS	Jackson	Fann, James "Mac"		PSA
NC	Charlotte	Apey, Darryl		PSA
NC	Raleigh	VACANT		PSA
SC	Columbia	Jones, Keith		PSA
TN	Nashville	Coffey, Mark A.		PSA
TN	Memphis	Innis, Michael G.		PSA

Region II				
STATE	CITY	NAME		TYPE
NY	New York	Wheatall, Frank		RD
NJ	Newark	Lafery, Tom		PSA
NJ	Newark	Trach, Mohamed		PSA
NY	Ruffalo	Krayer, Mark W.		PSA
NY	New York	Peterson, Kevin		PSA
NY	New York	Tadish, Joseph		PSA
NY	Albany	Stanton, Albert F.		PSA
NY	New York	VACANT		PSA
DE	San Juan	Gonzalez, Julio		PSA

Region III				
STATE	CITY	NAME		TYPE
PA	Philadelphia	Guest, John		RD
DC	Washington	VACANT		PSA
DC	Washington	VACANT		PSA
DE	Dover	Greason, Ken		PSA
MD	Baltimore	Hanna, Raymond A.		PSA
MD	Baltimore	VACANT		PSA
PA	Philadelphia	Ryan, William		PSA
PA	Pittsburgh	Wilkins, Robert E.		PSA
PA	Harrisburg	White, Stephen		PSA
VA	Richmond	Mooney, Rob		PSA
VA	Norfolk	Owen, Peter		PSA
WV	Charleston	Elliot, Kenneth C.		PSA

Headquarters				
STATE	CITY	NAME		TYPE
VA	Arlington	Bakony, Brian		FOI Branch Chief
VA	Arlington	Cifton, Elizabeth "Liz"		FOI Deputy Branch Chief
VA	Arlington	Richards, Jamie		Operations Planning and Coordination
VA	Arlington	Wombacher, Matthew		Current Operations Chief
VA	Arlington	Keane, Christopher (Military Leave)		Contingency Operations
VA	Arlington	Dagan, William		PSA
VA	Arlington	VACANT		PSA
VA	Arlington	VACANT		PSA
VA	Arlington	VACANT		PSA
VA	Arlington	VACANT		PSA



Homeland Security
 Department of Homeland Security
 Office of Infrastructure Protection (IP)
 IP Geographic Support Team
 Contact: IP_GSD@HQ.DHS.GOV

Courtesy of DHS

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

Non-disclosure

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.

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.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov 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.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and
- Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the CII Act and the Regulation.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended.**

Transmission: 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.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.

Email: 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. **Do not send PCII to personal, non-employment related email accounts.** Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment.

Mail: 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: **“POSTMASTER: DO NOT FORWARD. RETURN TO SENDER.”** Adhere to the aforementioned requirements for interoffice mail.

Fax: 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.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: 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.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative Products

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.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION



Homeland Security

Courtesy of DHS

Enhanced Critical Infrastructure Protection Visit

- Establishes and enhances DHS's relationship with critical infrastructure owners and operators
- During an Enhanced Critical Infrastructure Protection (ECIP) visit, PSAs focus on coordination, outreach, training, and education
- ECIP visits include local, state, and federal response and support partners to enable everyone to gain a better understanding of the site and enable us all to move forward together
- Perfect one stop shop to meet the local players of importance



**Homeland
Security**

Infrastructure Survey Tool

- The IST is a web-based vulnerability survey tool that applies weighted scores to identify infrastructure vulnerabilities and trends across sectors
- Collects data for a snapshot in time for sites for feedback
 - Physical Security, Security Force, Security Management, Information Sharing, Protective Measures, Dependencies
- The Dashboard tool allows facility owners and operators to:
 - Compare a facility's security in relation to similar facilities
 - Identify security gaps
 - Track progress toward improving critical infrastructure security



Example Dashboard - Protection



- 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](#)



LEGEND: Existing Scenario Selected High Average Low Selected Marker

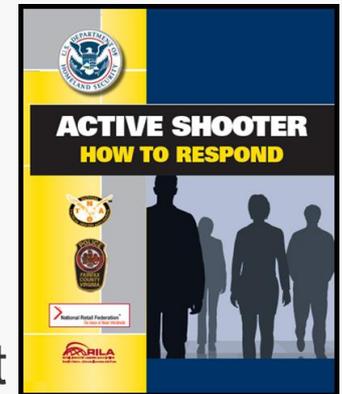
Compared to: 144 (Office Building - Stand Alone)
 Assessment Finalized Date: April 12, 2012
 Refresh Date: February 09, 2018
 Tracking Number: PCII1234

WARNING: Data contained on this system is Protected Critical Infrastructure Information. [Link to more info](#)

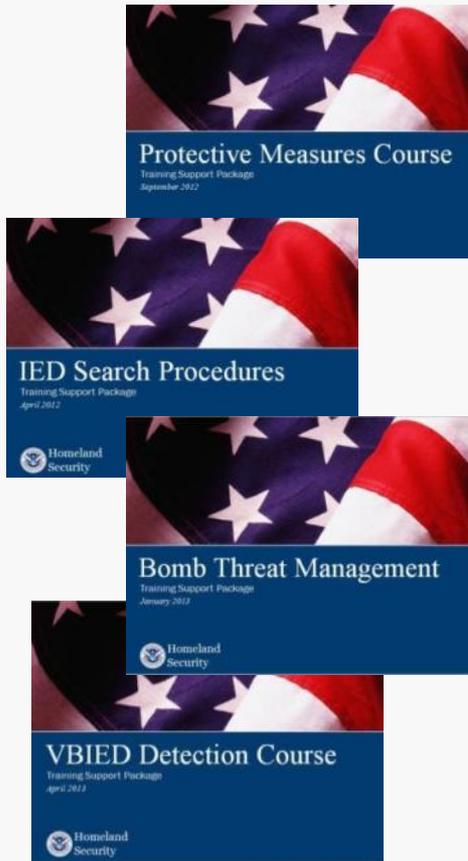


Active Shooter: Preparation and Response Presentations

- 1-hr. based on 2012 Joint DHS/FBI Bulletin and best practices
- Background Information on personalities that perpetrate these attacks
 - Propensity towards violence, mental illness, triggering point
 - To aid employees and disrupt possible events
- Planning
 - Individual mental maps
 - Organizational plans
- Response – Situationally based: Run, Hide or Fight
- Recovery – based on plans and profound nature of attack
- Also 3-hr TTX available



Counter-IED Training & Awareness



Courtesy of DHS OBP

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



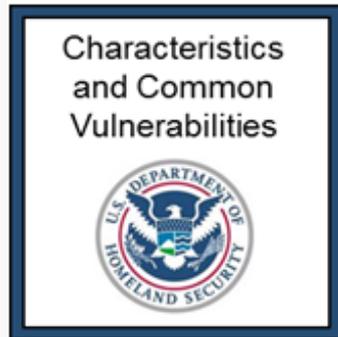
**Homeland
Security**

Homeland Security Information Network (HSIN)

- HSIN (<https://hsin.dhs.gov/>) is DHS's primary technology tool for trusted information sharing
- HSIN – Critical Infrastructure (HSIN-CI) enables direct communication between:
 - DHS
 - Federal, State, and local governments
 - Critical infrastructure owners and operators
- Content includes:
 - Planning and Preparedness
 - Incident Reporting and Updates
 - Situational Awareness
 - Education and Training



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**

DHS/IP – Partners

InfraGard

- An information-sharing and analysis effort serving the interests and combining the knowledge of a wide range of members
- Partnership between FBI and private sector
- Businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent/mitigate acts against the United States
- <http://www.infragard.net>

See Something Say Something

- Nationwide Suspicious Activity Reporting Initiative (NSI)
- States control most local programs with information and posters available
- Customized products can also be obtained
- DHS support in preparation of material, posters, etc
- Contact seesay@hq.dhs.gov



Report suspicious activity
to local law enforcement
or call 9-1-1 in case
of emergency.



if you
SEE
something
SAY
something™

If You See Something Say Something™ used with permission of the U.S. Department of Homeland Security.

Private Sector Resources Catalog

- www.dhs.gov/private-sector-resources-catalog
- All DHS agencies have available material
- Training
 - FEMA, Active Shooter, Workplace Violence, Surveillance Detection
- Information
 - Homeland Security Information Network, TripWire, National Terrorism Alert System, National Suspicious Activity Reporting
- Services
 - Wireless Priority Service (WPS)/Government Emergency Telephone System (GETS), Geographic Information Systems
- Systems
 - Protected Critical Infrastructure Information, Chemical Facility Anti-Terrorism Standards, Business Continuity
- Cyber – Assessments, bulletins, and best practices



**Homeland
Security**

DHS Cyber Security Programs

- Cyber Hygiene Evaluations
 - Assess Internet accessible systems for known vulnerabilities and configuration errors
- ICS Architecture Review
 - Intensive and exhaustive review of the security architecture for industrial control, process automation, and other cyber-physical systems
- Penetration Test/Risk and Vulnerability Assessment
 - Conducts red-team assessments and provides remediation recommendations



Homeland
Security

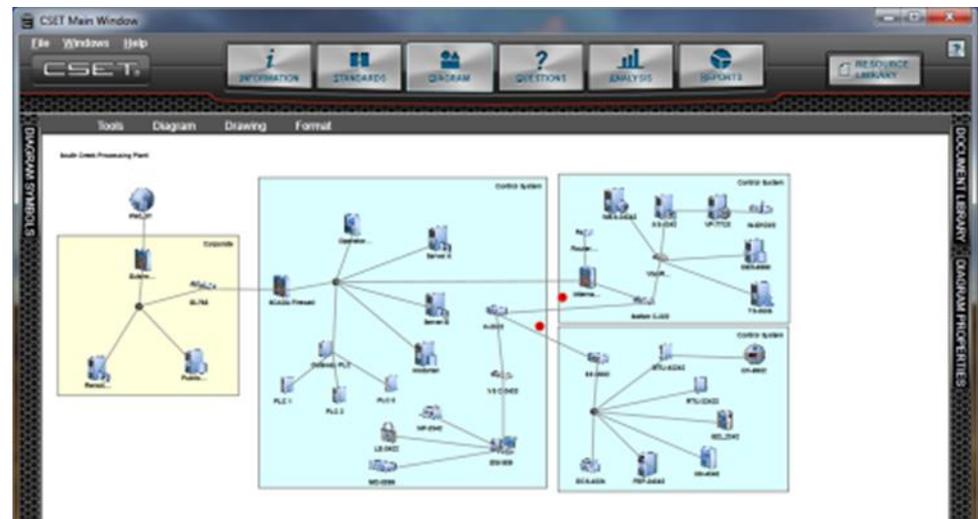
DHS Cyber Security Programs

- Cyber Resilience Review (CRR)
 - Evaluate how CIKR providers manage cyber security of significant information services and assets
- Cyber Infrastructure Survey Tool (C-IST)
 - Identify and document critical cyber security information including system-level configurations and functions, cyber security threats, cyber security measures, IT business continuity/disaster recovery and cyber security organizational management
- Cyber Security Evaluation Tool (CSET)
 - Self-assessment using recognized standards
 - http://us-cert.gov/control_systems/csetdownload.html



DHS Cyber Security Programs - CSET

- Network Mapping
- System comparisons to chosen standards
- Hard copy reports
- Resource library



The screenshot shows the CSET Resource Library interface. On the left is a 'Document Tree' with categories like Guidelines, Reports, Cryptography & Encryption, and Security Plans. The main area displays a document titled 'Resource Library' with a blue background and a grid pattern. The document text includes: 'This library of cyber security standards, reports, and templates are provided for your convenience. Additionally there are several cyber security guides and white papers to assist you in gaining a general background in cyber security, determining priorities, or specific needs. Specific topics include white papers and instructions on securing network components such as a firewall or web server. Library documents may be browsed using the "Document Tree" tab on the left side of the screen. Documents are grouped by type and topic. If you are looking for a specific document a keyword or the search may also be performed using the "Search" tab in the left pane. Clicking on a document title in the left-hand pane displays the document. To save a document to your local hard drive click the report button.'

Hard-copy Reports

The screenshot shows a hard-copy report titled 'SITE SUMMARY REPORT' for 'Prime Bufile Processing Plant'. The report includes a 'CONTROL SYSTEMS CYBER SECURITY EVALUATION' section. It features a 'CSET' logo and a 'Homeland Security' logo. The report also includes a 'SUMMARY EXECUTIVE OVERVIEW' section with a table showing 'Overall' and 'Standards' scores. The report is dated 'January 7, 2011'.



Cyber Security Contact Information

Evaluation Inquiries

cse@hq.dhs.gov

General Inquiries

cyberadvisor@hq.dhs.gov

Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications



Homeland Security

For more information visit:
www.dhs.gov/critical-infrastructure

Bob Winters - bob.winters@dhs.gov
Protective Security Advisor - Pittsburgh

Nationally – psaoperations@hq.dhs.gov



Homeland
Security