

# JOINT PROVOST/ACADEMIC SENATE RETREAT

## Session #3

Campus Safety:  
Faculty Training and Resources  
FEEC Recommendations

# FEEC Recommendations Participants

- Faculty
- Students
- DPS
- DHS

# FEEC Recommendations

- Training
- Physical Security
- Psychological Support for Students
- Security Assessments

# FEEC Recommendations Training

- Faculty / Classroom Focused
- In Person
- Exercises
- Mandatory

# FEEC Recommendations

## Physical Security

- Doors and Locks
- Alarm Buttons
- Classroom Emergency Plans
- First Aid Kits
- Wallet Size Emergency Cards
- Wear ID Cards

# FEEC Recommendations Students

- Increase Psychological Support
- Behavioral Indicators
- New Student Course on Safety

# FEEC Recommendations DHS Assessments

- Enhanced Critical Infrastructure Protection (ECIP)
- Infrastructure Survey Tool (IST)
- Cyber Infrastructure Survey Tool (CIST)
- Infrastructure Visualization Tool (IVT)

# Infrastructure Survey Tool (IST)

- Comprehensive / All Hazards
- 145 pages / 300 questions
- *Protective Measures Index*
- *Resilience Measures Index*



# IST Protective Measures Index

## Physical Security

- Access Controls
- Barriers
- CCTV
- Lighting

# IST Protective Measures Index

## Security Management

- Plans, Training, Exercises
- Background Checks
- Communications and Alerts
- Working Groups

# IST Protective Measures Index Security Force

- Staffing
- Training
- Equipment
- Command and Control

# IST Protective Measures Index

## Information Sharing

- Threat Information Sources
- Information Sharing Mechanisms

# IST Protective Measures Index

## Protective Measures

- Vulnerability Assessments
- Mitigation Strategies

# IST Resilience Measurement Index

- Preparedness
  - Awareness and Planning
- Mitigation Measures
  - Construction
  - Alternate Sites
  - Resources (Utilities, Communication, IT)

## IST Resilience Measurement Index

- Response Capabilities
  - Onsite and Offsite (LE, Fire, HAZMAT, EMS)
- Incident Management and Command Centers
  - EOC
  - DOC
- Recovery Mechanisms
  - Business Continuity Plans
  - Restoration Agreements (Utilities)
  - Recovery Time

# IST Results and Findings

- Argon National Lab
- Options for Consideration
- ECIP Dashboard



# Assessment Locations

- Library (Doheny)
- Student Center
- Dormatory
- Classroom Building
- HSC Building

# FACT SHEET

Office of Infrastructure Protection  
Protective Security Coordination Division

## Field Operations Branch



# Homeland Security

### Overview:

The Field Operations Branch (FOB) within the Office of Infrastructure Protection (IP) Protective Security Coordination Division (PSCD) facilitates IP's field activities in coordination with IP Divisions and other Department of Homeland Security (DHS) offices. IP has developed and maintained a robust operational field capability through the planning and execution of the Field Operations Branch (FOB) Protective Security Advisor (PSA) Program, providing assessments of nationally significant critical infrastructure known as Level 1 and Level 2 facilities, through Enhanced Critical Infrastructure Protection (ECIP) security surveys.

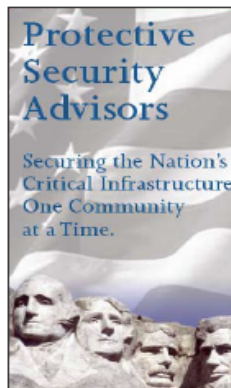
### Program Descriptions:

PSA Program – Protecting critical infrastructure is the PSA Program's primary mission support activity. Established in 2004, the PSA Program leads IP's efforts and is supported by other mission partners in this objective. Regional Directors and PSAs are security experts that serve as the link between State, local, tribal, and territorial organizations and DHS infrastructure mission partners. Regional Directors and PSAs assist with ongoing State and local critical infrastructure security efforts by establishing and maintaining relationships with State Homeland Security Advisors, State Critical Infrastructure Protection stakeholders, and other State, local, tribal, territorial and private sector organizations. Regional Directors and PSAs support the development of the national risk picture by conducting more than 1,000 vulnerability and security assessments each year to identify security gaps and potential vulnerabilities in the Nation's most critical infrastructure. Regional Directors and PSAs also coordinate training; support incident management; and serve as a vital channel of communication for officials and private owners and operators of critical infrastructure assets seeking to communicate with DHS.



Today there are 93 Regional Directors and PSAs, including 87 field deployed personnel, serving in 74 Districts in 50 States and one Territory. Because Regional Directors and PSAs are strategically dispersed across the US, they are often the first DHS personnel to respond to incidents that may require Federal intervention, especially those involving critical infrastructure. During incidents requiring Federal assistance and support, such as Hurricanes Ike and Gustav in 2008, the PSAs served as the Infrastructure Liaisons at the Federal Emergency Management Agency Joint Field Office and in the State and county Emergency Operations Centers, providing expert knowledge of the impacted infrastructure, maintaining communication with owners and operators, and prioritizing and coordinating response, recovery, and restoration efforts for critical infrastructure.

PSAs also work with the Federal Bureau of Investigation to conduct joint site visits and vulnerability assessments of critical infrastructure assets, and with the United States Secret Service to provide vulnerability assessments, security planning, and coordination during National Special



---

Security Events and other large scale special events, such as the 2009 Presidential Inauguration, and 2010 Super Bowl and Nuclear Security Summit.

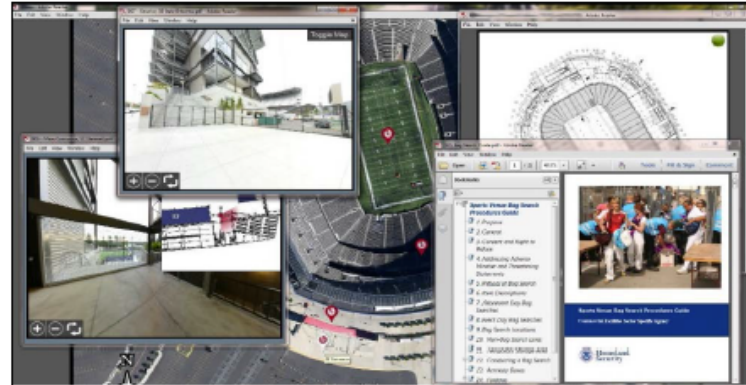
ECIP Security Surveys – The goals of ECIP security surveys are to assess the overall security postures and provide options for consideration to enhance protective measures at Level 1 and Level 2 facilities; inform facility owners and operators of the importance of their facilities and threats from terrorism; and develop strong relationships between critical infrastructure owners and operators, DHS, and Federal, State, and local law enforcement. To accomplish these goals, PSAs engage partners in activities including coordination and outreach, training and education, cataloging Level 1 and Level 2 security measures, and leveraging existing relationships with Federal, State, local, and private sector partners. The ECIP security surveys provide the ability to collect, process, and analyze facility assessment data and develop a detailed assessment of physical security, security management, security force, information sharing, protective measures, and dependencies. Data collected during the surveys is weighted and scored to develop ECIP metrics, conduct sector-by-sector and cross-sector vulnerability comparisons, identify security gaps, and track progress toward improving critical infrastructure security. Data from ECIP security surveys are provided to owners and operators in interactive ECIP Dashboards that enhance the ability to process and analyze facility data.





# Infrastructure Visualization Platform

The Infrastructure Visualization Platform (IVP) is a data collection and presentation medium that supports critical infrastructure security, special event planning, and response operations by integrating assessment data and other relevant materials. The platform provides immersive video, geospatial, and hypermedia data of critical facilities, surrounding areas, and transportation routes that assists security personnel in planning, protection and response efforts.



Examples of IVP capabilities. Courtesy of DHS.

IVP imagery captures are conducted in support of National Special Security Events; other special events; and the request of facility owners and operators, local law enforcement, and emergency response personnel via the local Protective Security Advisor (PSA). In support of special events, such as the Super Bowl, Presidential debates and inaugurations, and NCAA championship sporting events, the Office of Infrastructure Protection collaborates with the United States Secret Service, the Federal Bureau of Investigation, and other agencies to conduct IVP imagery collections. IVP data is also used to support the Regional Resiliency Assessment Program (RRAP) via the RRAP Multimedia Presentation, which includes an interactive version of the final Resiliency Assessment along with any supporting RRAP materials and documentation.

## Program Description

The IVP team consists of collection and production specialists who conduct IVP imagery captures. When conducting an imagery capture, the IVP team considers two viewpoints: hostile target and civil response. For the hostile target viewpoint in which a facility or building is viewed as a tactical objective, the team collects multimedia data to document approach and exit routes, use of lighting, visible and hidden entrances, loading docks, and parking garages. In considering the civil response viewpoint, the team collects data on obstructions and restrictions that would affect the approach of emergency response vehicles and equipment to the site and street/parking accessibility in proximity to building access points. Additional data includes significant assets in the area, such as exterior and interior critical support equipment (water valves, electrical shut-off panels, back-up generators, etc.), personnel emergency marshaling points, and control centers. Depending on the amount of data collected, the IVP team typically takes two weeks to produce the final product, which is a DVD containing the image captures, data, and analysis, and is provided to the facility representative, primary stakeholder of an RRAP, or special event security planning personnel. The final product assists these users in training, planning, and making rapid and informed incident preparedness and management decisions.

# JOINT PROVOST/ACADEMIC SENATE RETREAT

## Session #3

Campus Safety:  
Faculty Training and Resources  
FEEC Recommendations