DEPARTMENT OF STATE
BUREAU OF DIPLOMATIC SECURITY

SECURITY CLASSIFICATION GUIDE
FOR
DESIGN AND CONSTRUCTION
OF
OVERSEAS FACILITIES

JULY 2018

A SUPPLEMENT TO THE DEPARTMENT OF STATE (DOS) CLASSIFICATION GUIDE

RESPONSIBLE OFFICIAL:

TODD J. BROWN
DEPUTY ASSISTANT SECRETARY
FOR COUNTERMEASURES

Reproduction and Distribution: Authority is granted to reproduce all or part of this guide for official use by individuals or groups involved in architectural design, engineering, management, construction or subcontracting of new construction, rehabilitation efforts, equipment installations, and day-to-day operations at overseas Department of State (DoS) facilities. Any other release of this document must be approved by the Bureau of Diplomatic Security. **The posting of this guide on the internet is prohibited.** See also Administration of this Guide, Paragraph C.2 for further dissemination restrictions.

TABLE OF CONTENTS

I. PURPOSE 4

II. GOALS 4

III. BENCHMARKS 6
- A. AUTHORITIES 4
- B. RELATED STANDARDS 7
- C. ADMINISTRATION OF THIS GUIDE 7

IV. SPECIFIC GUIDELINES 8
- A. APPLICABILITY 8
- B. EXPLANATION OF FORMAT 9
- C. CLASSIFICATION TABLES 12

SPACES

TABLE IV-1 RESTRICTED CAA – EXCLUDING: SHIELDED ENVIRONMENTS/RED POWER SYSTEMS, TELECOMMUNICATIONS & TECHNICAL SECURITY 12

TABLE IV-2 CORE CAA – EXCLUDING: SHIELDED ENVIRONMENTS/RED POWER SYSTEMS, TELECOMMUNICATIONS & TECHNICAL SECURITY 14

TABLE IV-3 PCC – EXCLUDING: SHIELDED ENVIRONMENTS/RED POWER SYSTEMS, EMERGENCY POWER SYSTEMS, TELECOMMUNICATIONS & TECHNICAL SECURITY SYSTEMS 16

TABLE IV-4 SHIELDED ENVIRONMENTS/RED POWER SYSTEMS – APPLICABLE IN RESTRICTED CAA, CORE CAA, AND PCC – EXCLUDING: EMERGENCY POWER SYSTEMS, TELECOMMUNICATIONS 20

TABLE IV-5 PCC DEDICATED EMERGENCY POWER SYSTEMS 23

TABLE IV-6 BLAST RESISTANCE 25

TABLE IV-7 PHYSICAL SECURITY 27

TABLE IV-8 TECHNICAL SECURITY – INCLUDING BUT NOT LIMITED TO CCTV, INTRUSION DETECTION SYSTEMS (IDS), ELECTRONIC DOOR CONTROLS, IPMS, ETC. 29

TABLE IV-9 TELECOMMUNICATIONS – INCLUDES U-LAN, C-LAN, BAS, AND TELEPHONE… 31

TABLE IV-10 SENSITIVE COMPARTMENTED INFORMATION FACILITIES…….. 34

APPENDICES
- A. ACRONYMS 36
- B. DEFINITIONS 38
- C. HANDLING INSTRUCTIONS FOR CLASSIFIED, SBU, AND UNCLASSIFIED MATERIAL 40
- D. FREQUENTLY ASKED QUESTIONS 51

NOTE: This document supersedes the Security Classification Guide for Design and Construction of Overseas Facilities dated May 2003. There is no intent to classify, upgrade, downgrade, or declassify work dated prior to the date of this revision or for projects already underway. However, all new work generated from this date forward (including work derived from archival records) shall comply with this guide.

Reproduction and Distribution: Authority is granted to reproduce all or part of this guide for official use by individuals or groups involved in architectural design, engineering, management, construction or subcontracting of new construction, rehabilitation efforts, equipment installations, and day-to-day operations at overseas DoS facilities. Any other release of this document must be approved by the Bureau of Diplomatic Security. **The posting of this guide on the internet is prohibited.** See also Administration of this Guide, Paragraph C.2 for further dissemination restrictions.

I. PURPOSE

This guide establishes uniform procedures for categorization of sensitive and classified information relating to the architecture, engineering, interiors, construction, and rehabilitation of any U.S. government facility overseas which falls under Chief of Mission authority. It is to be used to determine the sensitivity of material and the protection of that material. This supplement shall be used as a standalone document and its use is independent of, and exclusive from, the DoS Classification Guide. It shall be used for all design and construction projects and day-to-day facility operations within existing facilities. This guide shall be used by all United States government and contractor personnel, including consultants (both retained and prospective), involved with the Department's overseas facilities.

Determination of sensitive and classified levels follows these precepts:

Sensitive material is categorized as:

- Sensitive But Unclassified (SBU) and indicates material which should be protected from unauthorized disclosure but does not pose a national security risk.

Classified material is categorized at three levels indicating the magnitude of potential harm to United States national security, were it to be disclosed to unauthorized individuals:

- Confidential (C) could cause damage to the United States;
- Secret (S) could cause serious damage to the United States; or
- Top Secret (TS) could cause exceptionally grave damage to the United States.

II. GOALS

A. General Goals:

1. Prevent the unauthorized disclosure of sensitive and classified information.
2. Keep as much information unclassified as practical.
3. Avoid the over- and under-classification of material.

B. Specific Goals:

Spaces

1. Functional Areas:

- Protect the configuration of those functional areas in site-specific Core and Restricted Controlled Access Area (CAA) spaces, as well as the location of weapons safe(s)/vault(s).
- Encourage the use of generic terminology to the maximum extent feasible.
- Protect the graphic depictions of floor plans for foreign affairs offices and representational housing overseas.

2. Post Communications Center (PCC):

- Protect the site-specific layout, to include partitions, equipment, building support systems (i.e. mechanical/electrical), telecommunications, and furniture of spaces within the PCC (excluding vault walls, if applicable).
- Protect site-specific details describing the transition of building support and telecommunications systems into a treated environment (if applicable).

- Protect tests, inspection and operational procedures, and results.

3. **Shielded Environments** (Acoustic and Electro-magnetic radiation):
   - Whenever Shielded Environments (SEs) are required, protect the design, location, and capabilities of its technical components (electrical, telecommunications, mechanical, structural, and acoustic), tests methods, vulnerabilities, and recovery procedures.
   - Protect site-specific details describing the transition of building support and telecommunications systems into a treated environment.

Systems

4. **Emergency Power Systems:**
   - Protect the detailed design, capabilities, and vulnerabilities of emergency power systems dedicated to PCCs.

5. **Blast Resistance:**
   - Protect critical aspects of the criteria used to develop specific blast resistant designs.
   - Protect the specific vulnerabilities of existing facilities or proposed designs.

6. **Physical Security:**
   - Protect existing vulnerabilities that are not readily visible to the general public.

7. **Technical Security:**
   - Protect details of any U.S. government-directed modifications to Commercial off-the-shelf (COTS) equipment and systems.
   - Protect the site-specific details of critical elements of the Technical Security Systems protecting CAAs.

8. **Telecommunications** (to include C-LAN, U-LAN, internet, telephone, fire alarm, public address, cable television, and building automation systems):
   - Protect site-specific design for telecommunications systems designed to carry classified data or voice signals.
   - Protect all site-specific telecommunications systems that enter shielded environments.

III. BENCHMARKS

A. Authorities:

1. Authorizing Official:

Assistant Secretary (AS)
for
Diplomatic Security (DS)
U.S. Department of State
Washington, D.C. 20520

2. Office of Primary Responsibility:

Deputy Assistant Secretary (DAS)
for
Countermeasures (DS/C)
Bureau of Diplomatic Security
U. S. Department of State
Rosslyn, VA 22209
571-345-3835

3. Executive Order (E.O.) 12829, Subject: National Industrial Security Program, dated January 6, 1993 as amended [*establishes the protection of information classified pursuant to E.O 12356 dated April 2, 1982, "National Security Information," or its successor, and the Atomic Energy Act of 1954, as amended*].

4. E.O. 13526, Subject: Classified National Security Information, dated December 29, 2009 [*establishes a uniform system for classifying, safeguarding, and declassifying national security information*].

5. 32 Code of Federal Regulations (CFR) Parts 2001 and 2003, Subject: Classified National Security Information; Final Rule, dated June 28, 2010 and July 9, 2012, respectively [*provides implementation guidance concerning the requirements set forth in E.O. 13526 which is applicable to U.S. government agencies*].

6. 32 Code of Federal Regulations (CFR) part 2004, Subject: National Industrial Security Program Directive No. 1; Final Rule, dated April 10, 2006 [*provides for implementation and oversight by the Information Security Oversight Office (ISOO) of E.O. 12829]*.

7. E.O. 12968, Subject: Access to Classified Information, dated August 2, 1995 [*establishes a uniform Federal personnel security program for employees who have access to classified information*].

8. DoS 1 FAM (Foreign Affairs Manual) 262.1, Subject: DAS for Countermeasures (DS/C): [*discusses DS/C functions, responsibilities, and authority, for the management, formulation, and representation on matters regarding security policy and program plans for physical and technical security countermeasures for the Department*].

9. DoS 12 FAM 355b and 360, Subject: Transit Security [*discusses the required handling of materials bound for CAAs and the Construction Security Certification Program which is used to notify Congress that the Department's projects are embedded with adequate security measures*].

10. DoS 12 FAM 530, Subject: Information Security [*establishes a uniform system for classifying, declassifying, and safeguarding national security information under control of Foreign Affairs Agencies, which includes the Department of State*].

11. DoS Notice 2001_03_014, Subject: Guidelines for Public Information Dissemination on the Internet, dated March 6, 2001.

12. DoS 12 FAM 540, Subject: Sensitive But Unclassified [*provides guidelines for SBU information handling, processing, transmission, and/or storage and destruction*].

B. Related Standards

1. DoS 12 Foreign Affairs Handbook (FAH)-5, Subject: Physical Security Handbook.

2. DoS 12 FAH-6, classified SECRET, Subject: Overseas Security Policy Board (OSPB) Security Standards and Policy Handbook [*establishes a uniform system for safeguarding national security information under control of Foreign Affairs Agencies at Diplomatic Missions abroad*].

3. Presidential Decision Directive (PDD) 63, Subject: Critical Infrastructure Protection dated May 22, 1998 [*establishes national effort to secure the U.S. interconnected infrastructure such as telecommunications, banking, finance, energy, transportation, and essential government services*].

4. Department of Defense (DoD) 5220.22-M, Subject: National Industrial Security Program Operating Manual (NISPOM), dated February 28, 2006 [*establishes requirements, restrictions, and other safeguards necessary to prevent unauthorized, and control authorized, disclosure of classified information released by U.S. government Executive Branch Departments and Agencies to their contractors*].

C. Administration Of This Guide

1. Reproduction and distribution: see notice on cover and table of contents.

2. The posting of this guide on the internet is prohibited. Transmission to specified individuals via the internet is permitted on a need to know basis.

3. Categorization, review, and changes: the contents of this guide and the determination of what information is categorized (on a Department-wide basis) as classified are the responsibility of DS/C. For project-specific issues, see Appendix C. **This guide will be reviewed every five years** by DoS for continued applicability and will be rewritten as necessary to ensure all changes have been incorporated in the base document. Revisions to this guide shall clearly differentiate new language from old. Comments regarding the administration of this guide should be directed, through your facility security officer, to:

Deputy Assistant Secretary and
Assistant Director for Countermeasures
Bureau of Diplomatic Security
U.S. Department of State
Rosslyn, VA 22209
571-345-3835

Comments should thoroughly describe the issue and suggestions for remedy are readily appreciated.

IV. SPECIFIC GUIDELINES:

A. Applicability

The tables included on the following pages shall be applied to all forms of information and information sharing (hardcopy, electronic, audio, video, digital, telephonic, and photographic) used to develop criteria, designs, and construct or renovate the subject facilities. These may include, but are not be limited to:

- As-Built documents
- Bids
- Bills of Material (BOMs)
- Budget Documents
- Calculations
- Construction Documents
- Construction Security Plans (CSPs)
- Contracts
- Cost Estimates (e.g. CWE)
- Designs
- DoS Standards
- Egress Plans
- Facsimiles
- Generic Designs
- Inspection Reports
- Maintenance Plans, Manuals, and Studies
- OBO Design Standards
- Operating Manuals
- Planning Papers and Reports (e.g. LROBP)
- Plans
- Photography
- Programming Documents
- Proposals
- Repair Manuals
- Requests for Information (RFI's in ProjNET)
- Requests for Proposals
- Review Comments (e.g. ProjNET)
- Shop Drawings
- Signage Plans, Schedules, and Room Keys
- Specifications
- Standardized designs (e.g. SED)
- Statements of Work (SOWs)
- Studies
- Submittals
- Submittal Registers
- Survey Reports
- Tests Procedures and Test Results

Explanation of Format

This table is an example of the format used in the classification tables on subsequent pages. It provides an explanation of terms and codes used to categorize information. The elements are listed in the chronological order usually encountered on design and construction projects. Classification and de-classification codes are explained on the next page.

[SUBJECT] *(explanation of basic elements included)*	Classification/ Sensitivity Level		Remarks
Non Site-Specific			
• Generic Criteria *Definition: Systemic standards and requirements which are applicable to a group of projects, programs, or sites.*			
• Design Standards: *Definition: Unless stipulated by contract as a binding requirement, a* standard *is non-binding direction on how requirements could be met. This* standard *is usually articulated, for example, in documents like the Building Code of the Bureau of Overseas Buildings Operations. Note: Design Standards differ from this Classification Guide in that the requirements of this Guide are binding.*			
• Research Tests and Results: *Definition: Information gathered during Research and Development for establishing new standards, certifiable assemblies, etc.*			
Site-Specific			See Appendix for definition of "Site-Specific"
Design Requirements			
• Criteria: *Definition: Mandatory project requirements including capabilities and quantified requirements.*			
• Design Guidelines: *Definition: Non-binding concepts or illustrative solutions used to describe the intent of a requirement.*			
• Proposed or Existing features: *Definition: Data usually included in surveys, planning documents, and statements of work used to describe existing conditions or determine project requirements. May include discussion of existing vulnerabilities.*			
Design			
• Design: *Definition: All direct and indirect architectural, interiors, and engineering work undertaken to prepare documents to be used by fabricators, constructors, vendors, and installers.*			
Operations			
• Operations and Repair Manuals: *Definition: Generic or custom documents (including electronic media versions), which are used to ensure the continued use of that feature. (Includes routine procedures, emergency procedures, troubleshooting, etc.).*			
• Results of tests and inspections: *Definition: Any findings from tests, inspections, surveys, post-failure diagnoses, etc.*			

*** Classification/Sensitivity Codes:**

U	Unclassified
SBU	Sensitive but Unclassified
SBU/NOFORN	Sensitive but Unclassified - No Foreign Dissemination
C	Confidential
S	Secret
S/NF	Secret-No Foreign Dissemination
TS	Top Secret
3.3(b)X	Exemption Code – 3.3(b), of E.O. 13526 [The authority for exemption from automatic declassification where paragraph X represents the reason for exemption, a subparagraph number in section 3.3(b).]

**** Classification:**

E.O. 13526 dated December 29, 2009 provides specific guidance on procedures related to classification management. Section 1.4 of that order provides a listing of classification categories for specific types of information. This document is the classification authority to be cited by persons within Department of State without original classification authority, and all contractors, and should be cited as the reason(s) for classification. DoS has determined that one or more of these reasons for classification apply to the subjects listed in Tables IV-1 through IV-10 of this guide.

> **Section 1.4 CLASSIFICATION CATEGORIES** (E.O. 13526)
>
> Information shall not be considered for classification unless it concerns:
>
> **(a)** military plans, weapons systems, or operations;
>
> **(b)** foreign government information;
>
> **(c)** intelligence activities (including covert action), intelligence sources or methods, or cryptology;
>
> **(d)** foreign relations or foreign activities of the United States, including confidential sources;
>
> **(e)** scientific, technological, or economic matters relating to the national security;
>
> **(f)** United States government programs for safeguarding nuclear materials or facilities;
>
> **(g)** vulnerabilities or capabilities of systems, installations**,** infrastructures, projects, plans, or protection services relating to the national security**;** or
>
> **(h)** the development, production or use of weapons of mass destruction.

***** Declassification:**

E.O. 13526, dated December 29, 2009, provides specific guidance on procedures related to classification management. Section 3.3(b) of that order prohibits a classification authority from exempting material for more than 25 years from declassification, at the time of original classification, other than information that meets the criteria listed in paragraphs 1-9. This may only be done at a time less than five years before the date of automatic declassification (i.e. after the 20th anniversary of the original classification). The office of Information Programs and Services (A/GIS/IPS) is responsible for the Department's systematic declassification review program.

Unless otherwise noted, all information that is identified for classification listed in Tables IV-I through IV-10 should be classified for 25 years from the date of origin.

Section 3.3b EXEMPTION CODES (E.O. 13526)

An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which should clearly and demonstrably be expected to:

(1) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;

(2) reveal information that would assist in the development, production, or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

(5) reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

(6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

(7) reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of national security, are authorized;

(8) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructure relating to the national security; or

(9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

C. Classification Tables

Table IV-1		
Subject	**Classification/ Sensitivity Level**	**Remarks**
Restricted CAA – Excluding: Shielded Environments/Red Power Systems, Telecommunications & Technical Security		
Non Site-Specific		
1. Generic Criteria	U	UNCLASSIFIED for all generic criteria excluding Noise Isolation Class (NIC) acoustic requirements when not designating a specific suite (i.e. all Regional Security Officers (RSOs) offices).
	S	SECRET when a specific NIC acoustic rating for the perimeter of the CAA is required.
2. Design Standards	U	
Site-Specific		See Appendix for definition of 'Site-Specific'
Design Requirements		
3. Criteria	U	UNCLASSIFIED for all criteria excluding acoustic requirements.
	C	CONFIDENTIAL when a specific sound transmission class (STC) acoustic rating for the perimeter of the CAA or CAA suites is required. CONFIDENTIAL when infrared (IR) performance criteria is specified for CAA windows.
	S	SECRET when a specific NIC acoustic rating for the perimeter of the CAA or CAA suites is required.

Table IV-1		
Subject	**Classification/ Sensitivity Level**	**Remarks**
4. Design Standards (generic and standardized graphics and details)	U	UNCLASSIFIED for all design guidelines, graphics and details unless a specific acoustical rating, radio frequency (RF), or infrared (IR) protection is noted. If specific acoustical rating is noted the classification will be in accordance with the Criteria classification listed above. (See also Table IV-4 for Shielded Environments).
Design		
6. Floor plans, infrastructure plans	U	UNCLASSIFIED when all plans depicting structural walls only (general construction).
	U	UNCLASSIFIED for all floor plans, internal configurations, furniture plans, infrastructure plans, building utilities, etc.
7. Identification of office spaces	U	UNCLASSIFIED when signage or labels identifies the space using generic terms (e.g. office, reception area, corridor, restroom, mechanical spaces).
	SBU	SENSITIVE BUT UNCLASSIFIED when signage or labels identifies office occupants listed in the unclassified space program (e.g. Executive Suite, Pol/Econ, RSO, etc.). UNCLASSIFIED – After accreditation and building occupancy.
	S/NF	SECRET/NOFORN when signage or labels identifies the area as a Treated Environment or a Tenant not listed in the unclassified space program.
Operations		
8. Operations and Repair Manuals	U	UNCLASSIFIED when not associated with a specific area of the building.
	U	UNCLASSIFIED when associated with a specific CAA space (e.g. CAA Fire Alarm Repair Manual, etc.). (Manuals for classified systems are to be considered classified to the level of the associated system).

Table IV-1		
Subject	**Classification/ Sensitivity Level**	**Remarks**
9. Results of tests and inspections	U	UNCLASSIFIED when all test and inspection results are identified, with no vulnerabilities.
	S/NF	SECRET/NOFORN when vulnerabilities are identified that could affect the security of classified information.

Table IV-2		
Subject	**Classification/ Sensitivity Level**	**Remarks**
CORE CAA – Excluding: Shielded Environments/Red Power Systems, Telecommunications & Technical Security		
Non Site-Specific		
1. Generic Criteria	U	UNCLASSIFIED for all generic criteria excluding NIC acoustic requirements when not designating a specific suite (e.g. all RSO offices).
	S	SECRET when a specific NIC acoustic rating for the perimeter of the CAA is required.
2. Design Standards	U	UNCLASSIFIED
Site-Specific		See Appendix for definition of 'Site-Specific'
Design Requirements		
3. Criteria	U	UNCLASSIFIED for all criteria excluding acoustic requirements.
	C	CONFIDENTIAL when a specific STC acoustic rating for the perimeter of the CAA or CAA suite is required.
	C	CONFIDENTIAL when infrared (IR) performance criteria is specified for CAA windows.
	S	SECRET when a specific NIC acoustic rating for the perimeter of the CAA or CAA suite is required.
4. Design Guidelines (generic and standardized graphics and details)	U	UNCLASSIFIED for all design guidelines, graphics, and details unless a specific acoustical rating, radio frequency (RF), or infrared (IR) protection is noted. If specific acoustical rating is noted, the classification will be in accordance with the criteria classification listed above.
Design		

Table IV-2		
Subject	**Classification/ Sensitivity Level**	**Remarks**
5. Floor plans, infrastructure plans	U	UNCLASSIFIED when all plans depicting structural walls only (general construction).
	C	CONFIDENTIAL for all floor plans, internal configurations, furniture plans, utilities, infrastructure plans, etc.
6. Identification of office spaces	U	UNCLASSIFIED when signage or labels identifies the space using generic terms (e.g. office, reception area, corridor, restroom, mechanical spaces, etc.).
	C	CONFIDENTIAL when signage or labels identifies office occupants listed in the unclassified space program (e.g. Defense Attaché Office, LEGATT, Executive Suite, Pol/Econ, RSO, etc.). UNCLASSIFIED after accreditation and building occupancy.
	S/NF	SECRET/NOFORN when signage or labels identifies the area as a Treated Environment or a Tenant not listed in the unclassified space program.
Operations		
7. Operations and Repair Manuals	U	UNCLASSIFIED when not associated with a specific area of the building.
	U	UNCLASSIFIED when associated with a specific CAA space (e.g. CAA Fire Alarm Repair Manual, etc.). Manuals for classified systems are to be considered classified to the level of the associated system.
8. Results of tests and inspections	U	UNCLASSIFIED when all test and inspection results are identified, with no vulnerabilities.
	S/NF	SECRET/NOFORN When vulnerabilities are identified that could affect the security of classified information.

Table IV-3		
Subject	**Classification/ Sensitivity Level**	**Remarks**
PCC – Excluding: Shielded Environments/Red Power Systems, Emergency Power Systems, Telecommunications & Technical Security		
Non Site-Specific		
1. Generic Criteria	SBU	SENSITIVE BUT UNCLASSIFIED when all generic criteria excluding acoustic, isolation, and adjacency requirements as well as any countermeasures.
	C	CONFIDENTIAL when a specific STC acoustic rating for PCC construction is required.
	S	SECRET for all isolation and adjacency requirements, or any countermeasures.
	S	SECRET when a specific NIC acoustic rating for PCC construction is required.
	S	SECRET when specifications, models, etc. of prime mission equipment is specified.
2. Design Standards	SBU	SENSITIVE BUT UNCLASSIFIED for all generic criteria excluding acoustic, isolation, adjacency requirements as well as any countermeasures.
	C	CONFIDENTIAL when a specific STC acoustic rating for PCC construction is required.
	S	SECRET for all isolation and adjacency requirements, or any countermeasures.

Table IV-3		
Subject	**Classification/ Sensitivity Level**	**Remarks**
	S	SECRET when a specific NIC acoustic rating for PCC construction is required.
	S	SECRET when specifications, models, etc. of prime mission equipment is specified.
Site-Specific		See Appendix for definition of 'Site-Specific'
Design Requirements		
3. Criteria	C	CONFIDENTIAL for all site specific criteria. (This is classified, because it is NOT generic.)
	C	CONFIDENTIAL when a specific STC acoustic rating for PCC construction is required.
	S/NF	SECRET/NOFORN for all isolation and adjacency requirements, or any countermeasures.
	S/NF	SECRET/NOFORN when a specific NIC acoustic rating for PCC construction is required.
	S/NF	SECRET/NOFORN when specifications, models, etc. of prime mission equipment is specified.
4. Design Standards (generic and standardized graphics and details)	U	UNCLASSIFIED for all design guidelines, graphics, and details unless a specific acoustical rating or radio frequency (RF) is noted. If specific acoustical rating is noted, the classification will be in accordance with the criteria classification listed above.
Design		
5. Floor plans, infrastructure plans	U	UNCLASSIFIED for all plans depicting structural walls only (general construction).
	C	CONFIDENTIAL for all floor plans, internal configurations, furniture plans, infrastructure plans, etc.

Table IV-3		
Subject	**Classification/ Sensitivity Level**	**Remarks**
6. Identification of office spaces	U	UNCLASSIFIED when signage or labels identify the space using generic terms (e.g. office, reception area, corridor, restroom, mechanical spaces, etc.). NOTE: Location(s) of safe haven/area(s) is Unclassified.
	C	CONFIDENTIAL when signage or labels identify office occupants listed in the unclassified space program (e.g. PCC). UNCLASSIFIED after accreditation and building occupancy.
	S	SECRET when signage or labels identifies the area as a Sensitive Compartmented Information Facility (SCIF), Shielded Environment, or a Tenant not listed in the unclassified space program.
7. Penetrations through the PCC six-sided perimeter	U	UNCLASSIFIED when location of penetration is noted (e.g. the two inch penetration above the vault door).
	C	CONFIDENTIAL when purpose of penetration is identified (e.g. the two inch penetration above the vault door used for the telephone system).
Operations		
8. Operations and Repair Manuals	U	UNCLASSIFIED when not associated with a specific area of the building.
	U	UNCLASSIFIED when associated with PCC specific area (e.g. PCC Fire Alarm Repair Manual, PCC Air Handler Manual, etc.). Manuals for classified systems are to be considered classified to the level of the associated system.
9. Results of tests and inspections	U	UNCLASSIFIED for all test and inspection results not specifically linked to the PCC.

Table IV-3		
Subject	**Classification/ Sensitivity Level**	**Remarks**
	SBU	SENSITIVE BUT UNCLASSIFIED for all test and inspection results linked to equipment external to the PCC, but dedicated to the PCC (e.g. HVAC, generator). Refer to 12 FAH-6 H-600 for specifics and limitations.
	S/NF	SECRET/NOFORN when associated with the PCC (e.g. PCC HVAC Inspection Report).
	S/NF	SECRET/NOFORN when vulnerabilities are identified that could affect the security of classified information.

Table IV-4		
Subject	**Classification/ Sensitivity Level**	**Remarks**
Shielded Environments/Red Power Systems – Applicable in Restricted CAA, Core CAA, and PCC – Excluding: Emergency Power Systems, Telecommunications & Technical Security		Shielded Environments include but are not limited to CSE, RFSE, SE, MTCR, and BCR.
		Isolated Power Systems (IPS) include but are not limited to isolation transformers, motor generator sets, power line filters, wave guides, etc.
Non Site-Specific		
1. Generic Criteria	C	CONFIDENTIAL when listed as a generic requirement at all locations (e.g. all unclassified – local area network (U-LAN) computer systems shall ___).
2. Design Standards	C	CONFIDENTIAL when listed as a generic requirement at all locations (e.g. all U-LAN computer systems shall ___).
3. Test Procedures and Results	C	CONFIDENTIAL when commercially available procedures for Shielded Environments or IPS results are indicated.
	C	CONFIDENTIAL for U.S. government-designed test procedures and results.
Site-Specific		See Appendix for definition of 'Site-Specific'
Design Requirements		
4. Criteria	C	CONFIDENTIAL when the absence or presence of a Shielded Environment is noted.
	C	CONFIDENTIAL when the absence or presence of an IPS is noted.

Table IV-4		
Subject	**Classification/ Sensitivity Level**	**Remarks**
5. Design-Standards (generic and standardized graphics and details)	S	SECRET when Shielded Environments or IPS specifications, model numbers, capabilities, specific locations, connections, internal configurations, etc. are noted.
6. Proposed or existing features	S	SECRET when Shielded Environments or IPS specifications, model numbers, capabilities, specific locations, connections, internal configurations, etc. are noted.
Design		
7. Floor plans, infrastructure plans	S	SECRET when Shielded Environments or IPS specifications, model numbers, capabilities, specific locations, connections, internal configurations, etc. are noted.
8. Identification of office spaces/systems	S	SECRET when the absence or presence of a Shielded Environment is noted.
	S	SECRET when the absence or presence of an IPS is noted.
Operations		
9. Operations and Repair Manuals	C	CONFIDENTIAL when the manual identifies the presence of a Shielded Environment or IPS (e.g. PCC Shielded Enclosure Maintenance Manual).
	S	SECRET when the manual identifies the presence of a specific type, capabilities, model, etc. of the Shielded Environment or IPS (e.g. PCC Lindgren Series X Shielded Enclosure specifications).

Table IV-4		
Subject	**Classification/ Sensitivity Level**	**Remarks**
10. Results of tests and inspections	C	CONFIDENTIAL when the test or inspection identifies the presence of a Shielded Environment or IPS (e.g. the PCC shielded enclosure was tested for isolation).
	S	SECRET when the test or inspection identifies a specific type, capabilities, model, vulnerability, etc. of the Shielded Environment or IPS (e.g. the Red Power System isolation was X ohms).
	S	SECRET when the vulnerabilities are identified that could affect the security of classified information.

Table IV-5		
Subject	**Classification/ Sensitivity Level**	**Remarks**
PCC DEDICATED EMERGENCY POWER SYSTEMS		
Non Site-Specific		
1. Generic Criteria	U	UNCLASSIFIED for PCC general emergency power requirements (e.g. total loading, Forced-Entry/Ballistic Resistant (FE/BR) protection, air flow, fuel tank, etc.).
2. Design Standards	C	CONFIDENTIAL for PCC specific emergency power requirements (e.g. specific system loads, point-to-point connections, etc.).
Site-Specific		
Design Requirements		
3. Criteria	C	CONFIDENTIAL for portion of emergency system exclusively dedicated to the PCC.
4. Design Standards	C	CONFIDENTIAL for portion of emergency system exclusively dedicated to the PCC (e.g. load factors and specific performance requirements).
5. Proposed or Existing emergency power systems (including discussion of vulnerabilities)	C	CONFIDENTIAL for portion of emergency system exclusively dedicated to the PCC.
	S	SECRET when vulnerabilities are identified for portion of emergency system exclusively dedicated to the PCC.
Design		
6. Location and/or capacity (i.e. rating) of units. Location of remote controls. Load shedding or similar prioritization strategy details.	U	UNCLASSIFED when only the location of the PCC generator room is identified.
	U	UNCLASSIFIED for overall system capacity and ratings.

Table IV-5		
Subject	**Classification/ Sensitivity Level**	**Remarks**
	C	CONFIDENTIAL for remote controls, load shedding, wiring connections, point-to-point diagrams, etc. for all systems serviced by the PCC dedicated generator.
7. Services and infrastructure supporting the emergency power systems	U	UNCLASSIFIED for services and infrastructure originating outside the PCC generator room in support of the PCC generator room (e.g. fire suppression system, technical security system (TSS), HVAC, fuel lines, telephone, and lighting).
8. Location of equipment within the generator room	SBU	SENSITIVE BUT UNCLASSIFIED for location of PCC dedicated emergency power system components and conduit infrastructure (e.g. generator, automatic transfer switch, conduit routing between system components, etc.).
9. Facilities/offices and infrastructure supported by the generator	C	CONFIDENTIAL for all systems serviced by the PCC dedicated generator.
Operations		
10. Operations and Maintenance Manuals and parts lists	U	UNCLASSIFIED for the emergency power system services provided by the PCC dedicated generator.
11. Results of acceptance tests and maintenance inspections	U	UNCLASSIFIED for the emergency power system services provided by the PCC dedicated generator
	S	SECRET when vulnerabilities are identified that could affect the security of classified information.

Table IV-6		
Subject	**Classification/ Sensitivity Level**	**Remarks**
BLAST RESISTANCE		
Non Site-Specific		
1. Generic Criteria	SBU/REL FVEY	SBU/REL FVEY when a design basis threat (DBT) is quantified in terms of charge size and distance.
	SBU	SENSITIVE BUT UNCLASSIFIED when a DBT is expressed as a combination of pressure, impulse, and/or duration.
2. Design Guidelines	SBU/REL FVEY	SBU/REL FVEY when a DBT is quantified in terms of charge size and distance.
	SBU	SENSITIVE BUT UNCLASSIFIED when a DBT is expressed as a combination of pressure, impulse, and/or duration.
3. Research Tests and Results	U	
Site-Specific		
Design Requirements		
4. Criteria	SBU/REL FVEY	SBU/REL FVEY when the DBT is quantified in terms of charge size and distance.
	SBU	SENSITIVE BUT UNCLASSIFIED when the DBT is expressed as a combination of pressure, impulse, and/or duration.
5. Design Standards	SBU/REL FVEY	SBU/REL FVEY when the DBT is quantified in terms of charge size and distance.
	SBU	SENSITIVE BUT UNCLASSIFIED when the DBT is expressed as a combination of pressure, impulse, and/or duration.
6. Proposed or Existing blast resistant features (including vulnerability analyses and feasibility studies)	SBU/REL FVEY	SBU/REL FVEY when the DBT is quantified in terms of charge size and distance.

Table IV-6		
Subject	**Classification/ Sensitivity Level**	**Remarks**
	C	CONFIDENTIAL when vulnerabilities are quantified by any measurement (charge or pressure/impulse).
	SBU	SENSITIVE BUT UNCLASSIFIED when DBT is expressed as a combination of pressure, impulse, and/or duration.
Design		
7. Documentation related to materials and assemblies of blast resistant construction or features.	SBU/REL FVEY	SBU/REL FVEY when charge weights and distances are identified (e.g. calculations).
	C	CONFIDENTIAL when vulnerabilities are quantified by any measurement (charge or pressure/impulse).
	SBU	SENSITIVE BUT UNCLASSIFIED when design information is expressed as a combination of pressure, impulse, and/or duration.

Table IV-7		
Subject	**Classification/ Sensitivity Level**	**Remarks**
PHYSICAL SECURITY		
Non Site-Specific		
1. Generic Criteria	U	
2. Design Standards	U	
3. Research Tests and Results	U	
Site-Specific		
Design Requirements		
4. Criteria	U	
5. Design Standards	U	
6. Proposed or Existing physical security features	C	CONFIDENTIAL when vulnerabilities not visible to the general public are described (e.g. when documented in surveys or statements of work).
Design		
7. Documentation indicating location, materials, and assemblies of physical security features	U	
Operations		
8. Operations and Repair Manuals	U	
9. Results of surveys and inspections.	C	CONFIDENTIAL when vulnerabilities not visible to the general public are described (e.g. when documented in surveys or inspection reports).

Table IV-8		
Subject	**Classification/ Sensitivity Level**	**Remarks**
TECHNICAL SECURITY		Including but not limited to Closed Circuit Television (CCTV), Intrusion Detection Systems (IDS), access control systems, other technical countermeasures, etc.
Non Site-Specific		
1. Generic Criteria	U	
	C	CONFIDENTIAL for U.S. government-specific features of modified commercial off-the-shelf (COTS) IDS equipment protecting the CAA.
2. Design Standards	U	
3. Research Tests and Results	U	
Site-Specific		
Design Requirements		
4. Criteria	U	
	C	CONFIDENTIAL for U.S. government-specific features of modified COTS IDS equipment protecting the CAA.
5. Design Standards	U	
6. Proposed or Existing technical security features	U	
	C	CONFIDENTIAL for U.S. government-specific features of modified COTS equipment.
	C	CONFIDENTIAL when specific components are not readily visible to the general public and are protecting the CAA.
	S	SECRET when system is protecting Core CAA.
Design		
7. General Power	U	
	C	CONFIDENTIAL for power supply and back-up systems exclusively serving Core CAA.
8. Conduit runs including cabling where system or device	U	

Table IV-8		
Subject	**Classification/ Sensitivity Level**	**Remarks**
types (e.g. detection, deterrent, monitoring) are not indicated	C	CONFIDENTIAL for PCC and Shielded Environments. (See Table IV-3 'PCC' and Table IV-4 'Shielded Environments/Red Power Systems')
9. Detection, Deterrent, and Monitoring Devices	U	
	C	CONFIDENTIAL when location within CAA is not visible to visitors and model is identified or for U.S. government-specific features of modified COTS equipment.
	S	SECRET when model and location in Core CAA are identified.
10. Wiring Diagrams indicating point-to-point routing to the terminations of individual conductors (differentiates cabling plans)	U	
	C	CONFIDENTIAL for CAA.
	C	CONFIDENTIAL for U.S. government-specific features of modified COTS equipment.
	S	SECRET for Core CAA.
11. Control Panels	U	
	C	CONFIDENTIAL for U.S. government-specific features of modified COTS equipment.
Operations		
12. As-builts	SBU	SBU for chancery/consulate compounds.
	C	CONFIDENTIAL for CAA.
	S	SECRET for Core CAA.
13. Operations and Repair Manuals	U	UNCLASSIFIED when data is commercially available in the public domain.
	SBU	SBU for COTS IDS systems unique to the CAA.

Table IV-8		
Subject	**Classification/ Sensitivity Level**	**Remarks**
	C	CONFIDENTIAL for U.S. government-designed IDS equipment or U.S. government-specific features of COTS IDS systems protecting the CAA.
14. Results of surveys and inspections	U	
	S	SECRET for description or vulnerabilities of systems located in the CAA.
	S	SECRET for description or vulnerabilities of IDS systems protecting the Core CAA.

Table IV-9		
Subject	**Classification/ Sensitivity Level**	**Remarks**
TELECOMMUNICATIONS – Includes Unclassified-Local Area Network (U-LAN), Classified-Local Area Network (C-LAN), Building Automation System (BAS), and Telephone		
Non Site-Specific		
1. Generic Criteria	S	SECRET for U.S. government-specific features of modified COTS equipment that will process/store classified information.
	S	SECRET when countermeasures requirements are included.
2. Design Standards	S	SECRET for U.S. government-specific features of modified COTS equipment that will process/store classified information.
	S	SECRET when countermeasures requirements are included.
Site-Specific		
Design Requirements		
3. Design - Telephones		
3.1 Demarcation point between host country and post and/or between post service point and main telephone frame room in chancery/consulate	U	
3.2 Equipment and Distribution systems (e.g. conduit trays, outlet locations, configurations, and distribution of station sets)	U	UNCLASSIFIED for equipment or distribution details in Restricted CAA.
	C	CONFIDENTIAL for equipment or distribution details for Treated Environments (TEs) in Restricted CAA.
	C	CONFIDENTIAL for equipment or distribution details in Core CAA areas.

Table IV-9		
Subject	**Classification/ Sensitivity Level**	**Remarks**
3.3 Documentation of telephone cable routes and terminal assignments	C	CONFIDENTIAL for documentation detailing Restricted CAA.
	S	SECRET for documentation detailing TEs in Restricted CAA.
	S	SECRET for documentation detailing Core CAA.
3.4 Details of specific design techniques used to protect any element of the telephone system from technical threat or attack	S	SECRET when specific design techniques are identified as protecting the telephone system from technical threat, attack, or exploitation.
3.5 Location of emergency telephones	S	SECRET when located in Core CAA.
3.6 Acceptance test results and deficiency lists	S	SECRET when the test results and deficiency lists identify system vulnerabilities.
	S	SECRET when tests identify specific countermeasures.
	S	SECRET when vulnerabilities are identified.
4. Design – C-LAN or Other Classified Computer System		
4.1 Plans, details, specifications, and identification of specific models or equipment related to C-LAN	S	SECRET for all plans, details, specifications, and identification of specific models or equipment related to C-LAN infrastructure and equipment.
4.2 Distribution conduits and terminal boxes	SBU	SENSITIVE BUT UNCLASSIFIED when not identified as C-LAN.
	S	SECRET when identified as C-LAN infrastructure.

Table IV-9		
Subject	**Classification/ Sensitivity Level**	**Remarks**
4.3 Acceptance test results and deficiency lists	C	CONFIDENTIAL for test results that detail system specifications or that identifies specific models or equipment.
	S	SECRET when tests identify specific countermeasures.
	S	SECRET when vulnerabilities are identified.
5. Design – U-LAN, BAS	SBU	SENSITIVE BUT UNCLASSIFIED for equipment or distribution details in Restricted CAA.
	C	CONFIDENTIAL for equipment or distribution details for TEs in Restricted CAA.
	S	SECRET for equipment or distribution details in Core CAA.
6. Telephone emergency service restoration plans, diagrams, repairs, parts lists, etc.	U	UNCLASSIFIED when related to Restricted CAA.
	S	SECRET when related to TEs in Restricted CAA.
	S	SECRET when related to Core CAA.
7. C-LAN emergency service restoration plans, diagrams, repairs, parts lists, etc.	S	SECRET when related to Restricted CAA.
	S	SECRET when related to TEs in Restricted CAA.
	S	SECRET when related to Core CAA.
8. Telephone Lists	U	UNCLASSIFIED for abbreviated phone listings showing key personnel and organizations or alphabetical listings.
	C	CONFIDENTIAL for telephone directories that contain complete phone and organizational listings.

Table IV-10		
Subject	**Classification/ Sensitivity Level**	**Remarks**
SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIFs)		For SCIFs located within Chief of Mission facilities abroad.
1. Generic Criteria	U	UNCLASSIFIED knowing the existence of one or more SCIFs within a building.
	C	CONFIDENTIAL Director of National Intelligence (DNI) standards, either by description or by graphics, to the design of a specific SCIF construction or renovation project.
2. Design Requirements	C	CONFIDENTIAL for specific location of a SCIF within a building (as identified by room number, organization, assigned personnel, or any other identifying information).
	C	CONFIDENTIAL for internal layout/office configuration of a SCIF.
	C	CONFIDENTIAL for identification of furnishings for a SCIF.
	C	CONFIDENTIAL for the identification of any alternative countermeasures used to meet DNI standards in place of specified countermeasures.
	S	SECRET for the facility type (e.g. open storage, closed storage, continuous operations, etc.) for which a specific SCIF is accredited.

Table IV-10		
Subject	**Classification/ Sensitivity Level**	**Remarks**
3. Proposed or existing features	C	CONFIDENTIAL for specific references to the presence or absence of an acoustic or radio frequency (RF) shielded environment (parent room), Shielded Enclosure (SE), Certified Shielded Enclosure (CSE), Acoustic Conference Room (ACR), etc., within a SCIF. SECRET for the specific reference to the presence or absence of the above at Critical Technical Threat Posts or High Vulnerability Buildings.
	S	SECRET for the identification of any physical, technical, or procedural vulnerabilities of a SCIF.
4. Operations	C	CONFIDENTIAL for the identification of any Sensitive Compartmented Information (SCI) accredited information technology (IT) systems, including the identity of the controlling organization or agency installed in a specific SCIF.
	C	CONFIDENTIAL for the identification of any Sensitive Compartmented Information (SCI) telephone system or video teleconferencing system installed in a specific SCIF.
	S	SECRET for all system specifications/capabilities, telephone components, and/or IT configurations.
	S	SECRET for the identification of specific technical security systems installed in a SCIF, the system specifications, and the associated infrastructure.
	S	SECRET for the compartments (SI/TK/G/HCS, etc.), for which a specific SCIF is accredited.

APPENDIX A - Acronyms

AIS – Automated Information System
ASTM – American Society for Testing & Materials
BAS – Building Automation System
BCR – Built-in Conference Room
BOM – Bill of Materials
BR – Ballistic Resistant
C – Confidential
CAA – Controlled Access Area
CAD – Computer Aided Design
CADD – Computer Aided Drafting and Design (now synonymous with CAD)
CATV – Cable television
CCTV – Closed-circuit television
CD – Compact Disk
C-LAN – Classified Local Area Network
CMPD – Compound
CMR – Chief of Mission Residence
CO – Contracting Officer
COB – Consulate Office Building
CON – Construction
COR – Contracting Officer's Representative
COTS – Commercial off-the-shelf
CSE – Certified Shielded Enclosure
CSMS – Comprehensive Security Monitoring System
DAS – Deputy Assistant Secretary
DCMR – Deputy Chief of Mission Residence
DECL – Declassify
DES – Data Encryption Standard
DoD – Department of Defense
DoS – Department of State
DSS – Diplomatic Security Service
FCL – Facility Security Clearance
FIPS – Federal Information Processing Standards
FE – Forced Entry
FSN – Foreign Service National
GFE – Government Furnished Equipment
GFI – Government Furnished Information
HVAC – Heating, Ventilating, and Air Conditioning
IDS – Intrusion Detection System
IOB – Interim Office Building
IPS – Isolated Power System
LAA – Limited Access Area
MSG – Marine Security Guard
MSGQ – Marine Security Guard Quarters
MTCR – Modular Treated Conference Room
NIC – Noise Interference Coefficient

NISP – National Industrial Security Program
NISPOM – National Industrial Security Program Operating Manual
NOB – New Office Building
NOFORN – No Foreign Dissemination
OBO – Overseas Buildings Operations
OBC – Office Building Chancery
OBX – Office Building Annex
OPR – Office of Primary Responsibility
PAC – Public Access Control
PBX – Private Branch Exchange
PC – Personal Computer
PCC – Post Communications Center
PDS – Protected Distribution System
PR – Parent Room
REL FYEY – Releasable To Five Eyes
RF – Radio Frequency
RFSE – Radio Frequency Shielded Enclosure
RMS – Roof Maintenance Shed
S – Secret
SBU – Sensitive But Unclassified
SCC – Security Control Center/Console
SCIF – Sensitive Compartmented Information Facility
SE – Shielded Enclosure/Environment
SIC – Security Interface Cabinet
SMSe – Security Management System enterprise
STE – Secure Terminal Equipment
STU –Secure Telephone Unit (obsolete term)
TE – Treated Environment
TS – Top Secret
TSCM – Technical Surveillance Countermeasures
U – Unclassified
U-LAN – Unclassified Local Area Network
UPS – Un-interruptible Power Supply/Source
USG – U.S. government

APPENDIX B - Definitions

The following definitions are to be used in conjunction with this guide:

Assembly - a combining of parts/materials to achieve a stated purpose (e.g. wall type).

Automated Information System - an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information (source: E.O. 12958).

Building - a singular structure.

Capability - the design limits of a product, system, assembly, or material.

Compound - see 'Facility'

Controlled Access Area - specifically designated areas within a building where classified information may be handled, stored, discussed, or processed. CAAs contain two categories of spaces; core and restricted.

Core - one of two categories of space (the other being Restricted) within a Controlled Access Area. It requires among the highest levels of protection and requires more stringent access control than the Restricted Area of the CAA. This area usually includes the PCC and other functional activities. (Note: This guide's use of the term 'core' differs from the industry standard that identifies the core of a building as the area containing elevators, fire stairs, restrooms, mechanical shafts, and other similar elements. These elements are usually consolidated and located in the center of mid-rise and high-rise buildings.)

Core Suite - a space in the Core comprised of an organized group of offices and individuals.

Defined - interpreted or elaborated.

Described - narrative or graphic depiction.

Delineated - graphic depiction.

Facility - a property comprising an assembly of one or more buildings.

Functional Area - office or suite of offices.

Generic Design - non-project specific depictions of spaces, adjacencies, or configurations prepared to illustrate requirements or guidelines.

Graphic - image.

Quantified - numerically defined.

Physical Security - an assembly or assemblies (using building materials and/or site features) that is designed to resist unauthorized or forced-entry and attack (by using hand tools, firearms, or other similar weapons). Designed to complement technical security.

Parent Room - a room that houses a SE and is separated by walls/partitions from other similar parts of the structure or building.

Post - a recognized mission that conducts the primary foreign affairs of the U.S. in the host country. The mission may comprise more than one parcel of land, but is usually located in the same city (or metropolitan area).

Prescribed - ordered the use of.

Restricted Area - one of two categories of space (the other being CORE) within a Controlled Access Area. An area in which cleared Americans work and to which other persons may be admitted only with a cleared American escort.

Sensitive But Unclassified - is a handling instruction used to distinguish between unclassified sensitive information and non-sensitive information. Examples are Privacy Act of 1974 data, personnel information, and derogatory information developed during a background investigation. For design and construction projects, examples would be graphic depictions of floor plans for foreign affairs offices and representational housing overseas. (See also Table IV-1, 6) It is not a classification level and replaced "Limited Official Use." Note**:** Floor plans posted within the facility for the purpose of depicting emergency evacuation routes are not considered SBU under this definition**.**

Site Specific - pertains to a specific country (or location therein) where the U.S. maintains or proposes a chancery, consulate, or annex. Also pertains to information that is sufficiently unique to identify its site with relative ease (e.g. a uniquely-shaped floor plan, site plans, key plans, street names, photographs, names of local consultants, or inclusion of landmarks).

Standardized Designs - depictions of design solutions for a specific set of identified projects.

Technical Security - a system or systems that uses an electrical power source and contains components designed to deter, detect, or monitor hostile attempts to surveil, harm, or compromise a facility or its occupants.

Telecommunications - the preparation, transmission, or communication of information by electronic means (source: E.O. 12958). (From a DoS wire management perspective, this applies to systems utilizing low voltage wiring. However, technical security has been excluded for the purposes of this guide.)

TSCM - technical surveillance countermeasures.

Treated Environment - a space designed to protect from acoustic or electromagnetic radiation. A manufactured or modular space.

U - unclassified.

ULAN - unclassified local area network.

UPS - un-interruptible power supply source.

Visible to the General Public - can be readily seen from off the compound, on the compound, Public Access Control (PAC) areas, or Public Access Areas (PAA).

Vulnerability - the deficiency of a product, system, assembly, or material to meet a stated requirement.

APPENDIX C

Handling Instructions for Classified, SBU and Unclassified Material

1. GENERAL INFORMATION

a. Interpretations and Clarifications: For Contractors, any project-specific requests for interpretations and clarifications should be forwarded through your facility security officer to your Contracting Officer (CO). In the case of Department of State employees, requests should be forwarded through your facility security officer to:

Office of Physical Security Programs
Bureau of Diplomatic Security
U.S. Department of State
Rosslyn, VA 22209
(703) 312-3089

Should the requestor disagree with the determination made by DS/PSP, he/she may seek adjudication through:

Office of Information Security
Bureau of Diplomatic Security
SA-20, Room C04
U.S. Department of State
Rosslyn, VA 22209

b. **Tentative Classification:** Personnel who have reason to believe that unclassified information should be classified or that classified information should be upgraded, are instructed to protect the information as though it is classified at that level by marking as follows:

"Classification/Sensitivity determination pending.
Protect as [classification/sensitivity level]."

Subsequently, clarification shall be sought following the guidance in paragraph 1.a above.

c. Downgrading and Declassifying Information: Where classified information is found that can possibly be downgraded/declassified, your facility security officer

should be contacted for a determination. (The facility security officer should contact the CO, or in the case of DoS employees, DS/C/PSP for clarification). Once a determination has been made, the classification shall be crossed-through, initialed and dated by the person making the change. The following notation shall be affixed (as applicable):

"Downgraded/declassified/redesignated to [*insert new classification*] per Part 3 of E.O. 13526, pursuant to U.S. DoS Security Classification Guide for Design and Construction of Overseas Facilities, dated [*issue date*]" U.S. Department of State Security Classification Guide May 2003 30-42.

The holder of any material approaching its review/declassification date shall contact his/her facility security officer for a determination on its continued classification or declassification. If guidance is not received prior to the date indicated, no automatic declassification shall take place until instructions are received from the Contracting Officer, or in the case of DoS employees, the facility security officer.

d. Declassification Instructions: Review and/or declassification guidance is provided for individual topics of information contained in this guide. That guidance is not intended to provide automatic declassification instruction. Holders that do not receive additional guidance prior to the indicated declassification point should not take automatic declassification action but must confirm and receive instructions from the DoS.

2. CLASSIFIED MATERIAL

a. Handling: Confidential (C) and Secret (S) material shall be handled in accordance with E.O. 13526 and the provisions in the NISPOM (for domestic contractors) and Department of State 12 FAM policies and procedures (for U.S. government employees domestically). All employees and contractors under Chief of Mission authority must also adhere to the provisions of 12 FAH-6. A summation of the most common handling provisions is provided below. Top Secret (TS) materials require additional protection and specific handling methods which will be provided when handling of such material is necessary.

b. Marking of Classified Material: All classified materials (including working papers and drawings) shall be marked with the appropriate classification level in accordance with E.O. 13526 and the provisions in the NISPOM (for contractors) and **5 FAM 480** policies and procedures (for government employees).

a. See Figure 1.

1.) Any document or set of documents containing classified information shall be marked with the highest level contained therein. The front page (or front and back cover if appropriate) shall be marked with the highest overall classification of the document at the top and bottom of the page. Downgrading or declassification instructions shall be shown at the bottom of the first page (or front cover if appropriate).

2.) Internal pages within the document will be marked with either the overall classification of the document or with a marking indicating the highest classification level of information (to include UNCLASSIFIED) contained on that page. Paragraphs within a text document will be individually marked (i.e. portion marked).

3.) Sets of documents large enough to be folded or rolled shall be marked so that the marking is visible on the outside of the set when it is rolled or folded. In addition, all classified project information shall contain the following label on the front cover, title sheet or first page (for classified plans and drawings the label shall be applied to each drawing):

> Derived from: DS Security Classification Guide for Design and Construction of Overseas Facilities [insert date of issuance of guide]
> Declassify On: [insert text as prescribed in part IV of this guide]

Every effort should be made to keep the subject and titles of classified documents unclassified and appropriately marked as such.

MARKING

The following examples of marking are provided for information. Marking of documents will vary based on the classification authority used (see figure 1). NOTE: Classified e-mail correspondence must also be appropriately marked with the overall classification of the e-mail, portion/paragraph marking and classification and declassification authorities. Classified Computer Media also requires appropriate marking (see figure 2).

Classifying Correspondence

(Classified For Training Purposes Only)

Date: XXX X, XXXX

SECRET
MEMORANDUM

TO: OBO Office XXX

FROM: DoS Office XXX

SUBJECT: Compromise of Reports (U)

1. (S) Enclosed, you will find the three Reports which were compromised by John Doe.

2. (C) Per E.O. 13526 you are requested to conduct a damage assessment to determine the damage to national security and to the activities in your organization..

3. (S) Per the XXX, DOE compromised more than we were aware of and will not talk further to any U.S. government official until he gets a daily ration of ice cream. This is all we know at present.

4. (U) Point of contact for this information is XXX,

DERIVED FROM: OBO SCG, dated _____
DECLASSIFY ON: (Date)

Figure 1

Identifying Classified Computer Media

Show classification on all removable electronic storage media, *including unclassified*.

Mark *ALL* types of removable electronic media (hard-drives, CD-R, floppies, etc.).

You may stamp, label, or hand-write the markings.

Figure 2

4.) All classified documents shall bear the proper name of the site/project. In addition, drawings, specifications and other similar products that document the design, construction or installation of equipment, etc. at overseas DoS facilities shall carry the following notice conspicuously displayed on the cover of all bound documents (or on each page of loose sheets):

WARNING: This document is the property of the U.S. government. Further reproduction and/or distribution outside the contractor team is prohibited without the express written approval of:

U.S. Department of State
ATTN: [name of Contracting Officer]
Washington, D.C. 20520

c. Access: All contractors (firms and individuals) requiring access to or generation of classified national security information (including those involved in the acquisition process) shall be cleared by the Department's Industrial Security Division (DS/IS/IND) prior to initiation of any activities involving the receipt or development of classified information. Prime contractors must possess a Secret Facility Clearance (FCL) and Secret safeguarding capability issued by the Defense Security Service (DSS), Columbus, Ohio. Subcontractors working on classified information or in classified areas must also possess a Secret FCL issued by DSS and may require safeguarding capabilities as required by the respective contract. Refer to the DD 254, Contract Security Classification Specification for more information.

d. Reproduction: Reproduction of classified information shall be kept to a minimum and accomplished by cleared personnel. The material cannot be reproduced if the originator prohibits it and the document is so annotated. Reproduced classified copies are subject to the same accountability and controls as the original. Only equipment approved by the facility security officer may be used to reproduce classified information. The equipment must be approved for the classification level of the information, or higher.

e. Electronic Processing and Distribution: Classified information shall be processed and distributed only on systems approved for handling classified material at that level or higher.

f. Wrapping (for hand carrying or use of a mail or courier service):
Transmission of classified information from one cleared facility to another must be wrapped in an opaque inner and outer cover. The inner cover shall be a sealed wrapper or envelope, clearly marked with the assigned classification and the addresses of both the sender and receiver.

A receipt shall be attached to the inner cover and returned to the sender upon receipt. The outer cover shall be sealed and addressed, but shall not identify the contents as classified.

g. Mailing (hand carrying and use of mail or courier service):

(1) Proper address: Only approved addresses can be used by contractors to receive classified information. Therefore, U.S. government employees sending classified information to contractors or others should contact DS/IS/IND to verify the proper address for recipient.

(2) Hand carrying: Properly wrapped classified information may be hand carried by appropriately cleared individuals appointed and briefed by the facility security officer. The individual must retain the material in his/her possession at all times. Further instructions are provided in NISPOM 5-410.

(3) Domestic Mail Service: Defined as within the 50 States, the District of Columbia, Commonwealth of Puerto Rico or other U.S. possession, mail facilities of the U.S. Army, Navy or Air Force, or other U.S. post office provided the material never leaves U.S. citizen employee control.

(a) UNCLASSIFIED and **SENSITIVE BUT UNCLASSIFIED** material may be sent via the U.S. Postal Service (USPS), commercial transportation companies, and international mail in sealed, addressed envelopes with no markings as to sensitivity of the information.

(b) CONFIDENTIAL and **SECRET** material may be sent domestically via USPS Registered Mail with overnight delivery service requiring a signature upon receipt. The classified material is placed in an inner sealed, addressed envelope identified with the appropriate classification marking, which is then placed in an outer sealed, addressed envelope with no marking as to classification. Within the Department, only cleared U.S. citizens must handle USPS Registered Mail.

See **14 FAH-4 H-315** for procedures for sending classified items by USPS Registered Mail. See **12 FAM 536.9-3 (3)** for sending classified items by USPS Express Mail, where the waiver-of-signature block must not be executed.

(c) CONFIDENTIAL and **SECRET** material may be sent domestically via commercial transportation companies with overnight delivery service requiring a signature upon receipt. The classified material is placed in an inner sealed, addressed envelope identified with the appropriate classification marking, which is then placed in an outer sealed, addressed envelope with no marking as to classification. No waiver-of-indemnity and signature block may be executed. These envelopes must be addressed to an employee with the appropriate clearance level. See **14 FAH-4 H-320** for procedures for sending classified items by commercial transportation companies.

DOMESTIC to OVERSEAS: All classified material sent to posts abroad must be sent via the Diplomatic Pouch and Mail (DPM) system and accompanied by an appropriately designated Diplomatic Courier. Use of commercial courier firms, express carriers (FedEx, DHL or UPS), USPS, or hand-carrying classified information across international borders by an unauthorized courier is strictly prohibited. There are no exceptions to this policy. To properly package classified documents/drawings for shipment via the DPM system that originates from a DoS domestic facility:

- Place it in an envelope/container and seal the edges and all seams with reinforced tamper-proof tape. A best practice is to place your signature along all the edges of the tape as an added measure to detect tampering.
- Affix the intended recipient's name and official address, and conspicuously mark the envelope/container on all sides with the appropriate classification level. This will alleviate any doubt that as to whether there is classified information in the package.
- DO NOT double-wrap this package. The diplomatic pouch bag creates the second outer cover. Double wrapping is the primary reason why classified packages sometimes make their way to the unclassified pouch.
- Attach a properly completed Form OF-120, Diplomatic Pouch Mail Registration.
- Take the package to your mailroom and ensure the mail clerk understands the contents are classified. Do not drop off your classified material at a location

without a clerk. The receiving mailroom clerk is ultimately responsible for ensuring properly identified classified packages are entered into the classified DPM system. The interoffice mail couriers will pick up the material and drop it off at SA-8 via HST.

If a domestically assigned employee or contractor working in a domestic facility receives classified material/drawings appropriately sent from domestic contractor addresses for placement in the DPM system they must remove the outer wrapping and properly prepare it for shipping according to the above instructions before taking it to the mailroom for onward shipment to a post abroad. If not properly packaged, this classified material could be improperly placed in the unclassified mail system and you could be held liable for a security violation.

h. Storage: Confidential or Secret information must be stored in a GSA-approved container in an accredited facility domestically or in a CAA abroad.

i. Public Release of Classified Information: Information relating to an overseas project is not authorized for release to any non-U.S. government entity without the specific written approval of the Assistant Secretary for the Bureau of Diplomatic Security. In addition, foreign disclosure of classified information must comply with the national disclosure policy prior to any prime contract or subcontract award to any reciprocally cleared firm. This policy requires that U.S. classified information, which is intended for release to a foreign owned U.S. contractor, must be approved for release to the government of that country.

The foreign government concerned must have entered into a security agreement with the U. S. Government under which the foreign government agrees to protect U. S. classified information at a level commensurate with U.S. government standards.

j. Disposal: Classified material shall be destroyed in a manner conforming to the procedures stipulated for destruction of classified material in NISPOM or 12 FAM. For example, hardcopy materials may be destroyed by burning, chemical treatment, or shredding. Your facility security officer is responsible for coordination of all disposal activities and should be consulted prior to the disposal of any classified material. When directed by the CO, the documents may also be returned to the DoS for retention or destruction.

3. SENSITIVE BUT UNCLASSIFIED (SBU) and SBU-NOFORN MATERIAL

a. Marking: SBU information relating to design and construction of diplomatic missions shall be marked with the appropriate sensitivity level (e.g. SBU or SBU-NOFORN). This requirement is in addition to those outlined in E.O. 13526 and 12 FAM 540. Questions regarding this additional marking requirement should be directed to Chief, DS/IS/APD. SBU documents shall bear the proper name of the site/project. In addition, drawings, specifications and other similar products that document the design, construction or installation of equipment, etc. at overseas DoS facilities shall carry the following notice conspicuously displayed on the cover of all bound documents (or on each page of loose sheets):

> WARNING: This document is the property of the U.S. government. Further reproduction and/or distribution outside the contractor team is prohibited without the express written approval of:
>
> U.S. Department of State
> ATTN: [name of Contracting Officer]
> Washington, D.C. 20520
> U.S. Department of State Security Classification Guide
> May 2003 34-42

b. Access: U.S. citizen, direct hire, supervisory employees are responsible for access, dissemination and release of SBU material.

c. Reproduction and Dissemination: Government and Contractor employees may reproduce and circulate SBU material to others, including Foreign Service Nationals (FSNs), to carry out official functions, if not otherwise prohibited by law, regulation, or inter-agency agreement. NOTE: "SBU-NOFORN" (meaning No Foreign Dissemination) is a handling restriction that prohibits release of the material to FSNs.

d. Electronic Distribution (email, files and attachments)**:** SBU-NOFORN material may only be created, stored, and transmitted on C-LAN and may not be transmitted via the Internet or DoS Intranet. All other SBU material may be transmitted via DOS Intranet or via ProjNet. All other SBU may also be transmitted across the Internet if the information is encrypted in accordance with the FIPS 140-1A (DES III) standard. DS Analysis and Certification Division certification of the encryption scheme is required before SBU may be transmitted

across the Internet. SBU-NOFORN shall be transmitted via classified facsimile transmission equipment. All other SBU information may be transmitted via unclassified facsimile transmission equipment.

e. Mailing: SBU information may be sent via the USPS or express mail services (e.g. DHL, FEDEx) provided it is packaged in a way that does not disclose its contents or the fact that it is SBU. Local courier services, domestically, are considered to be express mail services under the conditions of this requirement.

f. Storage: During non-working hours, SBU information shall be secured within a locked office or suite, or secured in a locked container. If the building is secured after nonworking hours (and/or guarded) the SBU information does not need to be secured within a locked office or suite, or secured in a locked container. However, at a minimum, the SBU information should at least be covered up.

g. Disposal: All excess copies of SBU documents or information, including sketches, notes, working papers, drafts, etc., must be destroyed by a method approved for classified information as noted in Paragraph C.2.j.

4. UNCLASSIFIED MATERIAL

a. Marking/Labeling of Documents: Unclassified documents shall bear the proper name of the site/project. In addition, drawings, specifications and other similar products that document the design, construction or installation of equipment, etc. at overseas DoS facilities shall carry the following notice conspicuously displayed on the cover of all bound documents (or on each page of loose sheets):

WARNING: This document is the property of the U.S. government. Further reproduction and/or distribution outside the contractor team is prohibited without the express written approval of:

APPENDIX D - Frequently Asked Questions (FAQ's)

Topic 1: Classification of Information

Question: I've read the classification guide and have begun to develop site specific designs, but I am not sure if that design is classified or not. What do I do and whom do I contact?

Answer: If you are not certain about the classification of the information or design, refer to Appendix C, paragraph 1.b.

Topic 2: Classified Information

Question: I've read the definitions of sensitive and classified information (i.e. SBU, Confidential, etc.), but I still don't really understand them. Can you provide examples?

Answer: Examples of sensitive and classified information based on level of sensitivity or classification.

- Sensitive But Unclassified - For design and construction projects, graphic depictions of floor plans for foreign affairs offices and representational housing overseas. (See also Table IV-1, 6.)
  NOTE: Floor plans posted within the facility for the purpose of depicting emergency evacuation routes are not considered SBU under this definition**.**
- Sensitive But Unclassified, No Foreigner Dissemination - Operations manuals for PCC-unique equipment.
- Confidential - General information about the nature of a secure environment (i.e. location, size, or arrangement) designed to permit conversations with little chance of eavesdropping.
- Secret - Details about the design of a secure environment (i.e. types of countermeasures, security systems, or performance standards) that permit conversations with little chance of eavesdropping.
- Top Secret - A Cryptographic key.

Topic 3: Classified Information versus Secure Procurement

Question: Is the furniture in the PCC classified?

Answer: No, but this can seem like a bit of a trick question. The depiction of the furniture (as shown on drawings) is classified information (as it reveals the internal configuration of the PCC). The actual goods are not. To ensure that the furniture is not compromised, the furniture must be procured in a secure manner. Procurement requirements for material bound for CAAs are articulated in 12 FAH-6. For each project involving CAAs, a Construction Security Plan (CSP), which incorporates the policy in 12 FAH-6, is prepared by a U.S. government representative (usually OBO, a tenant, or post). The CSP is approved by the Bureau of Diplomatic Security (DS).

Topic 4: Classified-LAN (C-LAN) design

Question: Can cable trays or cabling diagrams for the Classified LAN (C-LAN) system be shown on unclassified drawings?

Answer: The only instances where this is permitted is when the tray or diagram is located in restricted space and there is no indication that it is intended for use as a C-LAN run.

Topic 5: Compilation of Information

Question: How can the compilation of unclassified information result in the disclosure of classified information?

Answer: Below is a real example of how classified information was inadvertently disclosed and this edition of the Security Classification Guide has been structured to close this particular loophole. Nonetheless, this example conveys the kind of conditions that can result in inadvertent disclosures and potential security violations.

> In attempting to preclude the need to classify information about the presence of a Certified Shielded Enclosure (CSE) at a specific site, Person A refers to the site as Site Bingo and states that Site Bingo has a CSE. Person B is a contractor who submits drawings for the CSE to be reviewed by Person A's team. When the submittal is forwarded to Person A, it is attached to a specific contract number, which Person C uses to prepare the review comments. Since the contract number is attributed to a specific site, it can now be determined which site the CSE is located and thus, Confidential information available through unclassified means.
>
> Person A should not have used a fictitious name for the location because it creates a false sense of security. This edition of the SCG precludes the use of fictitious names.
>
> Person B created the ability to link the drawings to a specific site by referencing a contract number. Person B was simply following guidance from the Contracting Officer stating that all contract correspondence and submittals shall bear the contract number.
>
> Person C is unaware of the arrangement that A and B had developed regarding site naming and simply provided the proper site name to the tasker to ensure the documents got to the correct reviewers.

Topic 6: Controlled Unclassified Information

Question: I understand that the Federal Government has adopted the term "Controlled Unclassified Information" (CUI) for all information that is currently described as "Sensitive But Unclassified" (SBU) information. Should I now be using the term "CUI" instead of SBU?

Answer: No. DoS, much like the rest of the Federal Government, will be converting to the use of CUI over time. However, as of the publication date of this document the Department has not completed the conversion.

Topic 7: Declassification

Question: In reviewing classified documents, I see a 'Declassify On: 1 April 2030 (or some other date)' on the document. Does this mean that the document will be declassified on that date?

Answer: Not necessarily. Executive Order requires that all classified documents include a declassification date at which time a determination will be made as whether the information needs continuing protection or it may be declassified. For the DoS, the Office of Records Property Services (A/RPS) performs that review.

Topic 8: Emergency Generators

Questions: Please clarify when information regarding generators becomes classified?

Answer: For generators exclusively dedicated to the PCC, the systems supporting the generator itself are not classified. However, the power and signal lines that serve the PCC become classified information at the point they leave the generator room. Information indicating their routing, sizes, and capacities need to be protected as classified information.

Question: Is the capacity of the fuel tank classified?

Answer: No

Question: How about the size of the generator?

Answer: No

Topic 9: Room Names on Floor Plans

Question: Can you please clarify the requirements for labeling spaces on design documents? Specifically address the extent to which drawings may identify specific occupants and uses of spaces within a building.

Answer: Room functions and occupants such as Chief of Mission, Management Officer, Cashier Booth, Post 1, Waiting Room, and other terms used in the unclassified Space Requirements Program may be used on SBU drawings. The exception is the interior configuration of Core Areas, including the Type II Conference Room(s), shall be on Confidential drawings. (Refer to Table IV-1, items 6, 9, 11, and 13)

While SBU material may be provided to others who have a need to know, including host country officials, the U.S. government desires to minimize the amount of SBU information released. Public release must be approved in advance, and must comply with the respective contract requirements as well as with the requirements of Appendix C of this SCG.

Topic 10: FSNs

Question: Per paragraph c on page 34, who is considered a FSN (Foreign Service National)?

Answer: In its simplest terms, an FSN is a non-U.S. citizen. The term is usually used in association with a non-U.S. citizen employed at one of the Department's overseas missions or working on a project at one of those missions.

Topic 11: Limit Drawings and Project Pseudonyms

Question: Previously the use of limit drawings and pseudonyms was permitted to avert classification by avoiding/masking site specificity. Is this still permitted?

Answer: The use of “Limit Drawings” and project pseudonyms does not provide adequate protection in accordance with this guide. See paragraphs 2.b.4, 3.a, and most importantly paragraph 4.a. of Appendix C for more guidance.

Topic 12: O&M Manuals

Question: Are the Operations and Maintenance (O&M) manuals associated with equipment or systems wholly located in the PCC classified information?

Answer: When O&M manuals are published, COTS, they are not classified. However, they shall be handled as SBU/NOFORN.

Question: What about for equipment and systems supporting (exterior to) the PCC?

Answer: If they are unique to the PCC, then they are to be handled as Unclassified. See Table 3.10.

Topic 13: Penetrations

Question: I am about to draw some pipe penetrations through the vault wall. Does this have to go on the classified set?

Answer: No

Question: How about a penetration into a Shielded Environment?

Answer: In all instances, penetrations into Shielded Environments shall be delineated on a classified set.

Topic 14: Post Communications Center (and other Core Suites)

Question: In the past, it was permissible to show all walls/partitions for a PCC on unclassified drawings (provided the room functions were not identified). Is that still permitted?

Answer: No. Partitions/walls located in the Restricted Area of the CAA may still be shown as well as the perimeter (and vault walls) and non-functional areas of the Core Area. (Non-functional areas include restrooms, common use corridors, egress stairs, etc.) However, partitions delineating the internal configuration of the PCC or other Core suites may not be shown. There is one exception, and that is for vault walls.

Topic 15: **Previously Unclassified Information that is now classified.**

Question: I am working on a renovation at an Embassy and will be using old drawings (from archives) to show existing conditions. During my review of these drawings I see that the information portrayed was unclassified when the drawings were completed but that same information (depiction) is now classified. What do I do with the drawings for the renovation project as well as the drawings from the archives?

Answer: Since you will be creating new work based in part on archived information, you must comply with this guide. If the drawing is now considered classified, it must be appropriately marked in the ***new*** set of plans. Because of the difficulty in retrieving and remarking all copies of the old drawings, those archived plans retain the original classification.

Topic 16: Procuring Equipment for Specific Projects

Question: The Frequently Asked Question on Limit Drawings discusses the requirement for the use of proper project names on drawings, specs, and other documents. Does this require a procedural change that will affect the procurement of enclosures and similar products?

Answer: Yes, but a bit of explanation is needed. The requirement as introduced in the 2003 version of the SCG was the result of numerous incidents where project names were omitted on shop drawings and specs (to provide anonymity), but ended up in project specific files or forwarded to specific Posts anyway. Such actions invalidate anonymity. To mitigate that risk, Appendix C, paragraphs 3a and 4a of the 2003 guide required proper project naming. To meet the requirements of the 2003 and the 20**XX** (i.e. this guide), two recommended protocols have been developed and are articulated in the attached document.

Topic 17: SBU Information

Question: In reference to paragraph c on page 34-42, I am not clear on what this paragraph is saying. Does 'others' include non-U.S. citizen employees and non-U.S. citizen prospective suppliers and subcontractor personnel? Is this information only for U.S. Citizens? Who are the FSN's?"

Answer: The person determining who may have access to SBU information shall be a U.S. citizen. That individual can determine that non-U.S. citizens (a Foreign Service National/FSN) have a need to know and may be granted access to that SBU material. See Appendix B for definition of FSNs.

Topic 18: SBU Marking

Question: SBU Marking Instructions: Is this the same format as marking classified, i.e. top and bottom, marking the inner wrapping, is there double wrapping, or is it only an overall marking to show handling requirements?

Answer: Specifics of the marking requirements for SBU differ from what is required for classified material. SBU marking is not required to be top and bottom, nor is double wrapping required. Marking instructions for SBU are noted in Appendix C, paragraph 3 of the current guide.

Topic 19: SCIF

Question: What is a SCIF and is the term classified?

Answer: SCIF stands for Sensitive Compartmented Information Facility. The term is classified if the specific location is identified or discussed by room number or office designation.

Topic 20: Shielded Enclosures – Depictions

Question: In the past, it was permitted to show outlines of boxes, shaded or otherwise, if they were not identified. Is that still permitted?

Answer: No. With the determination that the areas containing these elements should be masked on unclassified drawings; no indications, identified or not, should be shown on unclassified drawings.

Topic 21: Signage

Question: Is signage permitted in the CAA? Is it classified?

Answer: Signage is permitted throughout the CAA. A good protocol is to use the space program that is usually issued with the unclassified portion of the statement of work. Signage should not be classified.

Topic 22: SMSe

Question: What is SMSe and is it classified information?

Answer: Security Management System enterprise (SMSe) is an unclassified security enhancement designed to provide more efficient monitoring of selected security systems at overseas facilities.

Topic 23: Specifications

Question: Generally speaking, are specifications unclassified or SBU? Also, are there any exceptions that change their level of categorization or classification?

Answer: Specifications are generally Unclassified. However, there are circumstances that can make them SBU or Classified. Examples: (1) When specifications include schedules (e.g. hardware, door, window, finish, etc.) that reveal the absence or presence of an SE, CSE, RFSE, MTCR, or SCIF or the location (i.e. room) and type of a treated environment they can become classified, that includes instances where PCC mission critical or support equipment are specified. (2) When electrical components unique to treated environments are specified or when details, assemblies, equipment, or technical protection unique to treated environments are noted. (3) When details of mechanical and electrical systems (including penetrations) are provided. (4) For emergency systems exclusively dedicated to the PCC, the specifications can be classified if they include capacity or rating information or if they articulate prioritization strategies (i.e. load shedding). (5) For technical security systems: U.S. government-directed modifications to commercial products, especially when the protect portions of the CAA. Also, for power supplies that protect sensitive areas. However, there are numerous and relatively specific rules. Most systems located in functional areas of the core and nearly all C-LAN components. Again, the requirements are specific.

Topic 24: Standard Details

Question: I have a standard partition detail that is used in the General Work Area (GWA) as well as in the PCC. Do I have to draw it twice (once on the unclassified drawings and once on the classified drawings)?

Answer: No. Using the Department's drawings standards, you may locate this detail on the unclassified set and reference to both the GWA drawings and the PCC drawings. Since the internal configuration of the PCC is only located in the classified set, there is no way for someone without a clearance to ascertain the location of the partition. The only information that is revealed is that the detail is used somewhere in a Core suite.

Question: How about if the detail is only used in the PCC?

Answer: Then the detail should only be delineated on the classified set.

Topic 25: STC Wall Ratings

Question: With regard to STC wall rating and treatments, can you provide examples of what constitutes unclassified versus classified information?

Answer: Yes. Assume that you are holding a document affiliated with a Specific Site (by name, contract number, etc.) and containing the following statements. The prefix (as exhibited by the 'U', 'C' or 'S') to each of the following statements indicates their classification level and the reason is stated in the column on the right.

a. (C) The transition between Non-CAA and CAA walls and penetrations meets STC XX.	Provides a measurable performance characteristic of a security countermeasure.
b. (U) Wall Z is built to STC XX.	Does not describe purpose of STC rating.
c. (C) Wall Z is built to STC XX to provide acoustic isolation.	It describes work for a specific security purpose and/or countermeasure.
d. (U) Suite A must be constructed using wall section Y (standard detail).	Does not quantify a countermeasure.
e. (C) Suite A in its entirety must be constructed to STC XX.	Provides a performance characteristic of a security countermeasure or treated area.

Topic 26: Shielded Environment - Definition

Question: The term "shielded environment" was a new concept in the 2003 edition of the classification guide. Is this the same as "shielded enclosures"?

Answer: No. The term is intended to encompass all spaces that are specifically designed and tested to ensure a specific acoustic or emanation radiation standard is met.

Question: I have read in the criteria for a particular project that the perimeter walls/partitions of the CAA shall include a sheet of foil-backed gypsum wall board. Is this considered a SE too?

Answer: No. Foil-backed gypsum board for the perimeter walls/partitions of the CAA does not imply a SE. While this is a preventative measure, it does not cover all the surfaces of the room or suite and there is no performance standard for it.

Topic 27: Shielded Environments

Question: With regard to Shielded Environments, can you provide examples of what constitutes unclassified versus classified information?

Answer: Yes. Assume that you are holding a document affiliated with a Specific Site (by name, contract number, etc.) and containing the following statements. The prefix (as exhibited by the 'U', 'C' or 'S') to each of the following statements indicates their classification level and the reason is stated in the column on the right.

a. (U) This post has a SE or TE.	Does not mention type of shielding or treatment.
b. (C) Room 308 has a SE or TE.	Provides the location of the SE or TE.
c. (C) There is a Built-in Conference Room (BCR) in Room 308.	Implies type of treatment (acoustic).
d. (S) There is a BCR built to STC 45 in Room 308.	Provides treatment performance characteristics.
e. (C) This post has a CSE.	Mentions presence or absence of CSE or RFSE.
f. (S) The CSE is located in Room 410.	Mentions type and location.
g. (S) The CSE in Room 410 is built to NSA standard XYZ.	Mentions type, location, and characteristics.
h. (U) There is a secure phone booth at post.	Does not mention type of treatment.
i. (C) That phone booth is located in room 512.	Mentions location.
j. (C) That phone booth is designed for acoustic protection.	Mentions type of treatment.
k. (C) That phone booth is designed for radio frequency protection.	Mentions type of treatment.

Topic 28: Vulnerabilities

Question: The determination that there is a vulnerability is confusing. Can you provide an example?

Answer: The prefix to each statement indicates the classification level of that statement. The explanation is in the column on the right. Again, assume you are talking about a specific site.

Statement	Explanation
1. (U) The safe haven is not designed to withstand a 24 hour forced-entry or ballistic attack.	24 hours exceeds Department standard.
2. (U) The door to the Compound Access Control	Vulnerability is visible to the general public.

(CAC) facility does not shut properly.

3.	(C) The Pedestrian Access Control (PAC) hardline is not constructed to meet 15 minute FE/BR (the welds are not continuous on the outmost layer of steel).	Condition is deficient when compared to Department standards and is not readily visible to the general public.
4.	(U) Upgrade hardline to 15 FE/BR standards.	Vulnerability is not identified.
5.	(C) Add second layer of 6 mm steel to bring hardline up to 15 minute FE/BR standards.	Vulnerability is identified.