



[About](#) [Contact](#) [Contribute](#)

<https://publicintelligence.net/dhs-facilities-guidelines-emp/>

DEPARTMENT OF HOMELAND SECURITY

DHS Electromagnetic Pulse (EMP) Protection and Restoration Guidelines for Equipment and Facilities

August 13, 2017

Search ...

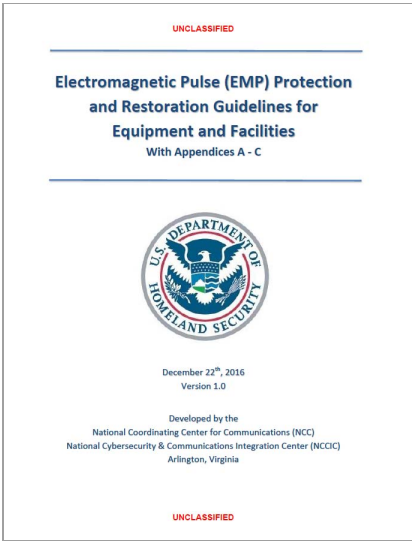
Follow Us



The following guidelines were obtained from the website of the [Infragard EMP Resource Center](#).

Electromagnetic Pulse (EMP) Protection and Restoration Guidelines for Equipment and Facilities With Appendices A - D

Page Count: 96 pages
Date: December 22, 2016
Restriction: None
Originating Organization:
Department of Homeland Security,
National Cybersecurity and
Communications Integration Center
File Type: pdf
File Size: 9,976,690 bytes
File Hash (SHA-256):
03E91F9B3F25E403B674B5B5C52B
03A632870E8EDDE53CBD748A5816
A9B3E9A8



[Download File](#)

This document provides recommendations for protecting and restoring critical electronic equipment, facilities and communications/data centers from:

ADVERTISEMENT

Categories

- Documents
 - [Afghanistan](#)
 - [Africa](#)
 - [African Development Bank](#)
 - [African Union](#)
 - [Botswana](#)
 - [Côte d'Ivoire](#)
 - [Djibouti](#)
 - [Egypt](#)
 - [Ethiopia](#)
 - [Gabon](#)
 - [Guinea](#)
 - [Kenya](#)
 - [Liberia](#)
 - [Libya](#)
 - [Mali](#)

- (1) High Altitude EMP (HEMP)
- (2) Surface-burst Source Region EMP (SREMP) fields propagating outside of the radiation region
- (3) Currents induced on undersea cables and long lines by solar storm generated geomagnetic disturbances (GMDs)
- (4) Intentional Electromagnetic Interference (IEMI) from nearby sources such as Electromagnetic (EM) weapons (also known as Radio Frequency (RF) weapons).

Collectively, these will be called by a general term in this document: “EMP”. However, it should be recognized that nearly all of the protection recommended in this document is for the frequency range above 10 kHz, which is the frequency range for E1 HEMP, SREMP and IEMI. A presentation describing the background, characteristics and effects of EMP is included in the Appendices to this document.

There are four DHS EMP Protection Levels defined herein, as outlined in Table 1. These levels were initially developed for use by the federal continuity community, such as for the Continuity Communications Managers Group, but are also applicable to any organization that desires to protect its equipment, facilities, and services against EMP threats.

In addition to making recommendations on how to physically protect electronic equipment from EMP, this guide provides guidance on how to help ensure communications and information systems (and their supported missions) can continue to function (or be rapidly restored) after one or more EMP events. Hence, Appendix C contains information on priority service programs (like GETS, WPS, and TSP) as well as on the SHARES alternate communications service that can be used to support critical missions and to facilitate and coordinate restoration activities.

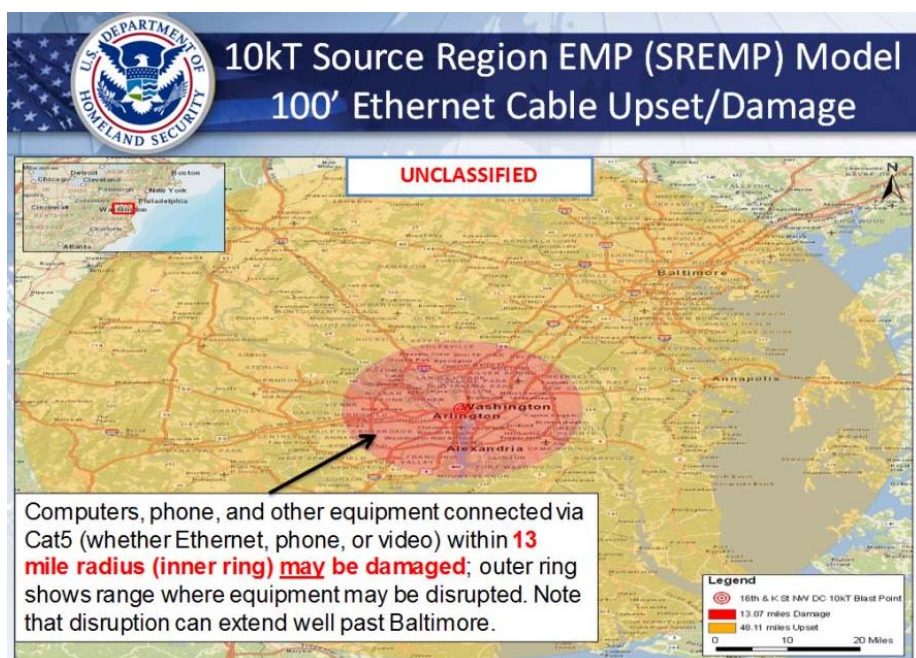
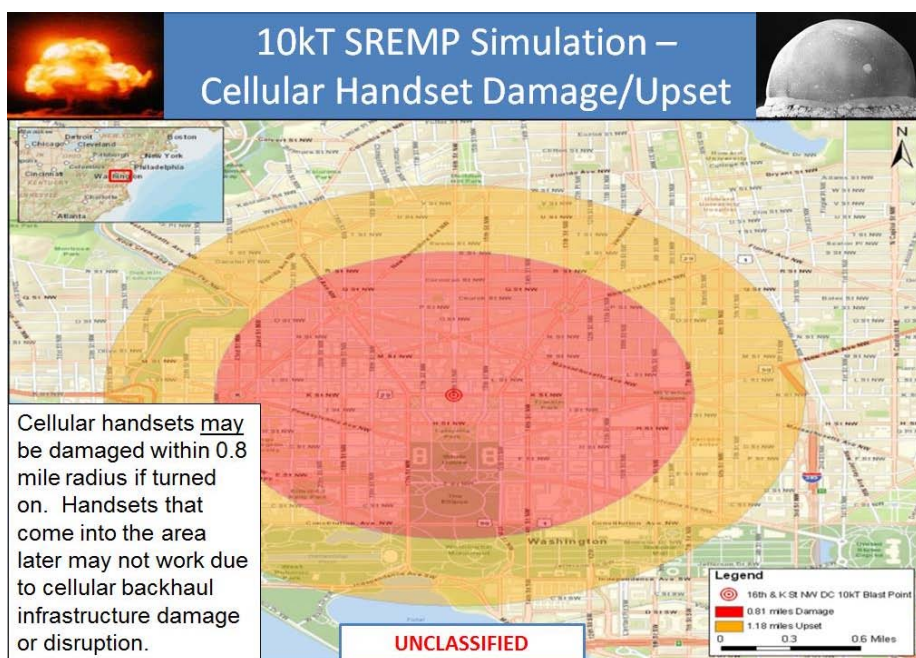
...

Table 1. Four DHS EMP Protection Levels for equipment and facilities


Level 1: Low \$s	Level 2: Hours	Level 3: Minutes	Level 4: Seconds
Use procedures & “low cost” best practices to mitigate EMP effects. Unplug power & data lines into spare/backup equipment. Turn off equipment that cannot be unplugged & that is not immediately needed for mission support. Store one week of food, water, & critical supplies for personnel. Wrap spare electronics with aluminum foil or put in Faraday containers. Have backup power that is not connected to the grid (generators, solar panels, etc.) with 1 week of on-site fuel (like propane/diesel). Use GETS, WPS, & TSP services; join SHARES if applicable (see Appendix C for more information).	In addition to Level 1, use EMP rated surge protection devices (SPDs) on power cords, antenna & data cables & have EMP protected back-up power. Use SPDs (1 nanosecond or better response time) to protect critical equipment. Use true on-line/double-conversion uninterruptible power supplies (UPS). Use fiber optic cables (with no metal); otherwise use shielded cables and ferrites/SPDs. Shielded racks/rooms &/or facilities may be more cost-effective than hardening numerous cables. Use EMP protected HF radio voice/email if need long-haul nets. Suppress EMP fires.	In addition to Level 2, use civil EMP protection standards (like IEC SC 77C). Use EMP shielded racks/rooms and/or facilities to protect critical computers, data centers, phone switches, industrial & substation controls & other electronics. Shielding should be 30-80 dB of protection thru 10 GHz. Use SPDs to protect equipment outside of shielded areas. Can use single-door EMP-safe entryways. Use ITU & IEC EMP standards for design guidance and testing. Have 30 days of back-up power with on-site fuel (or via assured service agreement with EMP resilient refuelers). Use EMP protected HF radio & satellite voice/data nets if need long-range links to support missions.	Use Military EMP Standards (MIL-STD-188-125-1 & MIL-HDBK-423), and 80+ dB hardening thru 10 GHz. Use EMP/RFW shielding in rooms, racks, and/or buildings to protect critical equipment. Use EMP SPDs to protect equipment outside of shielded areas. Use EMP protected double-door entryways. Have 30+ days of supplies & EMP protected back-up power (to include on-site fuel) for critical systems. Don't rely on commercial Internet, telephone, satellite, or radio nets that are not EMP protected for communications. Use EMP protected fiber, satellite, & radio links & Appendix B services

- Mauritania
- Morocco
- Mozambique
- Senegal
- Sierra Leone
- Somalia
- Sudan
- Tanzania
- Tunisia
- Uganda
- Andean Community of Nations
- Australia
- Bahrain
- Bank of International Settlements
- Belarus
- Belgium
- Bermuda
- Bilderberg
 - Bilderberg Archive
 - Bilderberg Participant Lists
- Bolivia
- Bosnia and Herzegovina
- Brazil
- Burma
- Cambodia
- Canada
- Chile
- China
- Colombia
- Corporate
- Council of Europe
- Cuba
- Cyprus
- Czech Republic
- Denmark
- Dominican Republic
- El Salvador
- European Union
 - European Central Bank
 - Europol
 - Eurosystem
- Finland
- France
- G8
- Georgia
- Germany
- Greece
- Guatemala
- Honduras
- Hungary
- India
- Indonesia
- International Criminal Police Organization
- International Monetary Fund
- Iran
- Iraq
- Israel
 - Israel Defense Forces
 - Israel Military Industries
- Italy

...

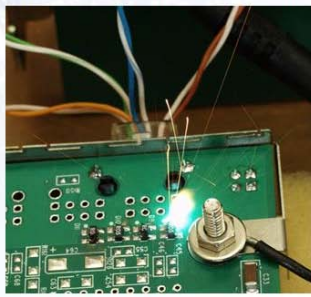


Japan
Jordan
Kosovo
Kuwait
Kyrgyzstan
Laos
Latvia
Lebanon
Liechtenstein
Lithuania
Macedonia
Malawi
Malaysia
Mexico
Michigan
Moldova
Netherlands
New Zealand
Nicaragua
North Atlantic Treaty Organization
North Korea
Norway
Oman
Organisation for Economic Co-operation and Development
Pakistan
Palestine
Panama
Paraguay
Peru
Philippines
Poland
Portugal
Puerto Rico
Qatar
Republic of Iceland
Romania
Russia
Saudi Arabia
Scholarly
Singapore
Solomon Islands
South Africa
South Korea
Spain
Sweden
Switzerland
Syria
Thailand
Threats and Takedown Notices
Trinidad and Tobago
Turkey
Ukraine
United Arab Emirates
United Kingdom
Her Majesty's Treasury
Home Office
United Nations
International Atomic Energy Agency
International Council of

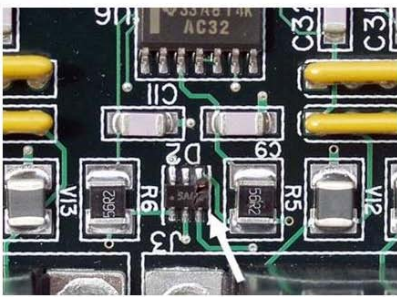


High-Altitude Electromagnetic Pulse Effects on Electronics

- There are no similar natural effects that routinely would be as strong – but HEMP is somewhat like:
 - Electrostatic Discharge (ESD) fields have some similarities to early part of HEMP – E1
 - Solar magnetic storms are similar to late part of HEMP – E3
- HEMP is of concern for electronic equipment – upset or damage




Network interface “blowing up”
– here from a SCADA unit



Damaged part from pulsing of a
timing port in a SCADA unit

(SCADA = “supervisory control and data acquisition”, electric power grid controls.)

UNCLASSIFIED

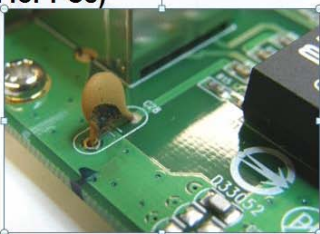


More Damage Examples, NIC Cards


NIC = Network Interface Cards (Ethernet card for PCs)



In-line capacitor
completely blown off a
NIC.



A ceramic capacitor
with a piece blown off;
from a NIC.



The main IC of
a NIC – with
the lid scorched
and deformed.

UNCLASSIFIED

Share this:



Related Material From the Archive:

1. [\(U//FOUO\) DHS Infrastructure Protection Note: Most Significant Tactics Against the Electricity Subsector](#)
2. [\(U//FOUO\) DHS-FBI-NCTC Bulletin: ISIL Supporters Targeting Uniformed Personnel for Weapons and Equipment](#)
3. [UN Guidelines for the Use of Force by Military Components in Peacekeeping Operations](#)
4. [\(U//FOUO\) DHS-FBI-NCTC Bulletin: Terrorists Call for Attacks on Hospitals, Healthcare Facilities](#)
5. [U.S. Army Worldwide Equipment Guide 2015 Update](#)

Chemical Associations
International Fund for
Agricultural Development
World Health Organization
United States

Alabama
Alaska
Arizona
Arkansas
Bureau of Alcohol Tobacco
Firearms and Explosives
Business Executives for
National Security
California
Center for Strategic and
International Studies
Centers for Disease Control
Central Intelligence Agency
Foreign Broadcast
Information Service

Colorado
Congressional Budget Office
Congressional Research
Service
Connecticut
Delaware
Department of Agriculture
U.S. Forest Service
Department of Commerce
Department of Defense
Defense Advanced
Research Projects Agency
Defense Contract
Management Agency
Defense Intelligence
Agency
Defense Logistics Agency
Defense Security Service
Defense Threat Reduction
Agency
Department of Veterans
Affairs
Joint Chiefs of Staff
Joint Improvised Explosive
Device Defeat Organization
Multi-National Corps Iraq
National Defense

6. Apple Inc. Legal Process Guidelines September 2015

Tags:

Department of Homeland Security

Electromagnetic Pulse

National Cybersecurity and Communications Integration Center

- University
- National Geospatial-Intelligence Agency
- National Security Agency
- North American Aerospace Defense Command
- Office of Inspector General of the Depratment of Defense
- U.S. Africa Command
- U.S. Air Force
- U.S. Air Force Research Laboratory
- U.S. Army
- U.S. Army Corps of Engineers
- U.S. Army War College
- U.S. Central Command
- U.S. Coast Guard
- U.S. Forces Iraq
- U.S. Forces Japan
- U.S. Joint Forces Command
- U.S. Marine Corps
- U.S. Navy
 - Naval Network Warfare Command
 - Naval Sea Systems Command
 - Office of Naval Intelligence
 - Space and Naval Warfare Systems Command
- U.S. Northern Command
- U.S. Pacific Command
- U.S. Southern Command
- U.S. Special Operations Command
- U.S. Strategic Command
 - U.S. Cyber Command
- United States Military Academy
- Department of Education
- Department of Energy
- Department of Health and Human Services
 - Indian Health Service
- Department of Homeland Security
 - Customs and Border Protection
 - Department of Homeland Security Testimony
 - Immigration and Customs Enforcement
 - Intelligence Fusion Centers
 - Regional Information Sharing Systems
 - Transportation Security Administration

U.S. Secret Service
Department of Housing and
Urban Development
Department of Justice
 Drug Enforcement
 Administration
Department of State
Department of the Treasury
 Financial Crimes
 Enforcement Network
 Office of the Special
 Inspector General for the
 Troubled Asset Relief
 Program
Department of Transportation
Department of the Interior
District of Columbia
Environmental Protection
Agency
Federal Aviation
Administration
Federal Bureau of
Investigation
 Infragard
Federal Bureau of Prisons
Federal Communications
Commission
Federal Reserve
 Federal Reserve Bank of
 New York
FEMA
Florida
Food and Drug Administration
General Services
Administration
Georgia
Government Accountability
Office
Hawaii
Idaho
Illinois
Indiana
Kansas
Kentucky
Louisiana
Maryland
Massachusetts
Michigan
Minnesota
Mississippi
Missouri
Montana
National Aeronautics and
Space Administration
National Guard
National Institute of Standards
and Technology
National Oceanic and
Atmospheric Administration
National Transportation Safety
Board

- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
 - Metropolitan Transportation Authority
- North Carolina
- North Dakota
- Nuclear Regulatory Commission
- Office of the Director of National Intelligence
 - Intelligence Advanced Research Projects Agency
 - National Counterintelligence Executive
 - National Counterterrorism Center
 - Open Source Center
- Ohio
- Oklahoma
- Oregon
- Pacific Northwest National Laboratory
- Pennsylvania
- Securities and Exchange Commission
- Tennessee
- Texas
- U.S. Agency for International Development
- U.S. District Court
- Utah
- Vermont
- Virginia
- Washington
- Washington D.C.
- West Virginia
- White House
 - National Security Council
- Wisconsin
- Wyoming
- Uruguay
- Uzbekistan
- Vatican
- Venezuela
- Verizon
- Vietnam
- World Bank
- World Trade Organization
- News
 - Featured
- Public Eye
 - Headline

[Contribute Documents and Information](#) • [Contact Us](#)

PI