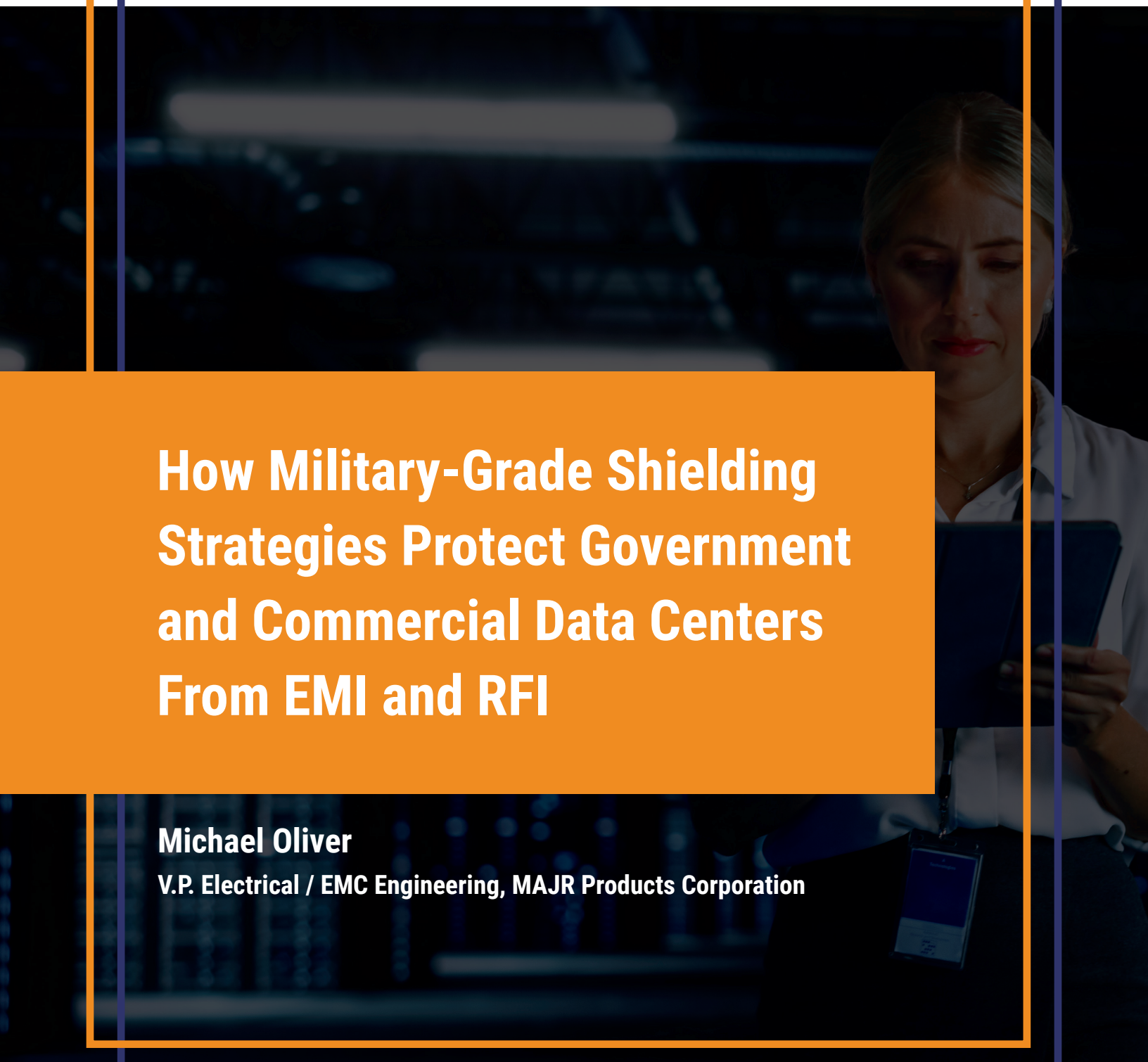


How Military-Grade Shielding Strategies Protect Government and Commercial Data Centers From EMI and RFI

Michael Oliver
V.P. Electrical / EMC Engineering, MAJR Products Corporation

Table of Contents

Government and commercial data centers are densely packed with servers, routers, power supplies, and network switches, making them susceptible to both electromagnetic interference (EMI) and radio frequency interference (RFI). Such interferences tend to come from both internal and external sources, including improperly shielded equipment, nearby broadcast towers, industrial machinery and purposeful criminal activity. Left unaddressed, EMI and RFI can degrade performance, corrupt data, and jeopardize both uptime and information security.

To defend against these risks, data centers have turned to advanced shielding solutions, like shielded panels and connector gaskets, that reduce the likelihood of signal infiltration or leakage. This creates a more controlled electromagnetic environment to not only preserve system performance, but also help data centers meet evolving security and compliance requirements.

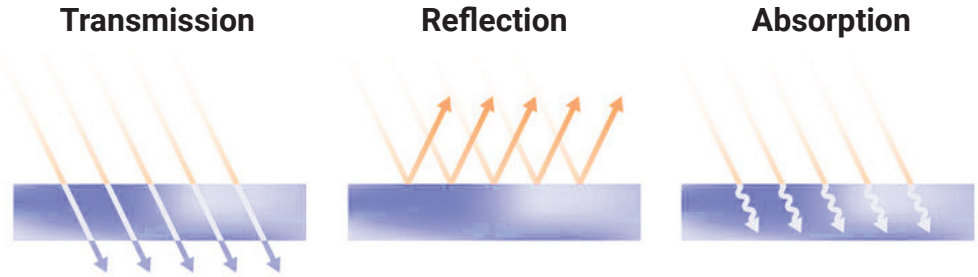
This white paper will address the following:

- *Data Center Shielding*
- *Design Principles of Shielding Technologies*
- *Types of Data Center Shielding Products*
- *Who Benefits From Data Center Enclosure Shielding?*
- *TEMPEST Shielding*
- *Regulatory and Compliance Considerations*

An Overview of Data Center Shielding

At its core, data center shielding functions on the principles of the Faraday Cage, a structure made from conductive materials that blocks external electromagnetic fields. When properly engineered, this shielding forces electromagnetic energy to travel along the exterior surface of the enclosure, preventing it from penetrating inside and thereby effectively containing and isolating EM and RF signals.

To achieve this, the shielding system must create a continuous, low-impedance barrier that addresses all potential vulnerabilities. This includes sealing structural seams, cable and airflow penetrations, doors, and any apertures. Without such a comprehensive approach, even a small gap can become a conduit for harmful interference or leakage.



Shielding Technology seeks to stop any EMI, RFI or EMP transmissions, reflect them or absorb them before they interfere with anything inside a SCIF.

Design Principles of Shielding Technologies

Shielding isn't just about arbitrary placement on metal walls or panels. It involves a strategic approach tailored to data centers, Sensitive Compartmented Information Facilities (SCIFs), and equipment enclosures to create a continuous, conductive barrier.

First, it's important to assess the type of EMI present, then determine the necessary level of shielding based on the equipment's vulnerability.

Next, consider the material properties essential to effective shielding, which are as follows:

- *Conductivity for reflecting and absorbing electromagnetic waves*
- *Permeability for magnetic shielding*
- *Composite solutions for plastic enclosures*

Once the material properties have been selected, several design considerations must be taken into account, including:

- *Frequency range*
- *Cost and feasibility*
- *Environmental conditions*
- *Functional integration*

By combining material properties with practical design considerations, shielding technologies can ensure long-term protection against electromagnetic interference.

Types of Data Center Shielding Products

The complex environment of a government or commercial data center typically involves dense racks of servers, networking equipment, power distribution units, and cooling infrastructures, which pose numerous pathways for EMI/RFI to penetrate or leak. As such, selecting the right combination of shielding products is essential to establishing a secure, continuous electromagnetic barrier.

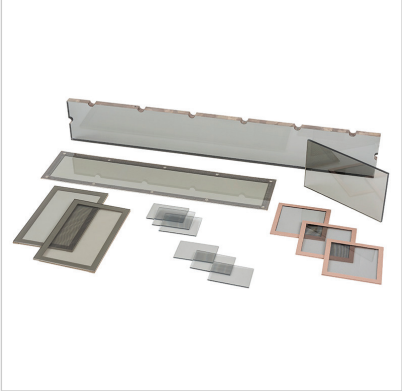
Here is an overview of the primary types of shielding products used in modern data centers:

- *EMI Shielded windows and coatings*
- *Waveguides, such as honeycomb waveguide panels*
- *EMI door/window gaskets for doors and access panels*
  - » *Conductive elastomer gasketing*
  - » *Shield seal gaskets*
  - » *Knitted wire mesh gaskets*
- *EMI washers for nuts and bolts used on any enclosure surface*
- *Vent fans and panels*
- *Honeycomb ventilation panels: HVAC units, ducts, and fans*
- *EMI connector gaskets for electrical/power and telecom cables, and panels*
- *EMI gaskets for all access, egress, and ingress points*
- *Shielded fan ventilation panels*
- *Shielded air filter panels*

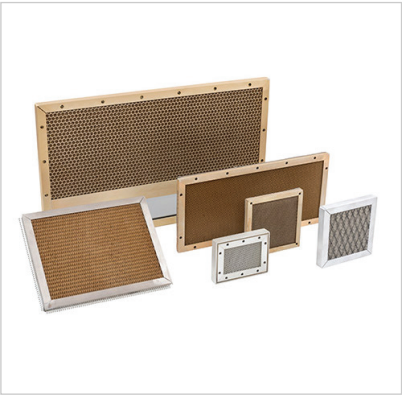
Data Center Shielding Products

Silver Conductive Film

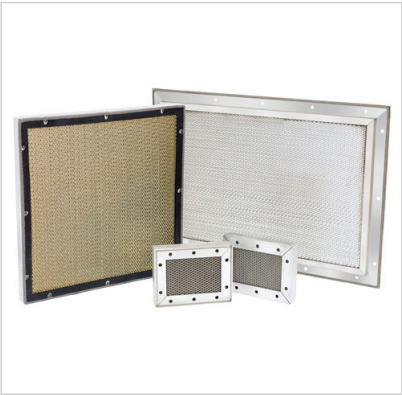
Conductive Coatings



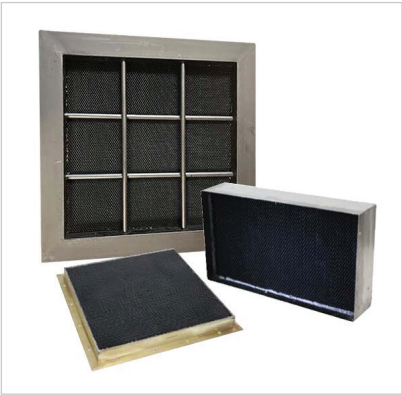
EMI Shielding Windows



Honeycomb Ventilation Panels



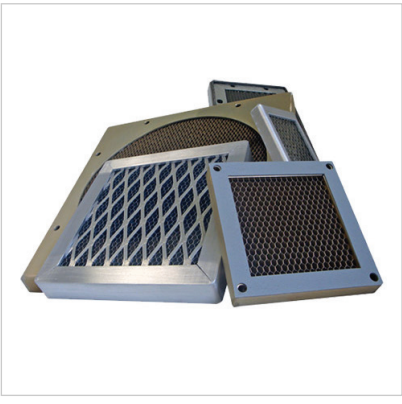
Honeycomb Waveguide Panels



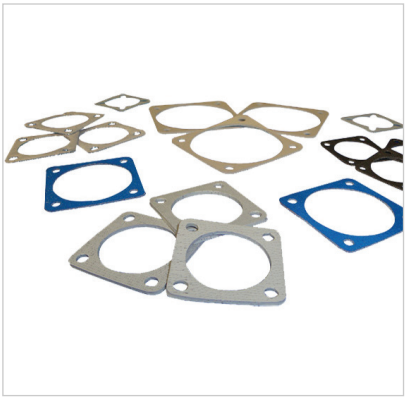
HVAC Waveguide Panels

Slim Line Ventilation Panels

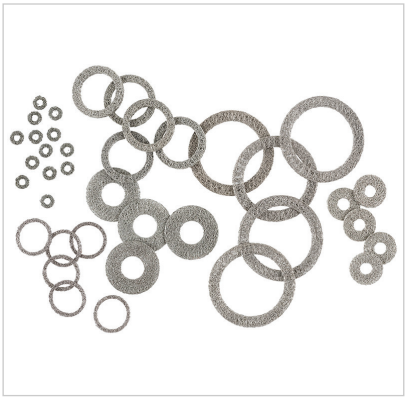
Shielded Air Filtration Panels



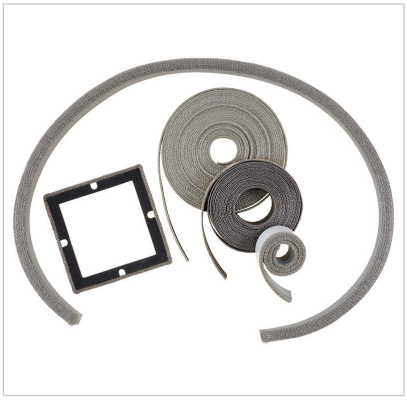
EMI Shielded Fan Ventilation Panels



EMI Connector Gaskets



EMI Grounding Washers



Shield Seal Gaskets

EMI Wire Mesh Gasket

Who Benefits From Data Center Enclosure Shielding?

Shielding isn't limited to one industry or application, as it's important for anyone designing or managing electromagnetic environments to ensure operational reliability, data protection, and regulatory compliance.

Such personnel include:

- *EMI/RFI engineers*
- *Military engineers*
- *SCIF designers*
- *Data center architects*
- *Electronics enclosure manufacturers*
- *Systems integrators*
- *Project managers / General contractors*

With the right products and expert guidance from MAJR Products, you can confidently build shielded environments that stand up to today's complex electromagnetic challenges.

TEMPEST Shielding for Enhanced Confidentiality

TEMPEST refers to the standards and technologies designed to prevent electromagnetic emissions from leaking confidential data outside secure enclosures, particularly for military facilities, government agencies, and secure data centers.

Unlike standard EMI/RFI shielding, TEMPEST shielding adheres to strict government and military standards, ensuring the highest levels of security and confidentiality. It involves comprehensive sealing of all structural seams, access points, ventilation systems, and cable penetrations to maintain a robust shield.

The table below provides a quick reference to the different TEMPEST shielding levels, helping designers and engineers choose the right solution based on the sensitivity of the information and the required confidentiality.

TEMPEST Shielding Levels			
TEMPEST LEVEL	**Standard**	**NATO Zones**	**Description**
Level A	Full	Zone 0	For environments located within 1 meter of a potential eavesdropper
Level B	Intermediate	Zone 1	For environments where interception could occur at distances up to 20 meters
Level C	Tactical	Zone 2	Nearest possible eavesdropper is at least 100 meters away

Regulatory and Compliance Considerations

One of the key regulations impacting contractors and vendors is DFARS 252.204-7012, which outlines requirements for safeguarding covered defense information (CDI) and mandates cyber incident reporting for any commercial entity working with the U.S. Department of Defense (DoD). Any business handling government-related data, including AI applications for defense, must comply with these security requirements.

Supply chain compliance is also becoming an increasingly important focus. A recent revision to DFARS 252.204-7012 increased the domestic component threshold for products used in covered DoD contracts under the Buy American Act (BAA). The new rule requires:

- *65% domestic components from 2024 to 2028*
- *75% domestic components starting in 2029*

MAJR Products is Buy America compliant, offering shielding components that align with both national security and federal procurement policies.

Shield Your Data Center with MAJR Products

MAJR Products offers industry-leading shielding solutions designed to provide comprehensive protection against EMI, RFI, and other vulnerabilities. Don't risk costly downtime or sensitive data exposure by leaving your data center unprotected. Partner with MAJR Products to design and implement a shielded environment that meets the highest standards of reliability and regulatory compliance. Contact us today for your TEMPEST and Data Center Shielding needs.

About the Author

Mr. Oliver is Vice President of Electrical / EMC Engineering at MAJR Products Corporation in charge of, new product development, EMC product consultation, technical quoting, and is the ISO-9001 Mgt. Representative. Mike has over 25 yrs. experience in EMI/RFI shielding technology that includes electronics, military shelter electrical systems, and high power antenna / radome design. Testing / design experience to MIL-STD 461, MIL-DTL-83528 and a variety of SAE and industry standards.

Mr. Oliver is an iNARTE certified Master EMC Design Engineer and holds a B.S. degree in Electrical Engineering from Gannon University and has been an Electrical Engineer since 1989. He currently holds three patents on thermal management-EMI/RFI shielding devices and has experience in the design and testing of aerospace antennas, military electrical systems, and electromagnetic shielding components. Throughout his career Mr. Oliver has performed open and anechoic chamber EMI / RFI radiated tests to military standards and has utilized many antenna and RF testing hardware systems. He has written numerous technical papers on electromagnetic compatibility (EMC) shielding components, EMC product enhancements, and the development of test specifications for antenna / radome radiated test methodologies. Mr. Oliver served on the Academy of Science Committee as an EMC expert concerning an investigation of unintended acceleration of automobiles, is a Senior Member of IEEE, served on the IEEE EMC Society Board of Directors, Chairman of the IEEE EMC Society Pittsburgh Chapter, Member of the SAE AE4 Aerospace Electromagnetic Compatibility Committee, and a member of the IEEE EMC Standards and Advisory Coordination Committee (SACCom).