

Critical Infrastructure Protection Conducting All Hazard Risk, Threat, and Vulnerability Assessments

Sponsored By Pierce County Emergency Management and
Tacoma Police Department with Setracon Inc.

How Safe is Your City?



When: January 24-27, 2011

Where: Tacoma PD Headqtrs

Time: 08:00 – 17:00 daily

TARGET AUDIENCE

Law Enforcement
Intelligence Analysts/Fusion Center Personnel
Fire
Homeland Security Liaisons
Emergency Managers
Crime Prevention Officers
Public Works Supervisors
Risk Managers
Managers and Operators of Critical Infrastructures

TO REGISTER:

Pierce County personnel should send an email to PCDEMTraining@co.pierce.wa.us with attendee's name, agency, and e-mail no later than January 14, 2011.

Some Backfill/Overtime funds are available to Pierce County Responders on a first-come, first-served basis. Request must be made at the time of registration for estimated dollars needed.

Out of County partners may register at any time and will be notified after January 14, 2011 regarding available seats.

PROGRAM HIGHLIGHTS

The Need for a Vulnerability Assessment	Analysis Preparation
Defining the Project	Mission Objectives
Threat Assessment/Definition	Prioritizing Facilities
Consequence and Target Identification	Site Surveys
Physical Protection Systems	Critical Interdependencies
Risk Analysis	Protection & Mitigation Upgrades
Incident Command	Final Report Structure
Comprehensive Field Exercise	

LOGISTICS: *This is a technical course. Attendees should come to the course prepared to receive a significant amount of information. A course book will be provided. Dress for the course is comfortable business casual. There will be four hours of practical exercise in a field environment on day three and attendees should dress appropriately. Attendance at all sessions is required. A certificate of training will be provided. There will be classroom amenities but lunch will not be provided.*

Critical Infrastructure Protection-Assessing Infrastructure Risk



How Safe Is *Your* Community
From a Criminal/Terrorist
Threat or a Natural Disaster?

Don't Wait to Find Out!

This comprehensive course provides an opportunity for personnel with a Critical Infrastructure protection mission to gain hands on experience and training in the skills, technologies, and best practices required for conducting a qualitative and quantitative, all hazards risk, threat, and vulnerability assessment. Further attendees will gain significant knowledge in identifying critical interdependancies and single points of failure thereby improving overall disaster resiliency.

Participants will gain knowledge in the following specific areas; Decisions and Risk, Planning for a Comprehensive Risk, Threat, and Vulnerability Assessment, Threat Assessment and Intelligence Operations to support an assessment including preparation of a threat report, Facility Characterization including consequence assessment, critical interdependancies, and evaluating existing physical protection systems. Further attendees will be introduced to SCADA System and Cyber System Vulnerabilities, Physical Protection Systems, Physical Protection Technologies including barrier systems, portal security, credentialing, camera systems, lighting, and other detection technologies. How to evaluate overall physical security system effectiveness through conduct of inspections, adversary pathing, and EASI modeling. Utilizing a mathematical formula for conducting a risk analysis, making recommendations that support risk reductions, and preparing a comprehensive final report. Lastly attendees will understand how a comprehensive assessment can support emergency response planning and disaster preparedness.

The following Federal and State Training Goals will be achieved by this Course:

- Develop and Sustain an Infrastructure Protection Programs
- Conduct/gather vulnerability analysis
- Locate, map, score, validate, prioritize and vet critical infrastructure data.
- Collect vulnerability assessment data and information
- Identify potential critical infrastructure protection strategies with the assessed infrastructure.
- Following a vulnerability analysis identify risk associated with critical infrastructure
- Collect additional vulnerability assessment data and information.
- Identify potential critical infrastructure protection strategies with the assessed infrastructure.
- Prioritize infrastructure and create (coordinate and write the state infrastructure) protection plan.
- Incorporate the NIMS into existing statewide education, training and exercise programs. Training will have two modules one that addresses NIMS, NIPP, and the NRF and correlates the findings of the vulnerability assessment into effective emergency response planning.

DAY 1

Session	Schedule	Topic
Registration	7:00am – 8:00am	Location TBD
Opening Remarks	8:00am – 8:30am	Workshop introduction and presentation of Critical Infrastructure Protection exercise
Session #1	8:30am – 9:30am	Decisions and Risk
BREAK	9:30am – 9:45am	Refreshments Provided
Session #2	9:45am – 11:30	Planning for a Risk Threat and Vulnerability Assessment
LUNCH	11:30am – 12:30pm	On your own
Session #3	12:30pm – 2:00pm	Threat Assessment and Intelligence Operations to Support a Risk Assessment
BREAK	2:00pm – 2:15pm	Refreshments Provided
Session #4	2:15pm – 3:15pm	Determining Consequence
Session #5	3:15pm – 4:15pm	Critical Interdependencies
Session #6	4:15pm – 5:00pm	Cyber/SCADA System Physical Security

DAY 2

Session	Schedule	Topic
Session #7	8:00am – 9:00am	Physical Protection Systems Concepts
Session #8	9:00am – 10:00am	Exterior Physical Security Systems Barrier Systems
BREAK	10:00am – 10:15am	Refreshments Provided
Session #9	10:15am – 11:00am	Exterior Physical Security Systems Lighting
Session #10	11:00am – 12:00pm	Exterior Physical Security Systems CCTV & Video Analytics
LUNCH	12:00noon – 1:00pm	On your Own
Session #11	1:00pm – 2:30pm	Interior Physical Security Systems Locks and Doors
BREAK	2:30pm – 2:45pm	Refreshments Provided
Session #12	2:45pm – 3:45pm	Interior Physical Security Systems Card Key Access Systems and Credentialing
Session #13	3:45pm – 5:00pm	Interior Physical Security Systems Interior Technologies

DAY 3

Session	Schedule	Topic
Session #14	8:00am – 9:30am	Security System Vulnerabilities
BREAK	9:30am – 9:45am	Refreshments Provided
Session #15	9:45am – 10:45am	Adversary Pathing, EASI Modeling, Estimating System Effectiveness
Session #16	10:45am – 11:45am	Calculating Risk and Risk Reduction
Session #17	11:45am – 12:00	Final Report Construct
Working LUNCH	12:00noon – 1:00pm	Practical Exercise Overview, Threat Brief, and Assignments
Session #18	1:00pm – 4:45pm	Deploy to Critical Infrastructure Facility and Conduct Assessment
Session #19	4:45pm – 5:00pm	Wrap-Up & Questions

DAY 4

Session	Schedule	Topic
Session #20	8:00am – 10:00am	Workshop Prepare Assessment Reports
Session #21	10:00am – 12:00pm	Group Report outs and Recommendations
LUNCH	12:00noon – 1:00pm	On your own
Session #22	1:00pm – 2:30pm	Interdependencies Exercise and Facilities Prioritization
BREAK	2:30pm – 2:45pm	Refreshments Provided
Session #23	2:45pm – 3:45pm	Utilizing Assessment Outcomes for Emergency Response, Disaster Preparedness, and Business Continuity Planning
Session #24	3:45pm – 5:00	Wrap-Up, Questions, and Issue Certificates

Taught by Nationally Recognized Speakers

Jeffrey A. Slotnick, CPP, PSP a Board Certified Security Management and Physical Security Professional is a nationally recognized security industry consultant with more than 28 years experience in providing professional development and training to security, law enforcement & military personnel, and conducting comprehensive Risk, Threat, and Vulnerability Assessments. Mr. Slotnick has extensive experience in conducting large scope assessments and has specific experience in the Public Works and Utilities Field. Mr. Slotnick is the President of Setracon Inc. an organization that provides advanced training to Federal, State, and local government entities. Mr. Slotnick is also a certified instructor for RAM-WSM Risk Assessment Methodology for Water Utilities, RAM-CSM Community Vulnerability Assessment Methodology, RAM-CiSM Critical Infrastructure Assessment Methodology, LE-VATSM Law Enforcement Vulnerability Assessment Teams, PAIR-PMTM Process for Assessing Infrastructure Risk and has trained thousands of law enforcement officers, utility personnel, engineers, emergency managers, and security consultants in methodologies for conducting Vulnerability Assessments. Jeff has personally supervised numerous comprehensive large scope Vulnerability Assessments for Counties, Cities, and Transportation Systems. Mr. Slotnick is currently on Faculty for ASIS International instructing the Physical Security Professional review course and at the Federal Law Enforcement Training Center (FLETC) where he instructs Physical Security at the Federal

HOWARD A. MOSTER, CPP, CRM, CFE, PSP Howard has more than 27 years experience in public law enforcement and corporate security. He is internationally recognized as an expert in *Physical Security* and Risk Assessments, is an instructor for the US Department of Homeland Security at The Federal Law Enforcement Training Center (FLETC); an Instructor at the University of Alberta; has co-authored three books, written many articles and is a sought after presenter and consultant. He holds the professional designation of Certified Protection Professional (CPP), holds a certification in Risk Management (CRM) from Simon Fraser University is a Certified Fraud Examiner (CFE) and Physical Security Professional (PSP). He has been qualified as an expert in physical & procedural security matters in court proceedings. He is the Senior Partner at Practical Protection Associates Inc. Edmonton, Alberta, Canada.

Phill leads The Banks (*Risk Mitigation*) Group in Vancouver, Canada. His security practice provides security program assessment, threat and risk mitigation strategies, security engineering design and strategic security planning services throughout North America and elsewhere. Phill served 25 years in federal law enforcement with the Royal Canadian Mounted Police specializing in security engineering design completing his career as the Officer-in-Charge, National Security Engineering and Electronic Security Programs. Phill is the Vice Chairperson, ASIS International Physical Security Council and frequently conducts workshops with respect to, threat and risk mitigation, security management and security technology programs. He is also a faculty member for the ASIS Physical Security Professional (PSP) certification review program.