

The Office of Infrastructure Protection

National Protection and Programs Directorate Department of Homeland Security

- Vision & Mission
- Cyber Threats
- Protective Security Advisor
- Cyber Resources
- Protected Critical Infrastructure Information (PCII)

Marty J. Smith
Protective Security Advisor
Orlando, FL
Marty.J.Smith@hq.dhs.gov



Homeland
Security

Vision and Mission

- Vision - A safe, secure, and resilient critical infrastructure based on, and sustained through, strong public and private partnerships
- Mission - Lead the National effort to mitigate terrorism risk to, strengthen the protection of, and enhance the all-hazard resilience of the Nation's critical infrastructure



Threats May Come from All Hazards



Homeland
Security

Cyber Threat Actors

- DHS is concerned with the recent rise in targeted and successful malware campaigns against industrial control systems (ICSs).
- These campaigns were associated with sophisticated threat actors with demonstrated capabilities to compromise control system networks.
- The depth of intrusion into the control system network provided the threat actors with the ability to potentially:
 - Manipulate control system settings
 - Control the process
 - Destroy data and/or equipment.



“Cyber Threats Pose an Enormous Challenge”

President Barack Obama: Speech at the National Cybersecurity and Communications Integration Center – Jan 13, 2015:

“It's one of the most serious economic and national security challenges we face as a nation. Foreign governments, criminals, and hackers probe America's computer networks every single day.”

President Obama also noted that protecting the nation's critical infrastructure is essential to public health and safety stating that,

“Neither government, nor the private sector can defend the nation alone. It's going to have to be a shared mission — government and industry working hand in hand, as partners.”



Homeland
Security

Growing Concerns for Control Systems

NSA Director, Admiral Michael Rogers
Testimony to House Select Intelligence
Committee – Nov. 20, 2014:

“There shouldn’t be any doubt in our minds that there are nation-states and groups out there that have the capability to enter industrial control systems and to shut down [and] forestall our ability to operate our basic infrastructure.”

“All of that leads me to believe it is only a matter of the ‘when,’ not the ‘if’ that we are going to see something dramatic.”



Homeland
Security

Protective Security Advisors

- PSAs are field-deployed personnel who serve as critical infrastructure security specialists
 - Regional Directors (RDs) oversee and manage the PSA program in their respective region
- State, local, tribal, and territorial (SLTT) and private sector link to DHS infrastructure protection resources
 - Coordinate vulnerability assessments, training, and other DHS products and services
 - Provide a vital link for information sharing in steady state and incident response
 - Assist facility owners and operators with obtaining security clearances
- During contingency events, PSAs support the response, recovery, and reconstitution efforts of the States by serving as pre-designated Infrastructure Liaisons (IL) and Deputy ILs at the Joint Field Offices



Value of the PSA Program

- PSAs:
 - Support comprehensive risk analyses for critical infrastructure
 - Assist in the review and analysis of physical/technical security for critical infrastructure
 - Convey local concerns and sensitivities to DHS and other Federal agencies
 - Relay disconnects between local, regional, and National protection activities
 - Communicate requests for Federal training and exercises



Protective Security Advisor Locations

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

Region VII				
STATE	CITY	NAME		TYPE
UT	Salt Lake City	Bekuhn, 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	Platte	VACANT	PSA	
UT	Salt Lake City	Lay, Keith	PSA	
WY	Cheyenne	Longfitt, Kanny	PSA	

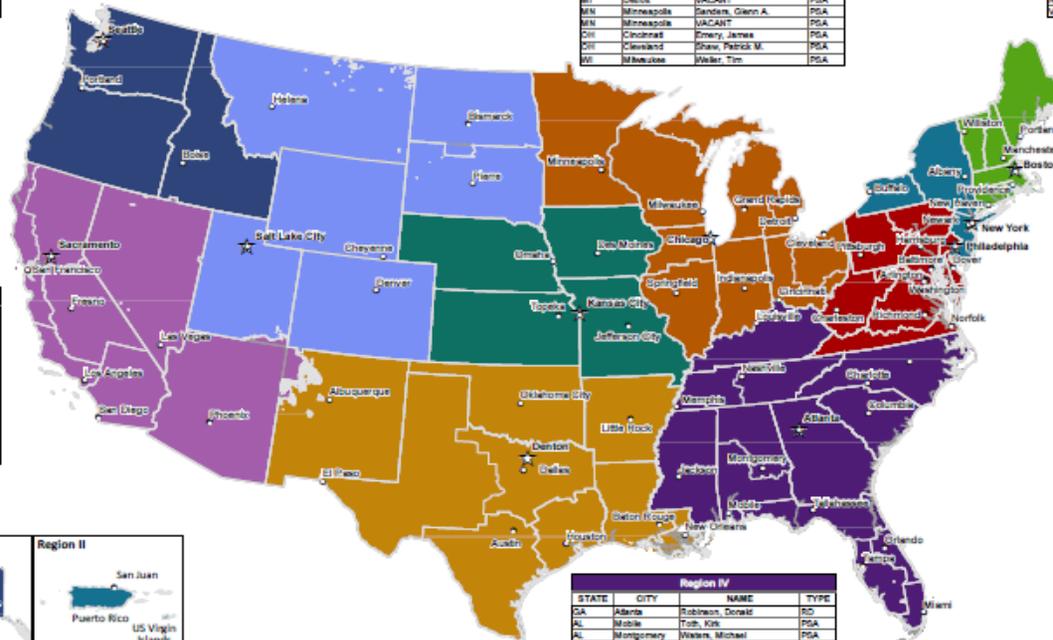
Region VII				
STATE	CITY	NAME		TYPE
MO	Kansas City	Sardner, Gregory B.	RD	
IA	Des Moines	Pleas, Philip "Tom"	PSA	
KS	Topeka	Santhan, Charles	PSA	
MO	Jefferson City	Soles, Rick	PSA	
MO	Kansas City	VACANT	PSA	
NE	Omaha	Hollingshead, Gregory A.	PSA	

Region V				
STATE	CITY	NAME		TYPE
IL	Chicago	Gleason, Edward J.	RD	
IL	Chicago	Bauch, John	PSA	
L	Chicago	Dulane, Chuck	PSA	
IL	Springfield	Pannell, 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	Cleveland	Gray, Patrick M.	PSA	
WI	Madison	Walker, Tim	PSA	

Region I				
STATE	CITY	NAME		TYPE
MA	Boston	Emaine, Donald "Ken"	RD	
CT	New Haven	Paton, Douglas J.	PSA	
MA	Boston	Donnelly, Timothy	PSA	
MA	Boston	Richmond, Albert	PSA	
ME	Portland	DeLong, William	PSA	
NH	Manchester	Phemer, Ronald	PSA	
RI	Providence	VACANT	PSA	
VT	Williston	Palazzi, Gabe	PSA	

Region X				
STATE	CITY	NAME		TYPE
WA	Seattle	Hornberger, 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	Calvillo, Frank	RD	
AK	Anchorage	Piquero, Christina	PSA	
NE	Omaha	VACANT	PSA	
CA	San Francisco	Castor, Edgar	PSA	
CA	Los Angeles	Kalsh, Brian	PSA	
CA	Los Angeles	Mitchem, Richard S.	PSA	
CA	Sacramento	Randel, 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	Condo, Gonzalo H.	PSA	



Region II				
STATE	CITY	NAME		TYPE
NY	New York	Wesfall, Frank	RD	
NJ	Newark	Lacey, Eric	PSA	
NJ	Newark	Yak, Mohamed	PSA	
NY	Duffalo	Kroyer, Mark W.	PSA	
NY	New York	Peterson, Kevin	PSA	
NY	New York	Tadlock, Joseph	PSA	
NY	Albany	Stinson, Albert F.	PSA	
NY	New York	VACANT	PSA	
PR	San Juan	Gonzalez, Julio	PSA	

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



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

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

Department of Homeland Security
 Office of Infrastructure Protection (OIP)
 IP Geospatial 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	Conestoga, Phil	PSA	
LA	Baton Rouge	Mackay, Jeff	PSA	
NM	Albuquerque	Murray, Jeff	PSA	
OK	Oklahoma City	Moore, Glenn	PSA	
TX	Houston	Cubber, Scott E.	PSA	
TX	El Paso	Henderson, Charles	PSA	
TX	Houston	Maiche, Mike	PSA	
TX	Austin	McPherson, Ronald A.	PSA	
TX	Dallas	Pariser, Harvey	PSA	
TX	Dallas	VACANT	PSA	

Region IV				
STATE	CITY	NAME		TYPE
GA	Atlanta	Robinson, Donald	RD	
AL	Mobile	Tubb, Kim	PSA	
AL	Montgomery	Waters, Michael	PSA	
FL	Tampa	Gagnon, Ovide T. II	PSA	
FL	Tallahassee	Sasser, Billy	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	Wheat, Greg	PSA	
MS	Jackson	Fann, James "Mac"	PSA	
NC	Houston	Cubber, Scott E.	PSA	
NC	Charlotte	Apery, Darryl	PSA	
NC	Raleigh	VACANT	PSA	
SC	Columbia	James, Keith	PSA	
TN	Nashville	Coffey, Mark A.	PSA	
TN	Memphis	Innis, Michael G.	PSA	

Headquarters				
STATE	CITY	NAME		TYPE
VA	Arlington	Buckley, Brian	FOD Branch Chief	
VA	Arlington	Cotton, Elizabeth "Liz"	FOD Deputy Branch Chief	
VA	Arlington	Richards, Jenie	Operations Planning and Coordination	
VA	Arlington	Wronoscher, Matthew	Current Operations Chief	
VA	Arlington	Keane, Christopher (Military Leave)	Contingency Operations	
VA	Arlington	Ragan, William	PSA	
VA	Arlington	VACANT	PSA	
VA	Arlington	VACANT	PSA	
VA	Arlington	VACANT	PSA	
VA	Arlington	VACANT	PSA	



Homeland Security

Cyber Offerings for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
 - US-CERT Operations Center
 - Remote and On-Site Assistance
 - Malware Analysis
 - Incident Response Teams
 - ICS-CERT Operations Center
 - ICS-CERT Malware Lab
 - Cyber Security Evaluation Tool
 - Incident Response Teams
 - NCATS
 - Cyber Hygiene service
 - Risk and Vulnerability Assessment
- US-CERT
 - National Cyber Awareness System
 - Vulnerability Notes Database
 - Security Publications
- Control Systems Security Program
 - Cybersecurity Training
 - Information Products and Recommended Practices
- Cyber Exercise Program
- Cyber Security Evaluations Program
 - Cyber Resilience Review
 - Cyber Infrastructure Survey Tool



Cybersecurity Evaluations – Summary 1

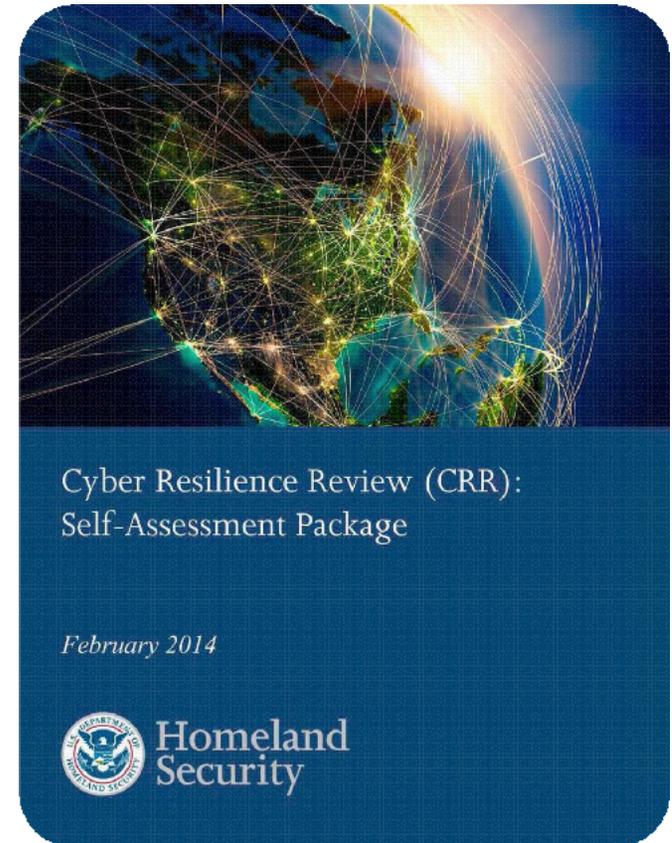
Name	Cyber Resilience Review (CRR)	Cyber Infrastructure Survey Tool (C-IST)	Supply Chain / External Dependency Management (EDM) Review	Onsite Cyber Security Evaluation Tool (CSET) Assessment
Purpose	Identify cyber security management capabilities and maturity	To calculate a comparative analysis and valuation of protective measures in-place	Identify external dependencies and the risks associated	Provides a detailed, effective, and repeatable methodology for assessing control systems security – while encompassing an organization’s infrastructure, policies, and procedures.
Scope	Critical Service view	Critical Cyber Service view	Organization / Business Unit	Industrial Control Systems
Time to Execute	8 Hours (1 business day)	2 ½ to 4 Hours	2 to 2 ½ Hours	8 Hours (1 Business Day)
Information Sought	Capabilities and maturity indicators in 10 security domains	Protective measures in-place	Third-party security requirements and contract management info	Industrial control system’s core functions, infrastructure, policies, and procedures
Preparation	Short, 1-hour questionnaire plus planning call(s)	Planning call to scope evaluation	Planning call to scope evaluation	Coordinated via Email. Planning call(s) if requested.
Participants	IT/Security Manager, Continuity Planner, and Incident Responders	IT/Security Manager	IT / Security Manager with Contract Management	control system operators/engineers, IT, policy/management personnel, and subject matter experts.

Cybersecurity Evaluations – Summary 2

Name	ICS-CERT Design Architecture Review (DAR)	ICS Network Architecture Verification and Validation (NAVV)	Network Risk and Vulnerability Assessment (RVA)	Cyber Hygiene (CH) Evaluation
Purpose	Supports the cybersecurity design via investigative analysis, production, and maintenance of control systems and ICS components.	Provides analysis and baselining of ICS communication flows, based upon a passive (non-intrusive) collection of TCP Header Data.	Perform penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks	Identify public-facing Internet security risks, at a high-level, through service enumeration and vulnerability scanning
Scope	Industrial Control Systems/Network Architecture	Industrial Control Systems/ Network Architecture/ Network Traffic	Organization / Business Unit / Network-Based IT Service	Public-Facing, Network-Based IT Service
Time to Execute	2 Days (8 Hours Each Day)	Variable (Hours to Days)	Variable (Days to Weeks)	Variable (Hours to Continuous)
Information Sought	Network design, configurations, interdependencies, and its applications.	Network traffic header-data to be analyzed with Sophia Tool.	Low-level options and recommendations for improving IT network and system security	High-level network service and vulnerability information
Preparation	Coordinated via Email. Planning call(s).	Coordinated via Email. Planning call(s).	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs	control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs	IT/Security Manager and Network Administrators	IT/Security Manager and Network Administrators

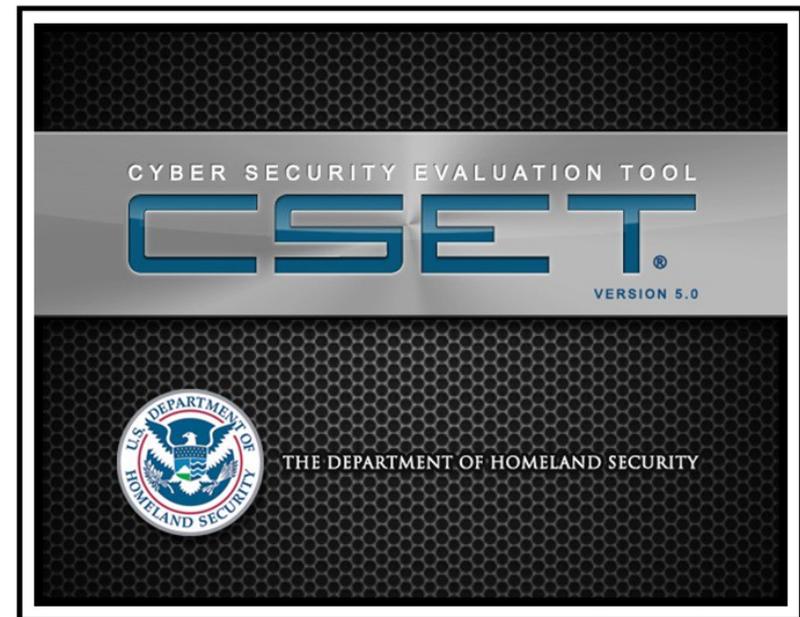
CRR Self-Assessment Package

- Released in February 2014 to complement the launch of the NIST CSF.
- The CRR Self-Assessment Kit allows organizations to conduct a review without outside facilitation.
- Contains the same questions, scoring, and reporting as the facilitated assessment.
- The kit contains the following resources:
 - Method Description and User Guide
 - Complete CRR Question Set with Guidance
 - Self-Assessment Package (automated toolset)
 - CRR to NIST CSF Crosswalk
- **CRR Self-Assessment Kit website:**
 - <http://www.us-cert.gov/ccubedvp/self-service-crr>



Cyber Security Evaluation Tool – CSET®

- Stand-alone software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy



CSET Download:

http://us-cert.gov/control_systems/csetdownload.html



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

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.

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

For more information visit:
www.dhs.gov/criticalinfrastructure

Marty J. Smith

Protective Security Advisor - Orlando

Marty.J.Smith@hq.dhs.gov / NICC@hq.dhs.gov



Homeland
Security