
Welcome to the
Joint Engineer Training
2017
JETC
Conference & Expo
SAME

2017 Joint Engineer Training Conference & Expo

Mission Operations & Resilience through Cyber/Infrastructure Security

Moderator: James Hagan

Partner, BBS Federal

Speakers:

- Corinne L. Murphy, P.E., PMP, DBIA

  Principal Project Manager, Weston Solutions, Inc.

- Peter A. Ciotoli, AICP

  Vice President, Weston Solutions, Inc.

SAFETY FIRST!

Please take note of the exits in case of an emergency.

Thank You to Our Sponsors!

SILENCE PLEASE!

Please silence your mobile phones.

CREDITS & PRESENTATIONS

Earn 1 PDH/ AIA credit for attending this session.

Where are the forms ? www.same.org/jetc

Presentations? www.same.org/jetc

Q&A & FEEDBACK

Please walk up to the mic for questions.

Questions will be addressed during the allotted time.

Rate our session in the JETC App.

2017 Joint Engineer Training Conference & Expo

Mission Operations and Resilience through Cyber/Infrastructure Security

worst case scenario: “destructive attacks focused on some aspect of critical infrastructure” and data manipulation “on a massive scale”

Admiral Michael Rogers,
Commander US Cyber Command
and Director NSA
May 9, 2017 testimony to Senate Armed Services Committee

Vital Infrastructure

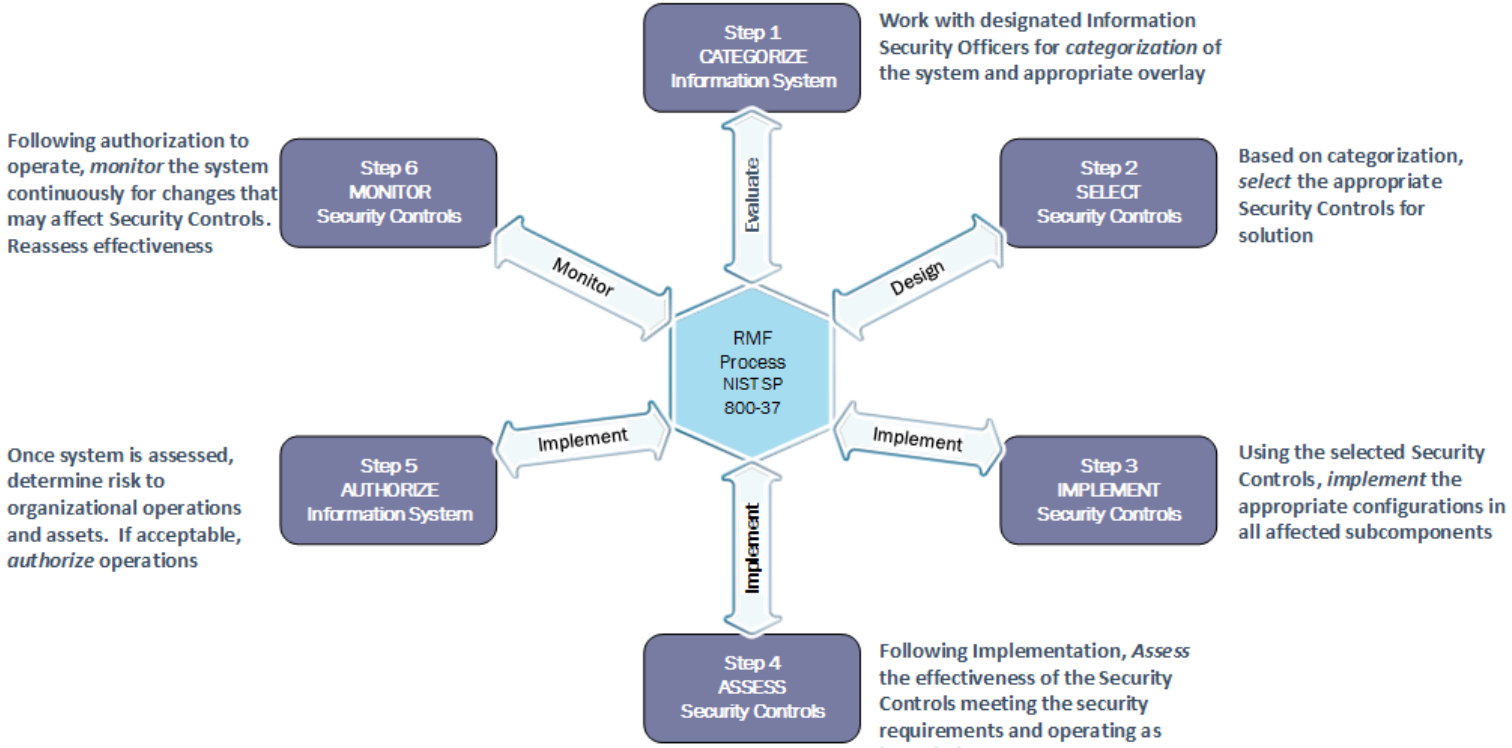
Threats

- Physical intrusion
- Technical incursion/attack
- Utility interruption
- Environmental disturbances
- Electro-Magnetic Pulse (EMP) threats

Vulnerabilities

- Out-dated systems
- Interconnected systems with weak links
- Co-located systems
- Re-purposed spaces inadequate for the new mission

Vulnerability & RMF Assessments



Potential Infrastructure Solutions

Physical Security
Technical Security
Utility Security
Environmental Security
HEMP Security

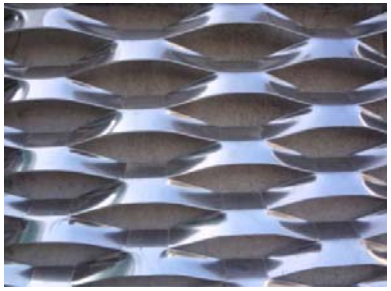
Physical Security

Physical Security Solutions

- Barriers
  - Gates & Fencing
  - Border Wall
  - Pop-up Barriers

Physical Security Solutions

- Hardening
  - Expanded Metal Walls
  - Rated Doors
  - Locks
- FEBR
  - Doors
  - Windows



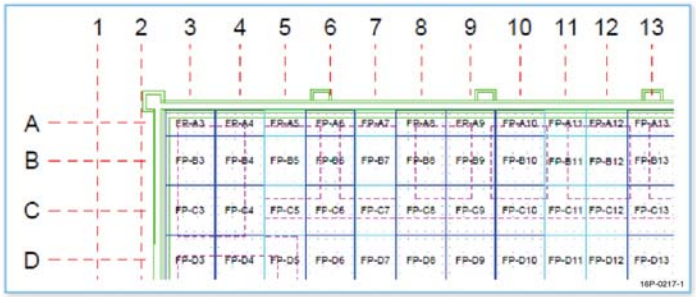
Physical Security Solutions

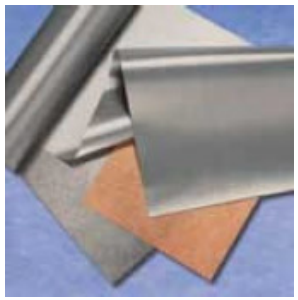
Objective	Responsibility	Solution	Challenges – Implementing & Maintaining
Physical			
Prevent or delay unauthorized personnel from gaining physical access to a location	Building/Physical Security Manager	**Barriers** • Walls • Gates • Pop-up Barriers	• Maintaining aesthetic of facility while increasing security posture • Providing security while maintaining operational capabilities and OPTempo • Modifying entrance/egress routings to accommodate changing traffic patterns and volumes
		Hardening • Locks • Expanded metal walls • Rated door assemblies	• Providing efficient access for those who need to enter space while providing a sufficient level of security • Re-evaluation of threats and vulnerabilities for new and repurposed buildings
		Forced Entry Ballistic Resistant (FEBR) • Doors • Windows	• Upgrading and strengthening older facilities to incorporate FEBR elements • Re-evaluating threats and vulnerabilities as mission evolves to identify needed upgrades and modifications

Technical Security

Technical Security Solutions

- Radio Frequency (RF) / Emanation Protection
  - Film / Foil
  - Dielectric breaks
  - Steel enclosures





Technical Security Solutions

- Intrusion Detection Systems
  - –CCTV
  - –PIRs & Microwave-based Motion Detectors
  - –Iris Scanners
  - –X-ray machines

Technical Security Solutions

- Information Assurance
  - Secure Technical Implementation Guidelines (STIG) Hardening

Technical Security Solutions

Objective	Respon-sibility	Solution	Challenges – Implementing & Maintaining
Technical Security			
Prevent electronic signals from leaving a space and being intercepted Prevent electronic signals from penetrating a space and influencing activities	Facility Security Officer (FSO)	**Emanation Protection** • TEMPEST • RF Shielding	• Inadequate maintenance of shielding and barriers; resulting in ineffective protection • Retrofitting existing spaces with effective shielding • Test, inspect and repair enclosures on a periodic basis • Monitoring/restricting future penetrations into the enclosure
Prevent unauthorized persons from gaining access to a location or capability		**Intrusion Detection Systems (IDS)** • Entry protection • Cameras • Alarms	• Old technology that is susceptible to intrusion or tampering • Old technology that is incompatible with updated technology
Prevent unauthorized persons from gaining electronic access to a network		**Information Assurance** • STIG Hardening	• Managing classified and non-classified data • Managing hybrid network communication system • Hardening a vast network with thousands of access points • Considering expansion capability of the system as needs evolve

Utility Security

Utility Security Solutions

- Continuous Power
  - Conditioned power
  - Uninterruptible power supplies (UPS)
  - Generators

Utility Security Solutions

- HVAC
  - Redundant Systems
  - Entry-resistant
  - Inspectable

Utility Security Solutions

- Industrial Control Systems

Utility Security Solutions

Industrial Control Systems

Graphic courtesy of MG T. Harrison

Utility Security Solutions

Objective	Respon-sibility	Solution	Challenges – Implementing & Maintaining
Utility Security			
Provide uninterruptible utilities to personnel and key infrastructure	Building Facilities Manager & Energy Manager	**Power** • Conditioned power • Uninterruptible power supply (UPS) & Generators	• Interconnected Power grids introduce vulnerabilities • Coordinating Energy security and Energy independence measures • Performing periodic system-wide vulnerability analyses
		HVAC • Filtration systems • Physical Barriers	• Interconnected HVAC systems introduce vulnerabilities • System serving secure & non-secure areas • Need for redundancy • Performing periodic system-wide vulnerability analyses
Provide remote control of critical SCADA systems and prevent tampering of critical systems by hostile elements		**Industrial Control Systems**	• Interconnected utility and control system introduce vulnerabilities • Portions of a utility system may be damaged or destroyed so control system need flexibility

Environmental Security

Environmental Security

- Chemical/Biological/Radiological/Nuclear Detection, Protection, Remediation
  - Real-time Monitoring
  - Bio and Rad Filters
  - Decontamination
- Potable Water
  - Real-time Monitoring
  - Redundant Systems

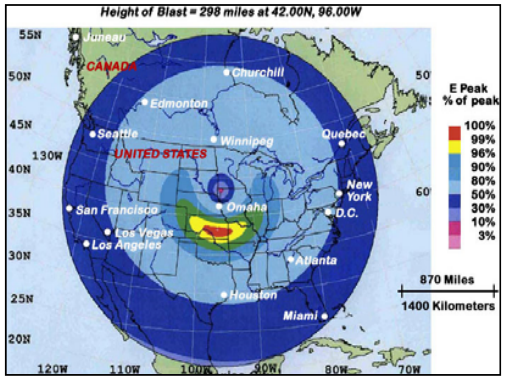
Environmental Security

Objective	Responsibility	Solution	Challenges – Implementing & Maintaining
Environmental Security			
Prevent disruption due to chemical, biological, radiological or E agents	Facility Environmental Manager	**CBRE** • Protection • Detection • Remediation	• Quickly realize if contamination is present and protect personnel • Provide safe shelter capability in critical locations
Provide sufficient quantity and quality of drinking water		**Potable Water** • Protected supplies • Constituent monitoring	• Supplies may be interrupted by emergency situation • Bad actor may seek to contaminate supply • Public water supplies are interconnected. • Local water supplies may have seasonal/permanent yield limitations

HEMP Security

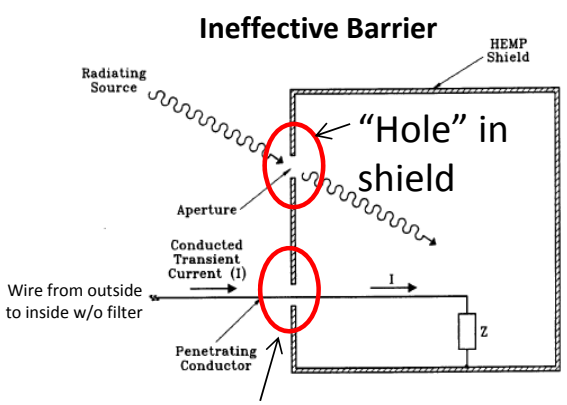
Electro-Magnetic Pulse (EMP)

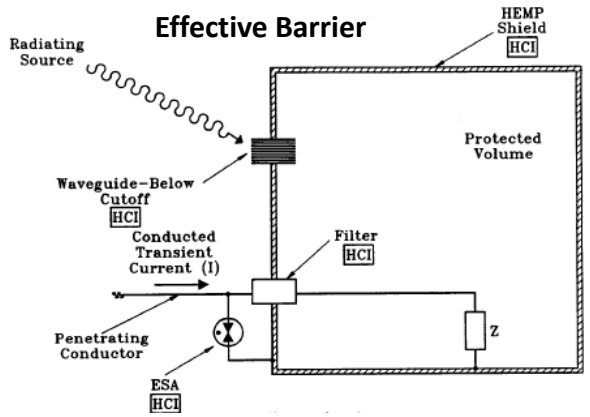
- High Altitude ElectroMagnetic Pulse -Exoatmospheric nuclear detonation produces intense electromagnetic field
  - An EM field from a high altitude burst creates three types of pulses which couple to wires and produce different waveforms
  - These threats can couple to ANY lines exposed to the threat field (outside the HEMP barrier)
    - Overhead power and telephone lines
    - Distribution power lines inside building
    - Control lines inside building



Electro-Magnetic Pulse (EMP) Security

- HEMP evaluation, design & repair
- Hardness Maintenance/Hardness Surveillance (HM/HS) implementation





Electro-Magnetic Pulse (EMP) Security

Objective	Responsibility	Solution	Challenges – Implementing & Maintaining
Electro-Magnetic Pulse Security			
Prevent high-altitude electromagnetic pulses (HEMP) from disrupting key systems	Operations Director	**HEMP** • Evaluation of HEMP Volumes • Design • Repair	• Determining those systems that are vital during an emergency • Retrofitting HEMP volumes into active spaces • Inspecting and maintaining effectiveness of the volumes as technology and missions evolve
		Hardness Maintenance/Hardness Surveillance (HM/HS) Programs	• Maintaining the effectiveness of HEMP volumes over time • Educating users and maintainers about the impacts of their actions on volume effectiveness • Assuring no new penetrations have been made

Conclusions

- Cyber Security ⟷ Infrastructure Security
- Holistic evaluation of threats and vulnerabilities
- Distributed responsibility for security