

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) VOLUME 1: BEST PRACTICES GUIDELINE FOR ARCHITECTURAL RADIO FREQUENCY SHIELDING

Prepared For:

The Intelligence Community and U.S. Government
Partners
Washington, D.C.



Final Submission: January 2022

Prepared by:

(b)(3) Center for Security Evaluation, NCSC

(b)(3)

(U) WARNING: This document is the property of the U.S. Government. Further reproduction and/or distribution by persons other than U.S. Government officials and the project team is prohibited.

(U) DISCLAIMER: Reference in this document to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public, and does not constitute endorsement, recommendation, or favoring by the U.S. Government.

(b)(3) Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b)(3)

(U) Change History

[illegible]

(U) This chart is UNCLASSIFIED

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) Table of Contents

(U) SECTION I: INTRODUCTION.....	4
(U) Purpose of the Document.....	4
(U) Audience.....	4
(U) Scope	4
(U) Relationship to Other Documents.....	6
(U) Acronyms	10
(U) Definitions	13
(U) SECTION II: METHODS OF ARCHITECTURAL SHIELDING.....	25
(U) Introduction	25
(U) General Installation Procedure.....	30
(U) Windows, Penetrations, and Doors.....	31
(U) Power	34

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

*Best Practices Guideline for Architectural Radio Frequency Shielding***(U) SECTION I: INTRODUCTION****(U) Purpose of the Document**

(U//~~FOUO~~) The Best Practices Guideline for Architectural Radio Frequency (RF) Shielding recommends construction practices that would enable secure facilities to achieve adequate levels of RF attenuation to mitigate electromagnetic emanations. Additionally, this document can be used as a reference for the design, build, and renovation of secure facilities to ensure compliance with security policies and applicable accreditation requirements

(U//~~FOUO~~) The Intelligence Community (IC), U.S. Department of State (USDOS), and other federal agencies should utilize this document regularly to ensure their facilities are adequately protected from technical threats by paying considerable attention to RF containment and how RF materials are integrated into the base building design. Organizations should carefully evaluate each facility to ensure sufficient shielding is incorporated to achieve adequate attenuation levels to meet requirements of the accrediting authorities.

(b)(3)

(U) Audience

(U) The readers of the document should be familiar with the design and construction of secure facilities, as well as associated physical and technical security guidelines. Readers do not need to have an in-depth background in RF containment and RF technologies.

(U//~~FOUO~~) This document is meant for a wide range of personnel involved in the construction and accreditation of secure facilities.

(b)(3)

(U) Scope

(U//~~FOUO~~) The Best Practices Guideline for Architectural RF Shielding (b)(3) by presenting best practices for how architectural radio frequency shielding (ARFS) and traditional construction materials can be used to increase RF attenuation. Best practices developed from this document can be used for new construction and major renovations to improve overall RF attenuation within secure facilities. The construction best practices found within this document were developed by conducting testing and evaluation on RF materials to achieve adequate levels of attenuation. Historically, the (b)(3) has conducted testing and validation of numerous RF materials that have been incorporated into this guide. Generic designs, specifications, and

(b)(3) Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

best practices were identified from each material study that could then be used to achieve adequate levels of attenuation within secure facilities.

(U//~~FOUO~~) While this document recommends several roles, responsibilities, materials, and best practices that should be included for new construction and major renovations, there are several other supplemental documents referenced within that should be used to ensure proper policies, industry standards, and guidelines are appropriately followed.

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

*Best Practices Guideline for Architectural Radio Frequency Shielding***(U) Relationship to Other Documents**

(U) This document is to be used in conjunction with other references, standards, documents, schematics, images, and specifications issued by the USDOS and Other Government Agencies (OGAs), and is not intended to be a substitute for any regulation, standard, or requirement. This document is advisory only, therefore the approving authority possesses the authority and responsibility for approving and permitting designs for construction projects.

(U) This document references publications that are frequently updated. The identified references can be used to validate the outlined standards, methods, procedures, regulations, or requirements used within this document. Please contact the Secure Facilities Group (SFG) if a reference is outdated. If a conflict is discovered between applicable codes and standards, and the specified best practice or recommended ARFS methods, the firm should identify and describe the conflict. Once the conflict is identified and described, the firm should request a decision in writing on which requirements(s) take precedence from the authority that has jurisdiction.

(U) The following industry standards and codes should be referred to during facility construction. The following documents encompass many of the applicable standards and codes used for building construction, however, other local, state, federal, and international references exist that should be referred to as well that may not have been incorporated into the latest version of this guide:

- (U) American Society of Heating & Refrigeration and Air-Conditioning Engineers Guidelines (ASHRAE)
- (U) Americans with Disabilities Act Accessibility Guidelines (ADAAG) or Uniform Federal Accessibility Standards (UFAS)
- (U) Institute of Electrical and Electronics Engineers (IEEE) Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures
- (U) International Building Code (IBC) or International Existing Building Code (IEBC)
- (U) International Mechanical Code (IMC)
- (U) List of NFPA Codes and Standards
- (U) National Electric Code (NEC)
- (U) National Fire Protection Association Documentation (NFPA)

(U) The following U.S. government (USG) standards and codes should be referred to during facility construction. The following documents encompass many of the applicable standards and codes used for USG building construction, however, other USG references exist that should be referred to as well:

- (U) ACES Installation Manual
- (U) ACES Installation Standards
- (U) Advanced Materials and Design for Electromagnetic Interference Shielding
- (U) An Interagency Security Committee Report: The Design-Basis Threat

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(b)(3)

- (U) ICD 705 Sensitive Compartmented Information Facilities
- (U) ICD 706 Security Standards for Protecting Domestic IC Facilities
- (U) ICD/Intelligence Community Standard (ICS) 705 Technical Specification for Construction and Management of Sensitive Compartmented Information Facilities
- (U) ICS 705-1 Physical and Technical Security Standards for Sensitive Compartmented Information Facilities
- (U) ICS 705-2 Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities
- (U) ICS 706-1 Domestic Facility Security Risk Assessments Standards
- (U) ICS 706-2 Protecting Mission Critical-Facility Related Control Systems (MC-FRCS) in Mission Critical Facilities (MCF)

(b)(3)

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(b)(3)



(b)(3)

Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~
~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(b)(3)



(b)(3) Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

*Best Practices Guideline for Architectural Radio Frequency Shielding***(U) Acronyms**

(U) This List is UNCLASSIFIED

Acronym	Term
ACS	Access Control System
ADAAG	Americans with Disabilities Act Accessibility Guidelines
(b)(3)	
AHJ	Authority Having Jurisdiction
ANSI	American National Standards Institute
AO	Accrediting Official
ARFS	Architectural Radio Frequency Shielding
ASHRAE	American Society of Heating & Refrigeration and Air-Conditioning Engineers Guidelines
BCR	Built-in Conference Room
BOM	Bill of Materials
BR	Ballistic Resistant
CA	Compartmented Area
CAA	Controlled Access Area
CE	Compromising Emanations
CER	Computer Equipment Room
CIPE	Classified Information Processing Equipment
CI	Counterintelligence
(b)(3)	
CLAN	Classified Local Area Network
COB	Consulate Office Building
CONOPS	Concept of Operations
COR	Contracting Officer's Representative
COTS	Commercial Off-The-Shelf
CSA	Cognizant Security Authority
CSA	Communications Support Activity
CSE	Certified Shielded Enclosure
CSP	Construction Security Plan
CST	Construction Security Technician
CTF	Common Transmission Facility
CTTA	Certified TEMPEST Technical Authority
CWA	Controlled Working Area
dB	Decibel
DS	Diplomatic Security
EPL	Endorsed TEMPEST Products List
EOB	Existing Office Building
FE	Forced Entry

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

FFC	Fixed Facility Checklist
FOUO	For Official Use Only
HHS	High Security Switch
HVAC	Heating, Ventilation, and Air Conditioning
IA	Information Assurance
IBC	International Building Code
IC	Intelligences Community
ICD	Intelligence Community Directive
ICS	Intelligence Community Standards
IDS	Intrusion Detection System
IEBC	International Existing Building Code
IMC	International Mechanical Code
IPC	Information Program Center
IPP	Isolated Power Panel
ITC	Information Technical Center
LAA	Limited Access Area
LAN	Local Area Network
M-G Set	Motor-Generator Set
MNS	Mass Notification System
NEC	National Electrical Code
NAB	Newly Acquired Building
NFPA	National Fire Protection Association Documentation
NOB	New Office Building
NOX	New Office Annex
NSI	National Security Information
NTSWG	National Telephone Security Working Group
OBO	Bureau of Overseas Buildings Operations
OBX	Office Building Annex
O.C.	On Center
OGA	Other Government Agency
OPE	Office of the Procurement Executive
OSHA	Occupational Safety and Health Act
OSPB	Overseas Policy Board
PAA	Public Access Area
PCC	Post Communications Center
PCU	Premise Control Unit
PDU	Power Distribution Unit
PED	Portable Electronic Device
PLF	Power Line Filter
RF	Radio Frequency
RFI	Radio Frequency Interference
SE	Shielded Enclosure

(b)(3) Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~
~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

SED	Standard Embassy Design
SETL	Security Environment Threat List
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facilities
SFG	Secure Facilities Group
SID	Security-in-Depth
SSM	Site Security Manager
STC	Sound Transmission Class
SWA	Secure Working Area
TSCM	Technical Surveillance Countermeasures
TSWA	Temporary Secure Working Area
TSSC	Technical and Signals Security Countermeasures
UFAS	Uniform Federal Accessibility Standards
U-LAN	Unclassified Local Area Network
UPS	Uninterruptible Power Supply
USDOS	United States Department of State
USG	U.S. Government
U.S.	United States
VoIP	Voice Over Internet Protocol Computer Technology
VTC	Video Teleconference

(b)(3) Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

*Best Practices Guideline for Architectural Radio Frequency Shielding***(U) Definitions**

(U) To more readily understand the information presented herein, certain terms unique to ARFS and USDOS/OBO must be understood. The following is a limited listing of terms to help establish the basic working vocabulary necessary to understand the materials and procedures presented throughout this document.

(U) ADJACENT AREA AND CONTIGUOUS SPACE: Space surrounding Controlled Access Area(s) (CAA) besides/below/above; includes adjoining spaces extending beyond external walls/floor/ceiling of CAA through such spaces to next set of walls/floor/ceilings of building.

(U) ADMINISTRATIVELY CONTROLLED AREA: An area into which unescorted access is limited to authorized personnel, either foreign national or American (e.g., cashiers, unclassified computer rooms, unclassified mail rooms, medical unit).

(U) AMBIENT LEVEL: According to the TEMPEST Glossary, ambient levels may be classified into two categories: (a) Test Environment Ambient Level--those levels that exist at a specific test location and time when only the equipment under test is inoperative. Atmospheric, interference from other sources, and circuit noise or other interference generated with the test detection system compromise the "test environment ambient level" (b) Equipment under test level--those levels of radiated and conducted noise that originate in the equipment under test and are not compromising emanations

(U) ANTENNA: A device employed as a means for radiating or receiving electromagnetic energy.

(U) APERTURE: An opening in a shield through which electromagnetic energy passes.

(U) ATTENUATION: A general term used to denote a decrease in magnitude of power or field strength in transmission from one point to another caused by such factors as absorption, reflection, scattering, and dispersion. It may be expressed as a power ratio or by decibels.

(U) AUTHORITY HAVING JURISDICTION (AHJ): (1) The governmental agency which regulates the construction process. (2) For Department of State projects, the Design and Engineering Division of the OBO Program Development (OBO/PDCS), is the Authority Having Jurisdiction.

(U) ARCHITECTURAL RADIO FREQUENCY SHIELDING (ARFS): RF shielding that is built into the structure of the parent building, consisting of one of several, or a combination of several types of light-weight RF shielding materials assembled to provide measurable plane wave attenuation.

(U) BALLISTIC RESISTANCE: Products and designs certified under the provisions of SD-STD-01.01 April 1993 G (see 12 FAH-5H-011, subparagraph (4)) to withstand a minimum of 7.62/5.56 mm rifle rounds fired from approximately 20 feet (6 m) without penetration or spalling.

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) BLACK: According to the TEMPEST Glossary, designation applied to telecommunications and automated information systems and to associated areas, circuits, components, and equipment, in which national security information is not processed.

(U) BOND: The electrical connection between two metallic surfaces established to provide a low-resistance path between them.

(U) BONDING: The process of establishing the required degree of electrical continuity between the conductive surfaces to be joined.

(U) CERTIFIED SHIELDED ENCLOSURE (CSE): An enclosure which is physically isolated from the parent room and uses shielding compliant with Department of State and national standards for acoustic and RF frequency protection.

(U) CERTIFIED TEMPEST TECHNICAL AUTHORITY (CTTA): This is an experienced technically qualified US Government employee who has met established certification requirements in accordance with NSTISSC-approved criteria and has been appointed by a US Government Department or Agency to fulfill CTTA responsibilities.

(U) CHANCERY/CONSULATE: The place in which the business of an embassy is conducted. Facility occupied by U.S. Government interests and activities. May include an office annex containing U.S. citizens on the same compound as the chancery or consulate.

(U) CLASSIFIED INFORMATION PROCESSING EQUIPMENT (CIPE): According to the USDOS OSPB Glossary, this refers to any electronic or electromechanical equipment which is used to create, store, reproduce, transmit, manipulate, or process classified information. CIPE includes, but is not limited to, computers, computer terminals, computer systems, and printers; microfiche and microfilm readers/printers; and audio/visual equipment, facsimile machines, photocopier equipment, and typewriters.

(U) CLOSE ACCESS: In the technical surveillance filed close access technical operations involve a suite of blended solutions which could involve an insider threat, but ultimately involve active emplacement of a technical device to get denied information outside a facility.

(U) COMMON WALL: A wall, floor, ceiling, or other physical barrier separating USG-controlled spaces from adjoining non-USG-controlled spaces.

(U) COMPROMISE: Unauthorized disclosure of classified information, or unauthorized access to secured products/materials/equipment.

(U) COMPROMISING EMANATIONS (CE): According to the CI Glossary, these are unintentional emissions that could disclose information being transmitted, received, or handled by any information-processing equipment. (ICS Glossary) Also see TEMPEST; TEMPEST Test.

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) CONTRACTING OFFICER'S REPRESENTATIVE (COR): See Project Director; also a person designated and appointed in writing by the Contracting Officer. The COR shall be the Government's representative on the project for technical operations. Certain and specific Contracting Officer duties may be delegated by the Contracting Officer to the COR. The COR is authorized to act on behalf of the Contracting Officer to perform only those duties expressly delegated by the Contracting Officer and as specifically set forth in the Contract Documents.

(U) CONTROLLED: The state of being directly protected by 24-hour presence of Cleared American Personnel, or being under protection of technical devices approved and installed by Bureau of Diplomatic Security (DS).

(U) CONTROLLED ACCESS AREA (CAA): Those areas of the building that fall into one of two categories of certified space in which classified information may be handled, stored, discussed, and processed. All unauthorized personnel entering the CAA must be under constant escort and observation. There are two categories of CAAs: Core and Restricted.

(U) CONTROLLED AREA: An area where an individual has passed one or more inspection points in order to gain entry, but in which no national security information is processed. This area must be behind the building hardline.

(U) CONSTRUCTIONS SURVEILLANCE TECHNICIAN (CST): These are Cleared U.S. citizens (Top Secret) who are selected, professionally trained in surveillance techniques in accordance with CST's field guidebook, experienced in construction and assigned to a project for the purpose of ensuring the security integrity of a site, building, CAA, and/or material and/or items which are scheduled for use or inclusion in a CAA.

(U) CORE AREA: Those areas of the CAA where unescorted access is limited to authorized U.S. citizens holding a TOP SECRET clearance. Authorized U.S. citizens with a SECRET clearance may have access to core areas, but must be under constant escort and observation. Certain areas also require special access authorization.

(b)(3)

(U) COUNTERMEASURES: Countermeasures includes the employment of devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities. Also, (in TEMPEST usage) action, device, procedure, technique, or other measure that reduces the vulnerability of any equipment that electronically processes information (b)(3)

(U) CUTOFF FREQUENCY: The frequency below which electromagnetic energy will not propagate readily in a waveguide.

(b)(3) Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) DECIBEL (dB): The dB is a measure of the ratio between two quantities and is used in a wide variety of measurements in acoustics, physics and Electronics. While originally only used for power and intensity ratios, it has come to be used more generally in engineering. The decibel is widely used in measurements of the loudness of sound. It is a dimensionless unit like percent. Decibels are useful because they allow even very large or small ratios to be represented with a conveniently small number (similar to scientific notation). This is achieved by using a logarithm.

(U) DEGRADATION: A decrease in the quality of a desired signal (i.e., decrease in the signal-to-noise ratio or an increase in distortion), or an undesired change in the operational performance of equipment as the result of interference.

(U) DESIGN-BUILD: Also known as “design-construct” or “single responsibility,” design-build is a system of contracting under which one entity performs both architecture/engineering and the construction under one single contract. (Design-Build Institute).

(U) ELECTROMAGNETIC FIELD: This is energy that exists in the vicinity of a conductor of electricity. It consists of electric radiation and magnetic radiation components.

(U) EMANATION: These are unintended signals or noise appearing external to an equipment.

(U) EMBASSY: (1) The diplomatic mission, representing the United States to another country, and typically consisting of an ambassador and staff. (2) The building(s) containing the offices of an ambassador and staff.

(U) ENGINEERING SERVICES OFFICE: This is a Diplomatic Security Element within a diplomatic mission, which is responsible for technical security.

(U) EXISTING OFFICE BUILDING (EOB): In terms of physical security for overseas USG facilities, there are two types of EOBs: (1) USDOS-designed office buildings or compounds which were at the 35% design development stage prior to July 1991; and (2) Office buildings or compounds not designed by USDOS which were acquired through purchase, lease, or other means, prior to July 1991.

(U) FACILITY GROUNDING ELECTRODE SYSTEM: This is the electrically interconnected system of conductors and conductive elements that provides multiple current paths to earth. This system is normally connected at the service point of the facility.

(U) FACILITY: A building or other structure, either fixed or transportable in nature, with its utilities, ground networks, and electrical supporting structures.

(U) FARADAY SHIELD: This is a grounded metallic barrier that can be used for improved isolation between the primary and secondary windings of a transformer. In this application, the shield reduces the leakage capacitance between the primary and secondary windings without affecting electromagnetic coupling.

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) FILTER: A device for use on power or signal lines, specifically designed to pass only selected frequencies and to attenuate substantially all other frequencies.

(U) FINISH WORK: Work, other than general construction as defined below, including insulation, partition/ceiling systems, finishes, cabinet work, conveyor systems, specialties, building furnishings/fixtures/equipment, and mechanical/electrical services and equipment including those specialized for fire protection, security, communication, control, energy conservation, safety, comfort, convenience, and similar purposes.

(U) FIRM; THE FIRM: Any one of several professional architectural, engineering, design, or construction companies engaged to design, build, or design and build and execute a project.

(U) FLOODING: Bombarding a facility with sound waves that results in the ability to get data out of the building.

(U) FORTUITOUS CONDUCTOR: This is any conductor, which may provide an unintended path for signals. Fortuitous conductors may include cables, wires, pipes, conduits, and structural metalwork in the vicinity of a signal source.

(U) FURNISH: Except as further defined for specific work, means supply and deliver to Project Site, ready for unloading, unpacking, assembly, installation, and similar handling as applicable for each instance of use.

(U) GENERAL CONSTRUCTION: Construction activity for completion of building foundations, structure, and enclosure or shell. Utility work that penetrates the exterior plane of the building and the installation of doors, windows and façade work are not considered general construction. Any reinforcement work done to increase load-bearing capacity in existing buildings is not considered general construction.

(U) GROUND: The electrical connection to earth through an earth electrode subsystem. This connection is extended throughout the facility via the facility ground system, consisting of the signal reference subsystem, the fault protection subsystem, and the lightning protection subsystem.

(U) GROUNDING ELECTRODE: This is a conductor that makes effective electrical contact with the earth.

(U) HARDLINE: Term referring to a system of barriers surrounding a protected area which afford degrees of forced entry, ballistic resistant, or blast protection, or combinations of these three. A hardline may include walls, floors, ceilings, roofs, windows, doors, or non-window openings, all of which must provide the level of protection specified for that hardline.

(U) HOST COUNTRY: The country in which the project is located; *also* – the nation to which a United States Embassy is accredited.

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) INDICATED: Refers to means of recording requirements for performing work of Contract Documents, and similar texts. Where term such as “shown,” “specified,” “noted,” or “scheduled” is used, it is for purpose of helping reader locate requirements in contract documents, and no limitation of location or requirements is intended.

(U) IN-PLACE MONITORING SYSTEM: A system that operates in the background to monitor for specific signals of concern.

(U) INSPECTABLE MATERIALS: These are materials that can be inspected through existing DS-approved means. Examples include single-wall duct work, drywall, wood, and nonelectrical fixtures.

(U) INSPECTABLE SPACE: This refers to the 3D space surrounding equipment that processes classified and/or sensitive information, within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists.

(U) INSTALL: Except as defined under specific work, means primary operations at Project Site, including, but not limited to, unloading, unpacking, assembly, erection, placing, anchoring, applying, working to dimension, finishing, during, protecting, cleaning, and similar operations, as applicable for each unit of work.

(U) INSTALLER: The entity (person or firm) engaged by Contractor or any of its subcontractors, at any tier of responsibility, for performance or installation of particular unit of work at Project Site, either singly or in conjunction/cooperation with other installers for portions of unit of work and adjoining work. It is a basic requirement that each installer be qualified for and equipped for operations it is engaged to perform.

(U) Experienced Installer: Installer qualified with at least five years of experience in operations engaged to perform, who meets or exceeds requirements for staffing, training, testing, certifying, licensing, tooling, equipping, and similar requirements as specified and otherwise implied in each instance, for type/quality of workmanship indicated, and who has demonstrated proficiency, safety, and compliance with regulations by recognized authorities having expertise or jurisdiction.

(U) Specialist: Where indicated, installation must be performed by specially qualified “specialists,” who are recognized experts in the work required as demonstrated by certificates of testing and performance, appropriate and applicable in each instance. Where indicated, the Contractor shall engage the related product manufacturer as specialist for installation of unit of work. Compliance with these requirements will neither be held to relieve Contractor of responsibility for fulfilling requirements of Contract Documents, nor interpreted to provide a basis for conflicts with applicable regulations, trade unions, and local authorities jurisdiction.

(U) ISOLATED POWER PANEL (IPP): This is a panel that receives and distributes the output from the secondary winding of an isolation device (transformer or motor-generator set). When used to support a shielded enclosure, the IPP is usually mounted on the outside skin of a shielded enclosure.

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) ISOLATION: This is the physical and electrical arrangement of system, facility, or equipment components to prevent electrical contact or electromagnetic interaction within or between these components.

(U) ISOLATION TRANSFORMER: A transformer that contains electrostatic shields between the primary and secondary windings, with no direct electrical path between the primary and secondary windings. These shields allow magnetic coupling between the primary and secondary windings without significant coupling of any other kind, such as conductive (ohmic) or electrostatic (capacitive) coupling.

(U) LIMITED ACCESS AREA: An area of U.S. control between the CAA and the general work areas.

(U) LOCK AND LEAVE FACILITY: A Department of State overseas office facility officially certified and designated as a (classified or unclassified) facility without 24-hour cleared U.S. presence.

(U) MAIN DISTRIBUTION PANEL: This is the first power distribution panel connected to the incoming power lines in the shielded enclosure parent room that receives power from outside the parent room and provides power to the primary side of the isolation device (transformer and/or motor-generator set) and all circuits within the parent room.

(U) MAN-PASSABLE: An opening having the minimum area required for an intruder to physically pass through a barrier and enter a secured area. In accordance with DS/PSP/PSD specifications (SD-STD01.01), the minimum area considered passable is 652 cm² (96 square inches) with its smallest dimension equal to, or larger than, 150 mm (6 inches). *Also* – Under the provisions of DS Certification Standard – SD-STD-01.01, the minimum area considered passable is 652 cm² (96 square inches) with its smallest dimension equal to, or larger than, 150 mm (6 inches). Nominal dimensions are as follows: Square Opening: 250 mm x 250 mm; Rectangular Opening: 150 mm x 400 mm; Circular Opening: 300 mm.

(U) MOTOR GENERATOR: This is a device sometimes used in the CAA as a countermeasure to filter or isolate power.

(U) MISSION: A delegation or representation of the U.S. headed by an Ambassador, such as to an international organization; also, a generic term for the U.S. presence in a host country.

(U) MULTIPOINT GROUND: More than one path to ground.

(U) NEUTRAL: The conductor in a polyphase or single-phase circuit that is intended to have a potential difference between it and the phase conductors that is approximately equal in voltage and equally spaced in phase.

(U) NEW OFFICE ANNEX (NOX): In terms of physical security for overseas USG facilities, a NOX is an office building constructed on an existing compound by or on behalf of the USG.

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) NEW OFFICE BUILDING (NOB): In terms of physical security for overseas USG facilities, a NOB is an office building or compound constructed by or on behalf of USG which was at the 35% design development stage subsequent to June 1991.

(U) NEWLY ACQUIRED BUILDING (NAB): In terms of physical security for overseas USG facilities, a NAB is an office building or compound not constructed by or on behalf of USG which was acquired by purchase, lease, or other means, subsequent to June 1991.

(U) NONCONDUCTIVE BREAK: An insulating section inserted in a conduit, duct, or any other metallic penetration to provide electrical isolation.

(U) NONINSPECTABLE Materials: Materials, which cannot be inspected by USDOS-approved means. Examples include electrical, electronic, and electromechanical materials, such as ballasts, switches, motors, and break panels.

(U) OFFICE BUILDING ANNEX (OBX): An addition to an existing building or a new office building constructed adjacent and connected to an existing office building.

(U) PARENT ROOM: This is the room that houses a CSE or RF shielded enclosure and is separated by walls from other similar parts of the structure or building.

(U) PENETRATION: The passage through a partition or wall of an equipment or enclosure by a wire, cable, pipe, or other conductive object.

(U) PHYSICAL HAZARD: This is any instance of information leaving an area by unauthorized means due to weaknesses in design or construction, damage, or degradation of the physical infrastructure. Physical Hazards are categorized as Unmitigated Hazards, or Exploitable Hazards. All Exploitable Physical hazards are presumed to be technical penetrations until determined to be otherwise by the appropriate Technical Surveillance Countermeasure (TSCM) authority.

(U) PLANE WAVE: An electromagnetic wave which predominates in the far-field region of an antenna, and with a wave front which is essentially a flat plane. In free space, the characteristic impedance of a plane wave is 377 Ω .

(U) POST COMMUNICATIONS CENTER (PCC): An area within the Chancery or Consulate where post communication activity takes place. *Also* – An area within the Chancery or Consulate requiring the highest levels of protection where intelligence, cryptographic, security, and other particularly sensitive or compartmentalized information may be handled, stored, discussed, or processed. The PCC normally includes the common transmission facility (CTF), information program center (IPC), information technical center (ITC), and the communications support activity (CSA).

(U) PRIMARY BUILDING: Typically the Chancery, Consulate or NOB of a United States diplomatic mission. A 24 hour/day Marine Security Guard Post is normally located in this primary building.

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) PROJECT DIRECTOR: The COR on all matters pertaining to the project. The Project Director is responsible for ensuring that all project design and construction activities are accomplished in a manner that complies fully with applicable statutes and security regulations. The Project Director acts as the interface between the Contractor and the USG as “owner” and is the only individual authorized to stop work for security purposes. *Also* – A professional construction manager representing OBO at a project site through the Construction and Commissioning Division of OBO’s Program Execution Office.

(U) PUBLIC ACCESS AREA (PAA): This is an area within the building that services are provided to the general public. There is no handling, storing, discussion, or processing of classified, controlled, or sensitive but unclassified (SBU) materials.

(U) RADIO FREQUENCY INTERFERENCE (RFI): Synonymous with electromagnetic interference.

(U) RADIO FREQUENCY (RF): The primary frequency to transmit over the air.

(U) RANDOM PROCUREMENT: An approved method, which must be executed in accordance with Office of the Procurement Executive (A/OPE) Procurement Policy Directive No. 5, whereby vendor is selected at random from among a number of possible vendors (usually 3 or more), each of whom has been identified as able to supply required item in required quantity from shelf stock. The required quantity of an item is procured and immediately taken into controlled possession by cleared U.S. citizen, and transported to CAA(s) or secure storage area (SSA), without vendor’s prior knowledge of intended procurement, and without referrals to or from vendor. This process is generally limited to procurement of low-volume and emergency items involving CAA. Cleared U.S. citizen (e.g., Contractor or Contracting Officer) is required to make random selection of required units from vendor’s shelf stock.

(U) REFLECTION LOSS: The portion of the transition loss, expressed in decibels, that is due to the reflection of power at a barrier or shield. Reflection loss is determined by the magnitude of the wave impedance inside the barrier relative to the wave impedance in the propagation medium outside the barrier.

(U) RESTRICTED AREA: Those areas of the CAA where unescorted access is limited to authorized U.S. citizen personnel possessing at least a SECRET clearance. Un-cleared personnel must be under the continuous escort of approximately cleared U.S. citizen personnel.

(U) RF CONTAINMENT: Architectural applications that provide measured RF attenuation.

(U) RF SHIELDING: This refers to any conductive material, such as sheet metal or metal fabric that is installed on the structure of a room or around equipment that attenuates electromagnetic radiation emanating from information processing equipment.

(U) RF-TIGHT: Offering a high degree of electromagnetic shielding effectiveness.

(U) SECURE ROOM: This is a specifically designated room, typically used to house security containers protecting classified information and/or equipment. This room is built with slab-to-slab construction of

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

some substantial material; i.e., concrete, brick, concrete masonry units (CMUs), or plywood, minimum ½ inch (1.26 cm). Any window or penetrations of wall areas over 96 square inches (625 cm²) (man-passable) must be covered with metal grilling or expanded metal commensurate with wall material. Entrance doors must be constructed of substantial material and be capable of holding a GSA-approved built-in, three-position, dial-type combination lock. All doors must have a pin-type-dogging device on the hinge edge. If a reverse-beveled door is used, hinges must include non-removable pins.

(U) SERVICE EQUIPMENT: This is the necessary equipment, usually consisting of circuit breakers or switches and fuses and their accessories, connected to the load end of service conductors to a building or other structure, or an otherwise designated area, and intended to constitute the main control and cutoff of the supply.

(U) SHIELD: A housing, screen or cover which substantially reduces the coupling of electric and magnetic fields into or out of circuits or prevents the accidental contact of objects or persons with parts or components operating at hazardous voltage levels.

(U) SHIELDED ENCLOSURE (SE): An area (box, room, or building) specifically designed to attenuate electromagnetic radiation, or electromagnetic radiation and acoustical emanations, originating either inside or outside the area. Necessary openings in shielded enclosures, such as doors, air vents, and electrical conduit, are fed through specially designed devices designed to maintain the required attenuation.

(U) SHIELDING EFFECTIVENESS: A measure of the reduction or attenuation in the electromagnetic field strength at a point in space caused by the insertion of a shield between the source and that point.

(U) SINGLE POINT GROUND: Grounding system based on the provision of a single, very large conductor from a grounding stud attached near the electromagnetic filter of a small shielded enclosure and then routed by the shortest path to a separate ground located within the perimeter of the building shell. The ground wire shall have less than 1 Ω of resistance between the enclosure and the ground connection. The ground connection must have less than 10 Ω of resistance under all-year conditions.

NOTE: For an in depth and detailed explanation of the theory of signal ground design, see MIL-HDBK419A or "Grounding, Bonding and Shielding for Electronic Equipment and Facilities".

(U) SITE SECURITY MANAGER (SSM): A designated USG representative responsible to Contracting Officer's Representative (COR) for all site security matters involving CAA construction projects.

(U) STANDARD EMBASSY DESIGN (SED): Drawings, specifications and other criteria that serve as the base standard to be site-adapted to produce project Construction Documents.

(U) SUPPLEMENTAL GROUNDING ELECTRODE SYSTEM: This is an extension of the existing facility-grounding electrode system that (1) Provides a continuous ground path from grounded systems within the CAA to a grounded electrode system, and (2) Ensures a ground resistance measurement of 10 ohms or less.

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) SURVEYED AREA: An office, area, or facility under survey by a TSCM team. Generally a SCIF, SAPF, or other specifically identified space containing sensitive information. The boundaries or perimeter of the surveyed area are described by the accreditation documentation for the space or specifically outlined in the TSCM request and represent the security perimeter for the information contained within. While TSCM activities will take place in various support areas outside this defined space, they are not included under this definition.

(U) SURVEY: A complete inspection of a Surveyed Area by an authorized TSCM activity using all approved tactics, techniques, procedures and equipment to detect a technical surveillance activity.

(U) TECHNICAL HAZARD: Any instance of information potentially leaving an area by unauthorized means due to equipment design or manufacture, damage, breakdown, configuration, or installation. Technical Hazards are categorized as Mitigated Hazards, Unmitigated Hazards, or Exploitable Hazards. All Exploitable Technical hazards are presumed to be technical penetrations until determined to be otherwise by the appropriate TSCM authority. According to the USDOS OSPB Glossary, this is a condition that results in the unintentional radiation of exploitable information or facilitates a hostile technical attack.

(U) TECHNICAL SECURITY ASSESSMENT: This is a comprehensive assessment that is conducted to identify and correct fundamental weaknesses in technical security at posts abroad.

(U) TECHNICAL SECURITY: this is a security discipline dedicated to detecting, neutralizing, and/or exploiting a wide variety of hostile and foreign penetration technologies.

(U) TECHNICAL SURVEILLANCE: This is the use of optical, audio, or electronic monitoring devices or systems to surreptitiously collect information.

(U) TEMPEST ADVISORY BOARD: A group comprised of CTTAs and other qualified representatives from OSPB member agencies, chaired by the Department of State.

(U) TEMPEST EQUIPMENT: Information processing equipment that has been certified to meet prescribed security requirements and appears on the national security agency endorsed TEMPEST products list (EPL), or which has been certified to meet specifications of NSTISSAM TEMPEST 1-92.

(U) TEMPEST INSPECTION: This is an inspection or assessment performed by qualified and equipped technical and procedural security personnel at facilities requiring TEMPEST countermeasures.

(U) TEMPEST: TEMPEST Countermeasures are designed to prevent exploitation of compromising emanations by containing them within the equipment or IS [inspectable space] of the facility processing classified information.

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) TEMPEST-ZONED EQUIPMENT: Non-TEMPEST equipment that has been profiled to meet TEMPEST performance standards at discrete distances greater than one meter away from the equipment as opposed to 1 meter (3.28 feet) as required for TEMPEST equipment.

(U) TRADES: Contract Document terminology oriented to recognize names of building trades and crafts (e.g., “Carpentry”); it is not intended to imply that certain construction activities must be performed/installed solely by tradespersons, unionized or non-union, or corresponding generic name (e.g., “Carpenters”). It also does not imply that related requirements apply exclusively to work performed by trades persons of matching generic name.

(U) UNCONTROLLED (AREA): Any area outside the PAC or an area controlled by measures that can be circumvented surreptitiously or forcibly.

(U) UNINTERRUPTIBLE POWER SUPPLY: This is a device that is guaranteed to provide power to equipment during power outages or interruptions in the incoming electrical power.

(U) VAULT: A space constructed to enclose and safeguard sensitive material or operations.

(U) WAVEGUIDE: Any of a class of devices that confines and directs the propagation of electromagnetic waves, such as radio waves, infrared rays, and visible light.

(U) WAVE IMPEDANCE: The ratio of the electric field strength to the magnetic field strength at the point of observation.

(U) WAVELENGTH: The ratio of C , the speed of light, to F , the frequency. Wavelength (ft) = $984/F$ (MHz).

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

*Best Practices Guideline for Architectural Radio Frequency Shielding***(U) SECTION II: METHODS OF ARCHITECTURAL SHIELDING****(U) Introduction**

(U//~~FOUO~~) This guide presents numerous references to RF shielding materials and procedures necessary to achieve adequate levels of attenuation within secure facilities for new construction and major renovations. It is intended for personnel familiar with the process of designing, building, and securing of secure facilities. It can also be used as an educational tool for anyone that requires a better understanding of facility security applications. Supplemental documents, schematics, and images should be referenced and reviewed routinely to ensure policies are being followed and construction materials are installed correctly.

(U) Risk Management

(U) The construction and renovation of secure facilities around the world comes with a wide range of risks that are based on several factors which include the physical location of the work being performed and potential threats identified by the CTTA. Individual risk assessments should be conducted at each location so that the CTTA can identify appropriate materials and equipment that should be applied to the base building design.

(b)(3)

(U) Construction Security

(U) A Site Security Manager (SSM) should be the single point of contact regarding construction security and the individual responsible for all security aspects of facility construction. Along with the SSM, Construction Security Technicians (CSTs) are necessary to mitigate potential threats of prohibited technologies being introduced into secure facilities. They should be familiar with construction tools, materials, and processes, as well as be able to identify prohibited devices. Additionally, they should understand how RF materials and mitigations are incorporated into the base building design. Construction plans and all related documents should be handled and protected IAW the Construction Security Plan (CSP).

(b)(3)

(U) Foreign National Contractors(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) Foreign national contractors pose a unique Counterintelligence (CI) threat to secure facilities. Extra precautions should be taken to mitigate threats from foreign national contractors. Accrediting Official (AO) approval may be necessary to authorize foreign national citizens or companies to perform work at secure facilities.

(b)(3)

(U) CWA/SCIF (NSI) Accreditation Requirements

(U) A clear, active Sensitive Compartmented Information (SCI) mission must exist before a Sensitive Compartmented Information Facility (SCIF) is requested. Furthermore, SCI will not be discussed or introduced into the proposed SCIF until the facility is formerly accredited and has acquired a letter of accreditation. A letter of accreditation is a formal statement on behalf of the IC element head that a facility has been designed, constructed, inspected, and certified for the protection of all SCI compartments, programs or special activities in accordance with the provisions of ICD 705.

(b)(3)

(U) Concept and Pre-construction Approval

(U) The concept approval step is a key element in future accreditation actions. Concept of Operations (CONOPS) approval certifies that clear operational requirements exist for the secure facility and there is no existing secure facility already to support the requirement.

(b)(3)

(U) The Fixed Facility Checklist

(U) The Fixed Facility Checklist (FFC) is a standardized document used in the process of accrediting a secure facility. It documents physical, technical, and procedural security information for obtaining an initial or subsequent accreditation. To support the accreditation process, designers of record, project managers, and construction managers should provide the AO/SSM site plans, building floorplans, Intrusion detection system (IDS) plans, and information related to perimeter and compartmented area wall construction. Information that should also be provided includes doors, locks, deadbolts, IDS, telecommunication systems, acoustical protections, and TEMPEST countermeasures.

(b)(3)

(U) Construction Requirements and Specifications

(b)(3) Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) Prior to secure facility construction, the SSM should be provided with a copy of all pre-construction drawings for approval. Based upon a threat analysis, additional technical or physical enhancements may be required.

(b)(3)

(U) Handling and Distribution of Drawings

(U) Drawings should be considered and marked For Official Use Only (FOUO) and handled IAW the Freedom of Information Act, The Intelligence Authorization Act of 2002. Where possible, drawings should be sanitized and a separate key document should be maintained by authorized personnel.

(b)(3)

(U) Security Milestones for Inspection

(U) To ensure proper installation of construction materials in secure facilities, security milestone inspections are recommended. These inspections should take place at specific phases of construction to ensure proper installation of construction materials. Except as otherwise specified herein, the contractor is responsible for the performance of all inspection requirements specified in the applicable specifications for all materials and associated equipment supplied. The CSA assigned representative should inspect the construction points described below.

- (U) During wall construction, but before walls are covered in gypsum wall board, all wall layers need to be inspected.
- (U) Following the installation of any man-bars, duct grills, or inspection ports.
- (U) Inspection of doors and hardware as specified, i.e. once doors are hung and all equipment is installed to include door sweeps, thresholds, and gaskets.
- (U) Final inspection to include confirmation of wall-to-ceiling (slab-to-slab) construction; complete sealing around all penetrations in perimeter walls, completion of walls above false ceiling in a workman-like manner to include painting both sides. Cable, either fiber or metallic, should be accounted for from the point of entry into the secure facility. Designated spare conductors should be identified, labeled, and bundled together.
- (U) Ceiling tiles will not be installed until after the final inspection to facilitate access to the plenum, and prevent damage to the tiles.
- (U) Both interior and exterior perimeter walls should be inspected for completion.

(b)(3)

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) Testing

(U//~~FOUO~~) To validate adequate levels of RF attenuation and identify any RF leaks from installed shielding materials, proper RF testing should be performed. (b)(3)

(b)(3)

(U) Photographic Construction Surveillance Record

(U) The lack of consistent construction surveillance photographs has made it difficult to iteratively develop effective best practices for new construction and renovations. This issue has made it more difficult to achieve adequate levels of RF attenuation needed to mitigate potential threats when facilities are constructed or renovated. To address this issue, CSTs should take photographs during various phases of construction and submit them to the government representative. Written contextual statements of the construction photographs should be submitted to the government representative as well. These photographs and statements should be kept on-site at the respective facility for historical reference and inspections.

(b)(3)

(U) Design Feedback loop

(U) Because design criteria for secure facilities are developed through assessments and interpretations, the design process is necessarily iterative. This creates the need for an efficient feedback loop between the design team and the AO that can be leveraged repeatedly throughout the process. This direct and recurring connection to the AO is arguably the most important feature of a successful design process. It is critical to agree to an appropriate frequency for sharing drawing updates with the AO, and to hold regular coordination between the AO, SSM, and design leads. In between these meetings, as the design is being developed, the SSM should be collecting questions and elevating them to the AO for review.

(U) Weather and Environmental Concerns

(U) Weather and environmental factors can contribute to the deterioration of materials used in the construction of secure facilities. Factors that can influence the deterioration of secure facilities include elevated temperatures, ultraviolet radiation, humidity resistance, and biological corrosivity. These factors should be accounted for when building construction is performed.

(b)(3)

(b)(3) Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~
~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) Corrosion Prevention and Control

(U) Because of the naturally corrosive nature of various materials and metals, it is necessary to identify and mitigate potential factors that could contribute to the corrosion in secure facilities. There are several corrosion prevention resources that can be referenced, as well as various materials, systems, components, and coatings that can be leveraged for preventative and corrective maintenance over the life-cycle of a facility.

(b)(3)

(U) Maintenance and Repairs

(U) Shielding materials deteriorate over time and lose their efficacy, therefore it is necessary to conduct maintenance and repairs to ensure adequate RF attenuation. Accidental damages from personnel or severe weather further contributes to this deterioration.

(b)(3)

(U) Safety and Health Guidelines

(U) The American National Standards Institute (ANSI) has determined that exposure to magnetic and electric fields is harmful to human tissue. Since shielding effectiveness testing requires generating such fields, these common sense precautions should always be followed:

- (U) Always place the transmitter inside the shielded enclosure
- (U) Never test a shielded enclosure with anyone inside
- (U) Do not turn on the transmitter until just prior to performing the test
- (U) Never transmit more power than necessary
- (U) Stay out of the transmitter antenna pattern

(U) Additionally, various building materials may release harmful gasses, chemicals, and volatile organic compounds (VOC), which could cause lasting respiratory, reproductive, nervous system, and brain damage. This health hazard, known as off-gassing, should be mitigated by not using materials that contain VOC, allowing materials to shed early fumes before the space is occupied, and providing adequate ventilation.

(b)(3)

(b)(3)

Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) General

(U) The building owner should coordinate with government representative to obtain final tenant approval and acceptance of build-out. The government project manager should perform a final acceptance and inspection before the space is released for occupancy. It is recommended that a SSM or CSA assigned representative be present with the project manager during the final acceptance inspection.

(b)(3)

(U) General Installation Procedure

(U) While a fully integrated ARFS solution requires a 6-sided envelope or perimeter be constructed, that envelope can be broken into four categories. These four categories consist of exterior walls, interior walls, floors, and ceilings. There are many similarities for the procedures on how these categories are constructed, but there are slight differences that should be noted between them.

(b)(3)

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~~~NOT FOR PUBLIC RELEASE~~

(b)(3)

*Best Practices Guideline for Architectural Radio Frequency Shielding***(U) Windows, Penetrations, and Doors****(U) Windows**

(U) Standard windows do not meet the attenuation levels necessary to mitigate many threats. Cracks and other deficiencies within windows expose secure facilities to vulnerabilities. To mitigate potential vulnerabilities, windows should be non-opening and provide visual and acoustic protection. Moreover, if windows are part of the perimeter they should be treated to maintain the attenuation standards required by the CTTA and AO.

(b)(3)

(U) Intrusion Detection Systems

(U) Secure facilities contain a wide range of entry points that may be vulnerable to intrusion by un-cleared personnel and potential threats. Interior areas of secure facilities through which reasonable access could be gained, including walls common to areas not protected at the SCI level, should be protected by an IDS. Additionally, secure facilities should be protected by IDS when not occupied. It is important to note that an IDS causes a new penetration into the facility, therefore this new vulnerability should be carefully evaluated.

(b)(3)

(U) Doors

(U) To maintain the six-sided RF attenuation requirement, RF attenuation doors will be needed, taking into account the physical and acoustic considerations. Standard doors do not meet the RF attenuation requirements necessary to mitigate RF signals. Sagging and inadequate installation of doors further increases the vulnerabilities present within secure facilities. To mitigate these vulnerabilities, standard RF-tight doors and frames that meet acoustic standards should be used in the construction of these facilities. Generally, secondary and emergency exit doors should have many of the same design standards as primary doors.

(b)(3)

(U) Grounding

(U//~~FOUO~~) Electronic devices and conductors in secure facilities may contain electromagnetic information that can be collected by adversaries if not properly protected or grounded. (b)(3)

(b)(3) Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(b)(3)

(U) HVAC

(U//~~FOUO~~) HVAC systems contain unique vulnerabilities that expose secure facilities to a wide range of threats. Appropriate measures should be implemented to mitigate vulnerabilities and provide adequate attenuation. (b)(3)

(b)(3)

(U) Nonconductive Break

(b)(3)

(U) RED/BLACK

(U) All equipment, wirelines, components, and systems that process unencrypted National Security Information (NSI) are considered RED. All equipment, wirelines, components, and systems that process encrypted NSI and non-NSI are considered BLACK. The RED/BLACK concept is utilized to establish guidance for physical separation to decrease the probability that electromagnetic emissions from RED devices might couple to BLACK systems. Consult CTTA to determine TEMPEST countermeasures.

(b)(3)

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) Telephone Security

(U) For the purposes of meeting RED/BLACK installation guidance, the administrative telephone system and its associated wiring are BLACK, and classified systems and associated wiring are RED. These administrative telephone systems are a potential source for fortuitous conduction of CE due to their proximity to building maintenance areas and their signal line distribution outside the facility. Due to these vulnerabilities, telephones located in RED electromagnetic environments may require additional protections. Furthermore, for on-hook security issues, refer to the National Telephone Security Working Group (NTSWG) publications.

(b)(3)

(U) Penetrations

(b)(3)

(U) Waveguides

(b)(3)

(U) Honeycomb Vent

(b)(3)

(b)(3) *Center for Security Evaluation, NCSC*

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~NOT FOR PUBLIC RELEASE~~

(b)(3)

Best Practices Guideline for Architectural Radio Frequency Shielding

(U) Pipe Penetrations

(b)(3)

Network Cabling

(b)(3)

(U) Power

RED Power

(U//~~FOUO~~) Is a methodology and installation practice used to provide power along with an isolated distribution system (IDS) that complies with National policy requirements to protect National Security Information (NSI).

(b)(3)

(b)(3)

(U) RED Power - (b)(3) Main Components

(U//~~FOUO~~) If determined by a CTTA that RED Power is a requirement for a facility/location (b)(3)

(b)(3)

(b)(3) Center for Security Evaluation, NCSC

(b)(3)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~