

Ready for the One-Year Blackout?



Protecting America Against
“Permanent Continental Shutdown”
From Electro-Magnetic Pulse Events

photo: composite of SOHO (ESA & NASA) + other art

Copyright 2009 by Instant Access Networks, LLC

**How the InfraGard National EMP SIG can serve
The Ashburn Data Center RRAP
Ashburn, May 28, 2015**

By Charles Manto
EMP SIG Chair, InfraGard National

EMP SIG ((o)))

Education. Communication. Power. Resilience.

Outline

- Purpose of InfraGard National EMP SIG
- Updates on high-impact threats, e.g. EMP
 - Supply chain (vertical and horizontal)
 - Network elements more exposed (POPs)
 - Failure of key suppliers will compel your resilience
- How you can address high-impact threats here
- How to save or find \$
- Bibliography

Outline -- Specifics to Save \$

1. Protecting key 10% saves up to 85% of economic damage
2. Triage – a tiered civilian approach to an EMP rating system calibrated from MIL SPECs
3. Total systems approach w future in mind
4. Leverage OPM
5. Examples of mitigation methods

National InfraGard EMP SIG

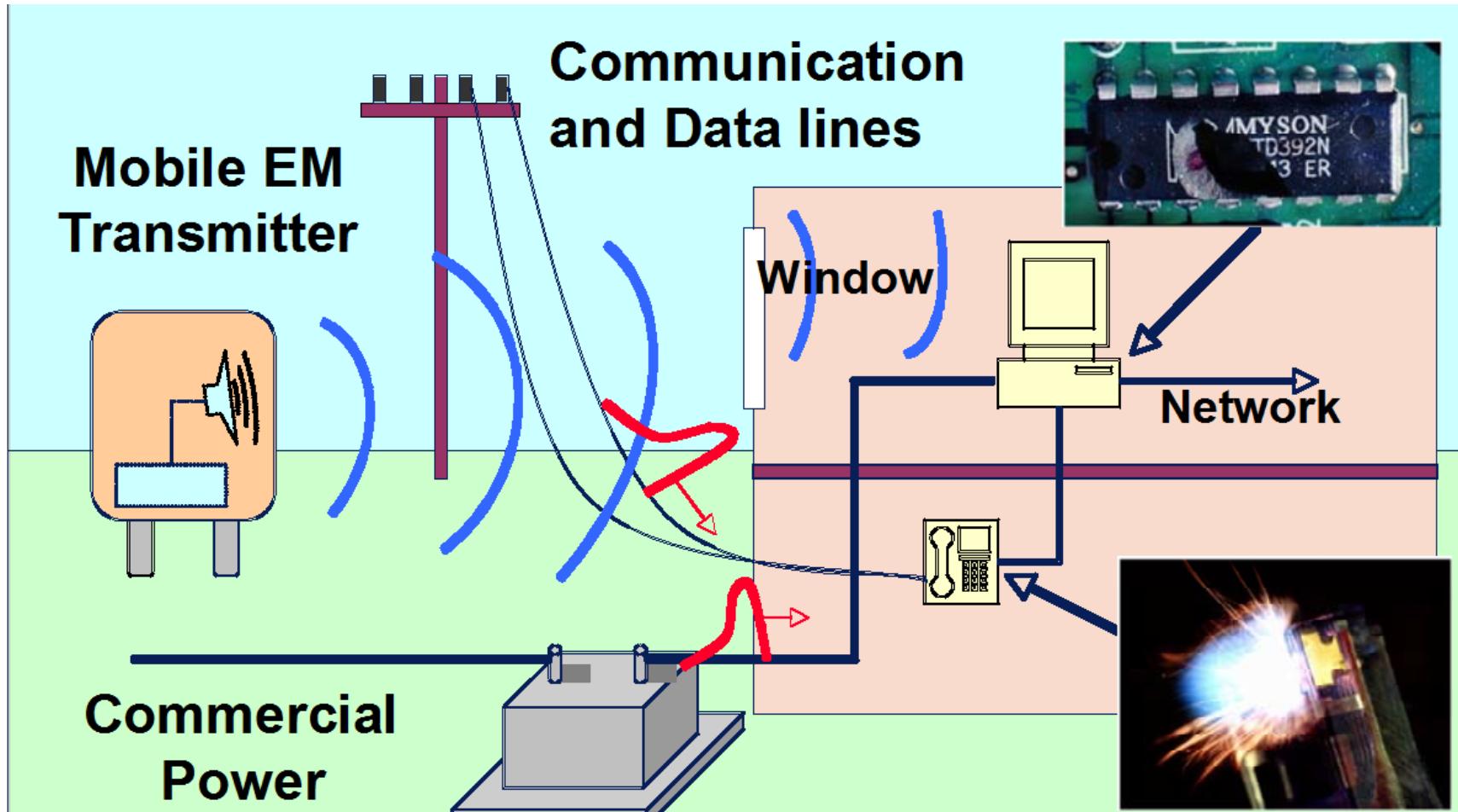
- Covers all high-impact low-frequency events that would cripple national infrastructure for > month
 - Special focus on electromagnetic pulse and GMD
- Purpose: assist local communities to enhance their resilience through local infrastructure & resources
 - Provides workshop & tabletop exercise programs
 - Provides panels of top experts
- Facilitates private sector discussion (FOUO-public)
- Supports events, e.g. NDU, DuPont Summit, August 8 EMP SIG JHUAPL meeting , Space Weather Workshop

IEMI and Frugal Attackers

- “Bad actor” terrorist, criminal or unethical competitors pick easy targets:
 - Your and your supply chain’s facilities
 - Your critical environment (power grid, water...)
 - Exposed elements (POPs, remote, less secure)
- Leverage space weather, cyber attacks...
 - See new National Space Weather Strategy
 - Comments due May 29, 2015
 - <http://www.dhs.gov/national-space-weather-strategy>

IEEE Standard 1642-2015

IEEE Recommended Practice for Protecting Publicly Accessible Computer Systems
from Intentional Electromagnetic Interference (IEMI)
Quoting Proc. 1st Asia-Pacific Symposium on EMC, 2008.



Frugal Defenders Save \$

- Save 85% of loss by protecting critical 10%
- Triage 4-tier protection system (see rating sys)
- Use all system full life cycle design (see pat.)
 - All-hazards resilience (other EM, cyber, physical)
- Use independent testers (sort good vendors)
- See examples (1000 times MIL SPEC, low cost)
- Use EMP fast “inferential detectors”
- Leverage other resources and funding

Savings with Shielding

From Sage EMP Assessment Study Sep '07

Exhibit 9: Total economic loss with and without shielding

	<i>Post-EMP capacity with shielding</i>			<i>Post-EMP capacity without shielding</i>		
	Low case	Middle case	High case	Low case	Middle case	High case
Total lost value of economic activity (billions)	\$9	\$30	\$586	\$34	\$212	\$771
Total lost value as share of annual regional gross domestic product	1.7%	5.7%	111.0%	6.5%	40.0%	147.0%
Total lost value as share of annual national gross domestic product	0.1%	0.3%	5.3%	0.3%	1.9%	7.0%

Civilian EMP Rating System

Instant Access Networks, LLC devised the Four-level EMP Rating System™ to show ranges of protection that may be relevant to various elements (power, data, communications) in a 4 level system-wide protection method where level three meets or exceeds various MIL SPECs for EMP and TEMPEST requirements:

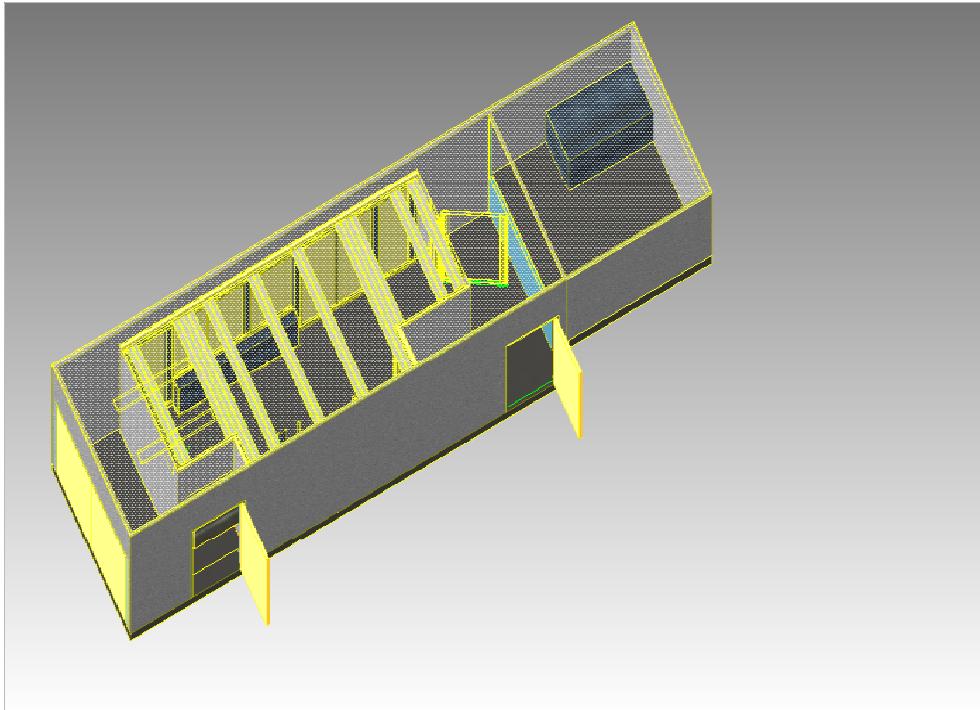
IAN LEVEL	Base Shield	Compare to MIL SPEC 188-125		
		1KHz- 10 MHz (ea 20 dB is a factor of 10)	10 MHz-1GHz	1GHz-10GHz (-10 series only)
EMP 4	140 dB	60dB above MIL SPEC to 1KHz	140 dB (60 dB above MIL SPEC)	140 dB
EMP 3	100 dB	20dB above MIL SPEC to 1KHz	100 dB (20 dB above MIL SPEC)	100 dB
EMP 2	60 dB	20dB below MIL SPEC to 1KHz	60 dB (20 dB below MIL SPEC)	60 dB
EMP 1	30 dB	50dB below MIL SPEC to 1MHz	30 dB (50 dB below MIL SPEC)	30 dB

Modular Mitigation Strategies: 32' EMP Trailer and GMC Pickup (CGVW <26,000 lbs)



Modular & Scalable Mitigation Strategies

IAN's EMP Protected Mobile Command Center



Modular Mitigation Strategies

- EMP Transportable pods:
 - Deploys one or 100's at a time
 - Stackable and stealthy
 - Deploys in, next, on or without buildings
- Protected modules can include:
 - Network management
 - Power management
 - Data storage
 - Critical communications
 - SCADA
 - Other critical infrastructure

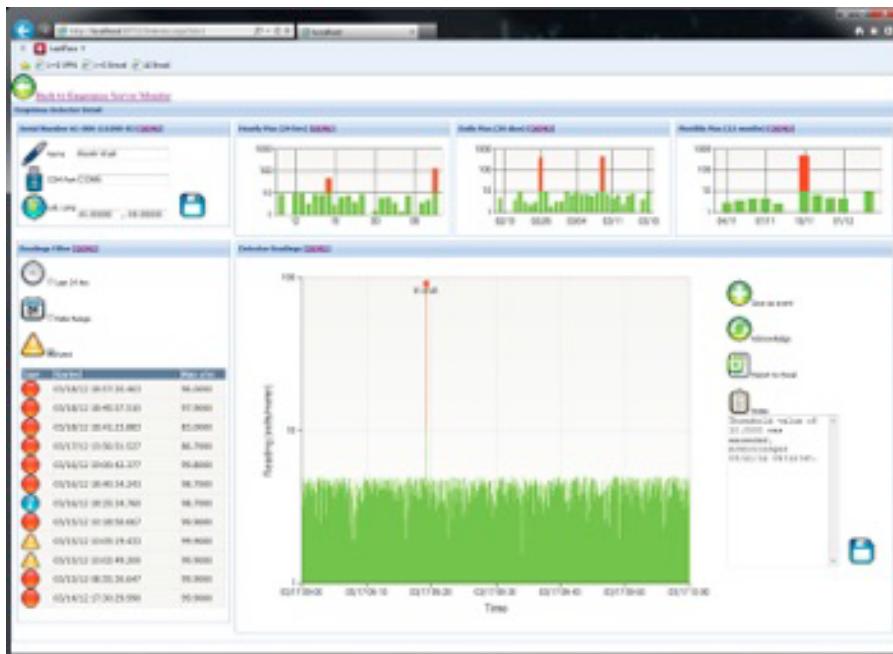


EMP Safe Micro Grids





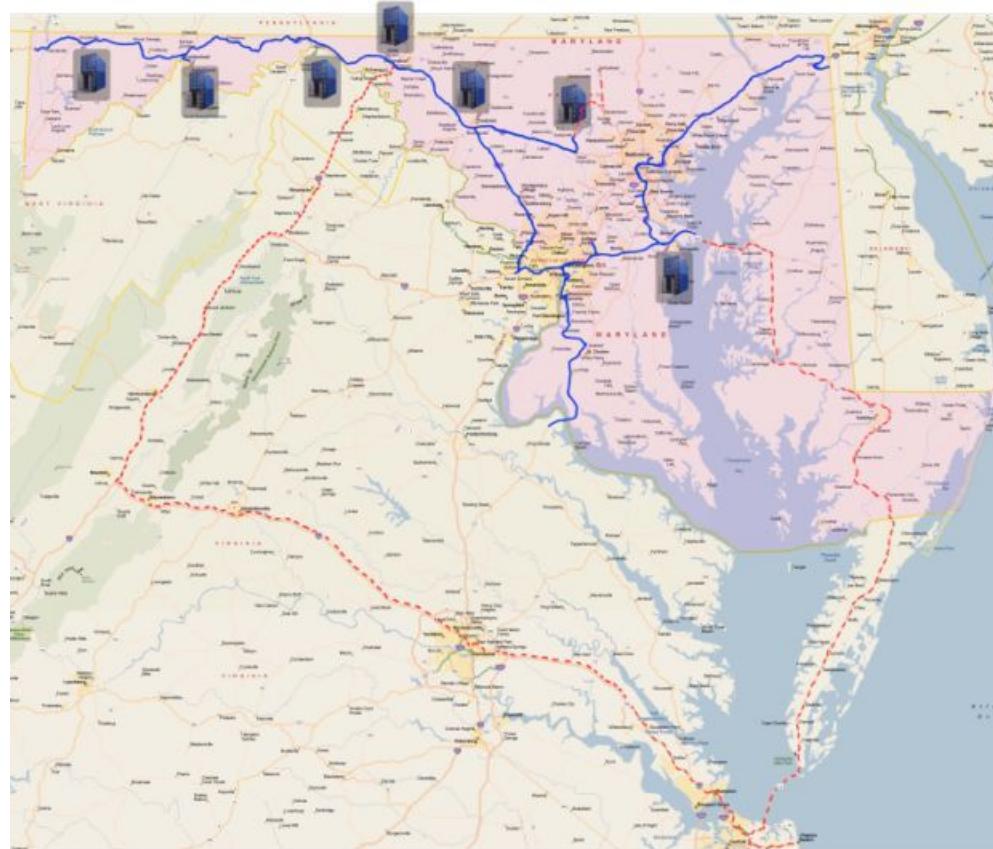
Emprimus InferentialDetector™



Data report from EMP
Detector that senses
signals at 2 nanoseconds
ranging from 100-100,000
volts per meter.

Networked Business Continuity Parks™

- Property / ROW by:
 - Local governments
 - Hospitals
 - Universities
- Cash provided by private sector
- Leverages grants by strong local match



Protect Critical Infrastructure
Renewable Energy:
Wind, Solar, Next Generation
Communications: Fiber Optic, 911 Centers
Computing
Water
Food
Medical
Manufacturing
Mobile Command
All-Hazards
Finance



EMP-Safe, Networked Business Continuity Parks™
Turn-key, EMP-Safe Communities
No Cash - In-Kind Match
Private/Public Partnerships

— Phase One
- - - Phase Two



Implications for Planning

- Qualitatively different disaster since can become high-impact
- Longer duration and broader area disaster factors
 - Outside help may not be available for months
 - Key supplies including power unavailable for months
 - Local sustainability mandatory (diverse power from self)
 - Without protection, interoperable tools won't operate
 - Stakeholders must include those who invest or fund infrastructure (e.g., gov't, utilities, communications co's)
- Work w supply chain and local/state gov't
- Mitigation enhances economic development

EMP Planning in NFPA 1600

Disaster/Emergency Management & Business COOP Includes EMP Plans and Mitigation

- CH 1 Business COOP, public & private
- CH 5 Comprehensive program elements
 - 5.3.2 Hazards to be evaluated:
 - Natural (including geomagnetic storms in #1b ix)
 - Human caused (accidental and intentional)
 - Includes EMP in #2b.ix
 - Technological-caused events
 - 5.3.3 Entity shall conduct an impact analysis
 - Health and safety
 - COOP
 - Economic
- See <http://www.nfpa.org/assets/files//PDF/CodesStandards/1600-2007.pdf>
- Work with public safety and local government groups (PTI) to implement

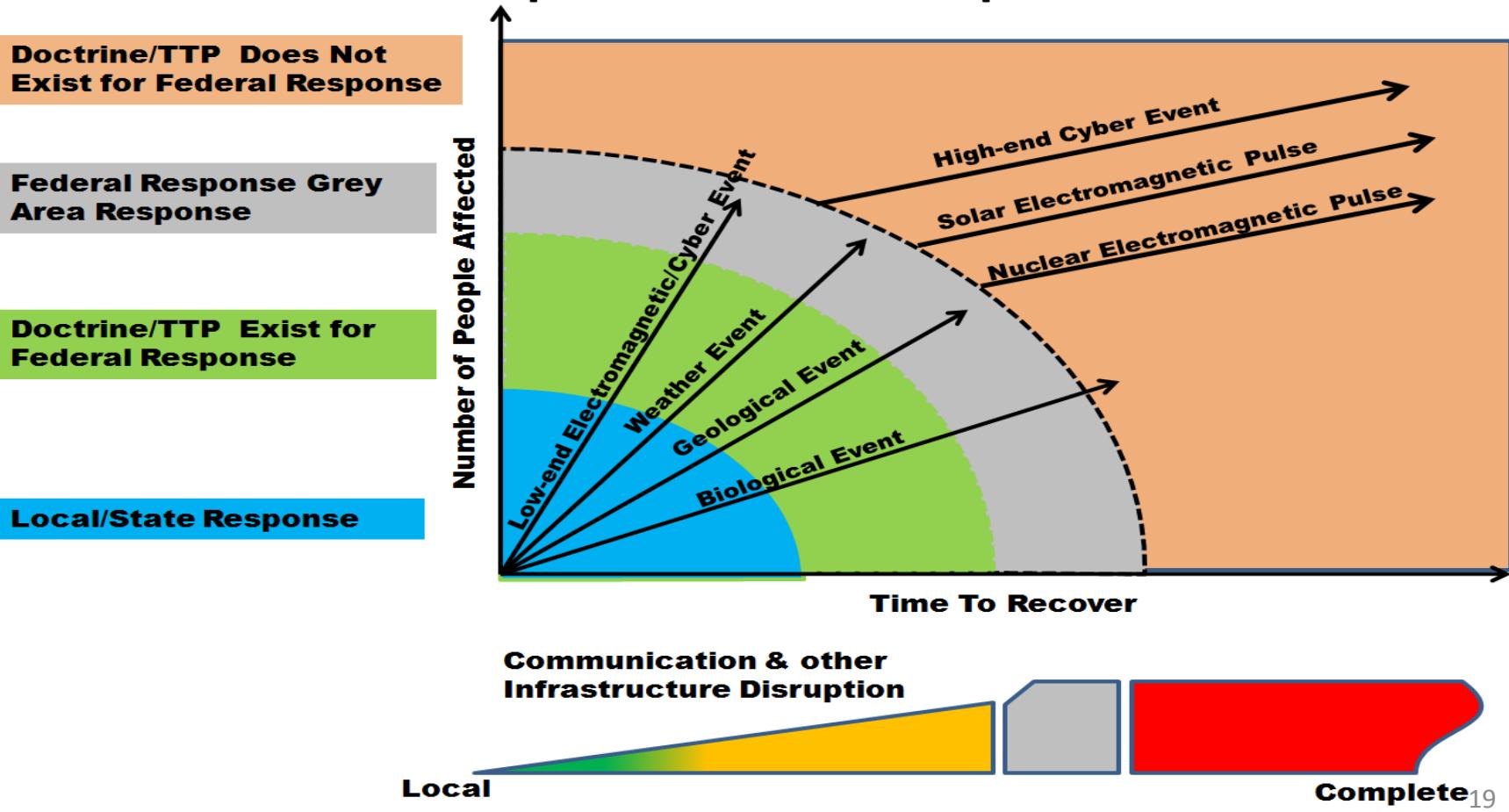
FIPS, NIST SP 800-53 Trigger

- **“A newly identified, credible, information system-related threat to organizational operations and assets, individuals, other organizations, or the Nation is identified based on intelligence information, law enforcement information, or other credible sources of information”**
- **“Triggers the immediate need to assess the security state of the information system and if required, modify or update the current security controls” (Sec 3.4, pp. 27-28)**

The Big Disasters We Ignore

Chart by Colonel Caton, US Army War College reviewing “In The Dark: Military Planning for a Catastrophic Critical Infrastructure Event” held 28-30 September 2010.

Catastrophic Event Spectrum



Thank You

For more information contact:

Chuck Manto, President

Instant Access Networks, LLC

Email: cmanto@stop-EMP.com

Phone: (410) 991-1469

EMP SIG ((•))

Education. Communication. Power. Resilience.

Bibliography

- [http://domesticpreparedness.com/
Infrastructure/Building Protection/
Electromagnetic Pulse Triage
%26 Recovery /](http://domesticpreparedness.com/Infrastructure/Building_Protection/Electromagnetic_Pulse_Triage_%26_Recovery /)
- <http://joom.ag/WM7b>
- **United States Patent 8,849,595**
 - *Manto , et al. September 30, 2014*

IEEE Std 1642™-2015

**IEEE Recommended Practice for
Protecting Publicly Accessible
Computer Systems from Intentional
Electromagnetic Interference (IEMI)**

Sponsor:
Standards Development Committee
of the IEEE Electromagnetic Compatibility Society

Approved 26 January 2015

IEEE-SA Standards Board
Copyrighted and Authorized by IEEE. Restrictions Apply

MIL SPEC 188-125 Series

(background from Wikipedia article)

- Faced with "past technical deficiencies in telecommunications systems and equipment and software...that were traced to basic inadequacies in the application of telecommunication standards and to the lack of a well defined...program for their review, control and implementation", the [U.S. Department of Defense looked to develop a series of standards that would alleviate the problem.\[1\]](#)
- By 1988, the [U.S. Department of Defense \(DoD\) issued Instruction 4630.8 \(reissued in 1992, 2002, 2004\) stating its policy that "all forces for joint and combined operations be supported through compatible, interoperable, and integrated Command, Control, Communications, and Intelligence systems. ...\[and that all such\] systems developed for use by U.S. forces are considered to be for joint use." \[2\]](#) To achieve this the [director of the Defense Information Systems Agency \(DISA\) is charged with "developing information technology standards to achieve interoperability and compatibility...\[and ensure that all\] systems and equipment shall conform to technical and procedural standards for interface, interoperability, and compatibility".\[2\]](#)
- The MIL-STD-188 standards were created to "address telecommunication design parameters based on proven technologies." [2] To ensure interoperability, DISA made these standards mandatory for use in all new DoD systems and equipment, or major upgrades.
- The mandatory use of these standards will aid significantly in achieving standardization and result in improvements in availability, maintainability, reliability, and supportability. This, in turn, will enhance lifecycle configuration management and logistic support with subsequent reductions in life cycle costs. [1]
- [125A - High-Altitude Electromagnetic Pulse \(HEMP\) Protection For Ground-Based Facilities Performing Critical, Time-Urgent Missions](#)

HIGH-ALTITUDE ELECTROMAGNETIC PULSE (HEMP) PROTECTION
FOR GROUND-BASED C4I FACILITIES PERFORMING CRITICAL,
TIME-URGENT MISSIONS (Validated April 2005) **MIL-STD-188-125**

4. As a result of a Joint Chiefs of Staff action, standards for all military communications are now being published in a MIL-STD-188 series of documents. The MIL-STD-188 series is subdivided into a MIL-STD-188-100 series, covering common standards for tactical and longhaul communications; 5. This two-part document contains technical requirements and design objectives for high altitude electromagnetic pulse (HEMP) protection of ground-based systems and facilities that are nodes in HEMP-hardened networks for performing critical and time-urgent command, control, communications, computer, and intelligence (C4I) missions. This part 1 of the document addresses HEMP hardening for fixed facilities; Part 2 addresses transportable systems. The requirements are stringent, in order to avoid both damage and functional upsets that prevent mission accomplishment within operationally prescribed timelines. The standards apply uniformly to all systems and facilities in the end-to-end chain, since disruption of a single node may result in network failure.

HANDBOOKS

DEPARTMENT OF DEFENSE

MIL-HDBK-419 – Grounding, Bonding, and Shielding for Electronic Equipment and Facilities

MIL-HDBK-423 –Fixed Facilities Implementation of MIL-STD-188-125-1 is supported by MIL-HDBK-423, "High-Altitude Electromagnetic Pulse (HEMP) Protection for Fixed and Transportable Ground-Based Facilities, Downloaded from <http://www.everyspec.com>

MIL-STD-188-125-2

Volume I: Fixed Facilities." The handbook also includes planning, management, logistics, and data requirements for HEMP protection acquisition programs and hardness maintenance/ hardness surveillance requirements for operational systems and facilities. Some sections of MIL-HDBK-423, Volume I, are also applicable to MIL-STD-188-125-2. References to sections of MILHDBK-423 are made within this standard, where applicable.

EMP SIG Milestones

- Dupont Summit Tech Policy 2012-2014 Conferences
- Published annual proceedings, “High Impact Threat” series through Westphalia Press & Amazon, Kindle)
 - Posted live videos (also on YouTube)
<http://www.ipsonet.org/conferences/the-dupont-summit/dupont-summit>
- NOAA Space Weather Workshop, Boulder, CO each April
- Table top exercises for distribution to states and counties
- Publish: DomPrep http://www.domesticpreparedness.com/Infrastructure/Cyber_%26_IT/Solar_Storm_Near_Miss_%26_Threats_to_Lifeline_Infrastructure/

EMP SIG ((•))

ElectroMagnetic Pulse Special Interest Group

The EMP SIG addresses any high-impact low-frequency threat that could cause long-term nationwide collapse of critical infrastructure. These threats include EMP, extreme space weather, cyber attacks, coordinated physical attacks or widespread pandemics. The EMP SIG provides trusted communications and information for InfraGard members active in any critical infrastructure in any community to enhance planning, mitigation and sustainable infrastructure. The EMP SIG continues to attract leading subject matter experts who have agreed to make themselves available for local InfraGard chapters that may need their special guidance.

The ultimate goal of the national EMP SIG is to assist local communities to enhance their own sustainability with a special emphasis on developing local infrastructure capacity from areas as diverse as local power generation and storage to local food production. Liaison panels are forming across various infrastructure silos to foster discussion and action across subject matter specialities and community organizations.

InfraGard's EMP SIG plans to continue its role in fostering public/private cooperation in a comprehensive "all-of-nation" approach to disaster mitigation and planning. InfraGard members may join the EMP SIG on the InfraGard secure website. To join InfraGard and have access to the secure site, apply on the home page of www.InfraGard.net.

