THE PROTECTOR

A QUARTERLY NEWSLETTER

A MESSAGE FROM THE CHIEF:

THIS QUARTERLY NEWSLETTER IS PART OF THE PROTECTIVE DESIGN CENTER'S CONTINUING EFFORTS TO PROVIDE THE FEDERAL GOVERNMENT SECURITY COMMUNITY WITH INFORMATION RELATED TO PROTECTIVE DESIGN, ANTITERRORISM, PHYSICAL SECURITY, HARDENED STRUCTURES, AND ACCESS CONTROL.

SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIFS)

GENERAL INFORMATION

- A Sensitive Compartmented Information Facility (SCIF) is a designed space for the processing of Sensitive Compartmented Information (SCI). The SCI in its many forms must be protected from the threats of leakage by means of electromagnetic (EM) emanations, acoustic emanations, surveillance methods, and security events.
- The EM emanations can be produced from any electronic signal carrying medium, EM wave generation, or induced electronic signals. Examples are cables, circuitry, transducers, and other electrically conductive material.
- Acoustic emanations are all sound waves that have a path out of the SCIF. Examples are voice and amplified sound.
- Surveillance methods include microphones, cameras, optics, antennas, radio transmitters and visual observation.
- Security events include unauthorized entry, possession of personnel electronic devices, removal of SCI, duplication of SCI, and un-cleared access to SCI.

CONCERNS AND CONSIDERATIONS

- The risk of a faulty SCIF design or implementation is the compromise and leakage of classified information. In the case of a SCIF in use, this means that this risk can continue undetected for long periods of time. To complicate matters the SCIF is a system that is an array of complex planes, apertures and transmission lines. All of which can create a threat.
- The engineering and design of a SCIF requires an array of materials, systems, and techniques that must work in concert to nullify threats. To defeat the technical and security threats, the SCIF design and construction should be reviewed for validation by experts in the design and the technologies involved, and tested for functionality once deficiencies corrected. The requirements placed on OCONUS SCIFs add layers of complexity to a successful SCIF project.
- The Protective Design Center is the Army's Center of Expertise for SCIFs. The PDC works with projects for all agencies of the federal government and the military. See the "Sensitive Compartmented Information Facility (SCIF)" forum on the PDC website.

Read more…

PROTECTIVE DESIGN CENTER
SERVING THE NATION AND THE WORLD

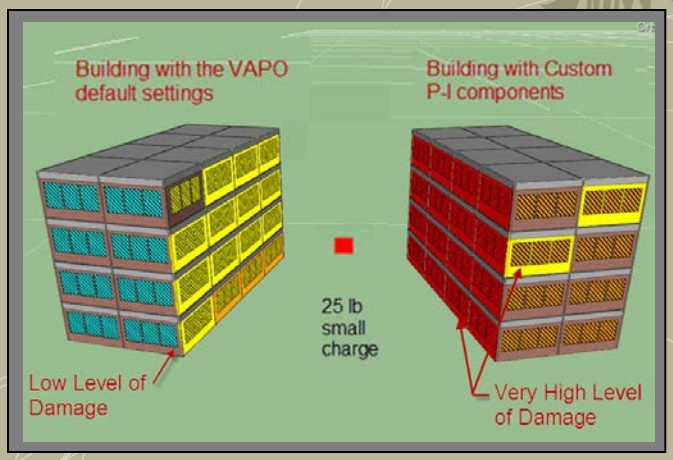
AVAILABLE SUPPORT SERVICES

Planning	• Criteria Development • AT Plan Development • Contingency Plan Development
Design	• Protective Design • Design of Hardened Structures • Blast Resistant Window Design • Access Control Point (ACP) Design • Chemical/Biological Protection & Design • SCIF and E3 Facility Design • Energy System Protection & Continuity
Review and Assess	• Risk and Vulnerability Assessments • Infrastructure Assessments • UFC Compliance Reviews/Assessments • Analysis of Hardened Structures • Blower Door (Building Leakage) Testing
Training	• Security Engineering and ACP Training • Blast Design Training

UNDERSTANDING THE COMPLEXITIES OF VAPO BLAST ANALYSIS

SAME BUILDING, VASTLY DIFFERENT RESULTS

The results of a blast analysis are only as good as the information that was used to develop the model on which the results are based. If the software defaults are used, the results can be vastly different than those achieved by using the actual building construction information. Different types of construction react differently to the blast pressures associated with the detonation of an explosive device. Therefore, there is a wide range of limits with respect to component failure. Inaccurate results can lead to a false sense of security or the pursuit of expensive retrofits that are unnecessary.



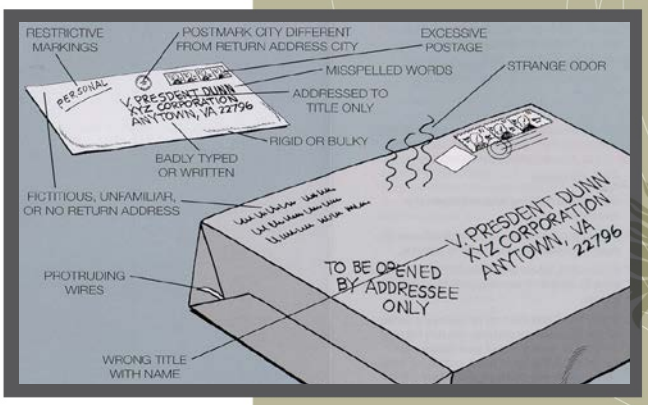
A discussion and slideshow illustrating the complexities of VAPO can be found at: https://pdc.usace.army.mil/newsletter/.

For questions or assistance with blast analysis and/or the use and application of VAPO, please contact:

Mr. Kelvin Chan, 402-995-2378, kelvin.t.chan@usace.army.mil or Mr. Matt Tomanek, 402-995-2382, mathew.t.tomanek@usace.army.mil

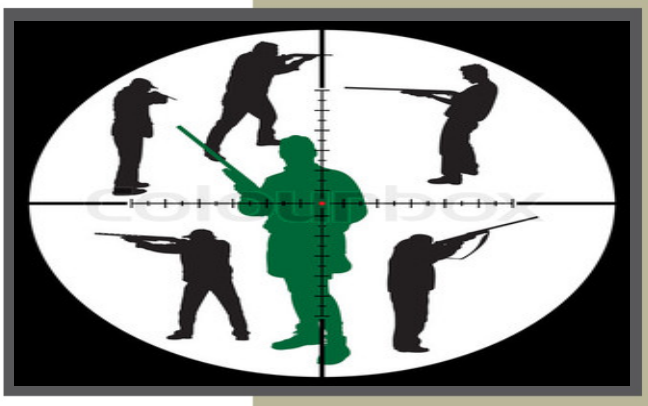
MAIL ROOM STANDARDS AND PROCEDURES

Protective measures can deter or prevent an aggressor's ability to execute certain tactics, but use of the postal system offers a degree of anonymity and safe distance that other tactics do not. Given the relative ease with which the mail and packages can be used to deliver explosives or biological agents, it is imperative that mail-handling personnel receive proper training in identifying suspicious packages. Adhering to all applicable standards for mail rooms will greatly enhance a facility's security posture. Examples include mail room location (outside wall away from occupied areas), construction, HVAC shutoffs, etc. Read more w/videos…



ACTIVE SHOOTER PREPAREDNESS

Incidents involving a lone active shooter are becoming more common. The motives often range from a disgruntled employee to a domestic dispute to mental health issues. A facility's ability to prevent and minimize the impacts of a catastrophic incident will depend largely on these factors: personnel training/awareness, proper physical security measures, and planning/preparedness. Examples of protective measures include access control, parking control, bullet resistant windows, safe haven locations, a response plan, and emergency egress. Read more w/video…



ANTI-RAM VEHICLE BARRIERS

The Protective Design Center maintains the U.S. Department of Defense (DOD) Anti-Ram Vehicle Barrier List. The barriers included on the list are marketed and manufactured by private corporations and have been successfully tested in accordance with Department of State SD-STD-02.01 and/or ASTM International F2656-07 standards**.** The Protective Design Center validates all test reports submitted for inclusion on the list, which is updated on a quarterly basis. The list is not an all encompassing list, but does include multiple listings for active and passive barriers. Active barrier categories include bollards, drop-arm beam, gate, net, post & beam, wedge, and cable. Passive barrier categories include bollard, cable, fence, and inertial. Please consult the DoD Anti-Ram Barrier List or contact a PDC representative for assistance. Test reports are treated as proprietary information and are exempt from public disclosure under the Freedom of Information Act (FOIA). Furthermore, PDC engineers can use the information to validate that barriers are selected and installed in a manner equivalent to that which led to the successful test results.

ANTI-RAM VEHICLE BARRIER SELECTION AND DESIGN

Ever wondered if your vehicle barriers are DOD certified, appropriate for your specific application, and designed and installed in a manner equivalent to which they were successfully tested and certified?

The following key steps will help ensure that your vehicle barriers provide the protection that they are intended to provide:

- Have experts review existing or proposed Access Control Point (ACP), Entry Control Facility (ECF), or protected area designs. Ensure compliance with all applicable standards. For the Army, this includes The Army Standard for Access Control Points and for Air Force and Navy it includes 4-022-01 *Security Engineering – Entry Control Facilities; Access Control Facilities*.

- Select vehicle barriers from the DOD Anti-Ram Vehicle Barrier List**.** These products are proven to defeat vehicle threats under the specific conditions identified for the barrier rating required. Consider environment, design basis threat vehicles, impact velocity range, method of deployment, controls, O&M, life cycle costs, etc. prior to and during solicitation of vehicle barrier products. Consulting with experts can greatly reduce construction and operational expenses and minimize ACP/ECF downtime.

- Ensure that the barrier design and installation will yield the same results as the "as tested" barrier product. Include expert review of the design and the shop drawings to ensure compliance. Through threat delay analysis, verify that the AVB location and operational method are conducive to design basis threat defeat. An engineering analysis of these often yields unexpected results and identification of additional vulnerabilities.

- Ensure that AVBs and related control systems operate safely in accordance with the Surface Deployment Distribution Command Transportation Engineering Agency AVB safety schemes. Perform a commissioning of AVBs and their control systems, and the AVB safety schemes. A properly conducted commissioning will often identify faults in the control system, equipment, and/or software. Commissioning should only be performed by knowledgeable, experienced personnel.

- Maintain barriers according to manufacturer's guidance. If maintenance is ignored, barrier systems won't provide protection when the need arises. Consider a maintenance contract if on-site maintenance is questionable.

Enlisting the support of experts during programming, design, selection, and commissioning could significantly reduce construction and operational expenses, limit overall liability exposure, and minimize ACP/ECF downtime.

The Protective Design Center provides an **Access Control Point/Entry Control Facility Training Course** that is intended for an interdisciplinary group including engineering planners and designers, as well as provost marshal/security and law enforcement personnel, and is intended for civilian and military personnel involved in security or engineering support of security. **Read more…**

COURSE OUTLINE

- Introduction/Overview
- ACP/ECF Criteria/Standards
- ACP/ECF Planning
- Threat Scenarios/Performance Standards
- Active Barrier Control Systems/Commissioning
- Electronic Security Systems Overview
- Lighting and Power
- Geometric Design
- Traffic Engineering Study
- Sizing ACP Features/Threat Delay Time
- ACP/ECF Signage and Pavement Markings
- Speed Management Strategies
- Limited Use and Pedestrian ACP's/ECF's
- Estimation of Costs

Next Class Tentatively Scheduled for Summer 2013

APRIL/MAY/JUNE 2013 VOL # 2 ISSUE # 3

SECURITY ENGINEERING CLASSES

UPCOMING CLASSES

Contracted:

- 6-10 May 2013 – Department of the Army*
- 24-28 June 2013 – USAREUR (Germany)*
- 8-12 July 2013 – Department of the Army*

* Army gets priority placement; non-Army pays tuition if seats are still available

Open Enrollment:

- 12-16 August 2013 – Open class at Fort Belvoir

To schedule a class, contact the Training Coordinator:

Ann Mittelsdorf, 402-995-2930, ann.m.mittelsdorf@usace.army.mil

To register for a class, contact the Registrar:

Katherine Barnett, 402-995-2393, katherine.d.barnett@usace.army.mil

Management:

Mr. Curt Betts, Chief, PDC 402-995-2376
Mr. Steve Carter, Chief, Security Engineering 402-995-2359

E: curt.p.betts@usace.army.mil

A: U.S. Army Corps of Engineers, Omaha District
ATTN: CENWO-ED-S (Mr. Curt Betts)
1616 Capitol Avenue, Suite 9000
Omaha, NE 68102-9000

W: https://pdc.usace.army.mil

US Army Corps of Engineers
BUILDING STRONG®

Protective Design Center

CONTACT INFORMATION:

Structural Hardening, Blast Analysis & Protective Design:
Mr. Eric Martin 402-995-2391

Blast Resistant Window/Door Design and Analysis:
Mr. Bill Veys 402-995-2379

Vulnerability Assessments and AT Plan Development:
Mr. Thomas Schuberth 402-995-2374

Infrastructure Assessments:
Mr. Bryan Cisar 402-995-2362

Access Control Point Design, Review, & Commissioning:
Mr. Brian Erickson 402-995-2394

Chemical/Biological Protection Design:
Mr. Ken Christenson 402-995-2361

Criteria Development:
Mr. Curt Betts 402-995-2359

Blower Door (Building Leakage) Testing:
Mr. Don Dittus 402-995-2364

SCIF and E3 Facility Design & Energy System Protection:
Mr. John Benefiel 402-995-2396