UNITED STATES DEPARTMENT OF STATE
BUREAU OF DIPLOMATIC SECURITY

SECURITY CLASSIFICATION GUIDE
FOR
DESIGN AND CONSTRUCTION OF OVERSEAS FACILITIES

MAY 2003

RESPONSIBLE OFFICIAL:

W. RAY WILLIAMS
DEPUTY ASSISTANT SECRETARY AND
ASSISTANT DIRECTOR FOR COUNTERMEASURES

TABLE OF CONTENTS

NOTE: This document supercedes the Classification Guide for Design and Construction Projects Overseas dated June 13, 1989. 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.

I. PURPOSE

This guide establishes uniform procedures for categorization of sensitive and classified information relating to the architecture, engineering, interiors, construction, and rehabilitation of Department of State (DoS) overseas facilities and other facilities that fall under Chief of Mission authority. It is to be used to determine the sensitivity of material and the protection of that material. It shall be used for all design and construction projects as well as day-to-day operations within existing facilities. This guide shall be used by all United States Government (USG) 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. Avert 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 spaces and location of weapons safe(s)/vaults.
- 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. **Treated Environments** (Acoustic and Electro-magnetic radiation):
   - Whenever Treated Environments (TEs) 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 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 USG-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 Controlled Access Areas (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 treated 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,
Washington, D.C. 20520
202-663-0538

3. Executive Order (E.O.) 12829, Subject: National Industrial Security Program, dated January 6, 1995 [*establishes the protection of information classified pursuant to E.O 12356 dated April 2, 1982, "National Security Information," or its successor or predecessor orders, and the Atomic Energy Act of 1954, as amended*].

4. E.O. 12958, Subject: Classified National Security Information, dated April 17, 1995 [*establishes a uniform system for classifying, safeguarding and declassifying national security information*].

5. E.O. 12958, as amended, Subject: Executive Order: Further Amendment to Executive Order 12958, as amended, Classified National Security Information, dated March 25, 2003 [*prescribes a uniform system of classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism]*.

6. 32 Code of Federal Regulations (CFR) 2001, Subject: Classified National Security Information; Final Rule, dated October 13, 1995 [*provides implementation guidance concerning the requirements set forth in E.O. 12958 which is applicable to U.S. Government agencies*].

7. 32 Code of Federal Regulations (CFR) 2004, Subject: Protection of Classified Information. [*provides implementation guidance on the safeguarding of classified national security information]*.

8. 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*].

9. Department of Defense (DoD) 5220.22-M, Subject: National Industrial Security Program Operating Manual (NISPOM), dated January 1995 [*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*].

10. DoS 1 FAM (Foreign Affairs Manual) 263, Subject: DAS for Countermeasures and Information Security (DS/CIS): [*discusses DAS/CIS functions, responsibilities, and authority, for the management, formulation, and representation on matters regarding security policy, program plans for countermeasures, and information security programs for the Department*].

11. 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*].

12. 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*].

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

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.

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

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 the Department of State 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
Washington, D.C. 20520
202-663-0538

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 and designs and construct or renovate the subject facilities. These may include, but not be limited to:

- As-Built documents
- Bids
- Bills of Material (BOMs)
- Budget documents
- Calculations
- Construction Security Plans (CSPs)
- Contracts
- Cost Estimates (e.g. CWE)
- Design Guidelines (e.g. AEDG, SED)
- Designs
- DoS Standards
- Egress Plans
- Facsimiles
- Generic Designs
- Inspection Reports
- Maintenance Plans, Manuals and Studies
- Operating Manuals
- Planning papers & reports (e.g. LROBP)
- Plans
- Photography
- Programming documents
- Proposals
- Repair Manuals
- Requests for Proposals
- Review Comments (e.g. ProjNET)
- Shop Drawings
- Signage
- Specifications
- Standardized designs (e.g. SED)
- Statements of work (SOWs)
- Studies
- Submittals
- Submittal Registers
- Survey Reports
- Tests Procedures and Test Results

B. Explanation of Format

This table is an example of the format used on the following 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)*	Class'n/ Sensitivity Level*, Reason**	Declass'n Exempt'n ***	Remarks
Non Site-Specific			
• Generic Criteria *Definition: Systemic Standards and requirements which are applicable to a group of projects, programs or sites.*			
• Design Guidelines: *Definition: Unless stipulated by contract as a binding requirement, a guideline is non-binding direction on how requirements could be met. This guidance is usually articulated, for example, in documents like the Architectural and Engineering Design Guidelines for U.S. Diplomatic Mission Buildings (AEDG). Note: Design Guidelines differ from this Classification Guide in that the requirements of this Guide are binding.*			
• Research Tests and Results: *Definition: Information gathered during R&D 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
TS	Top Secret

**** Classification:**

E.O. 12958, as amended, 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. DoS has determined that one or more of these reasons for classification apply to the subjects listed in Tables IV-1 through IV -8 of this guide.

"Sec. 1.4. Classification Categories. 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 special activities), 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, which includes defense against transnational terrorism;

(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, which includes defense against transnational terrorism**;** or

(h) weapons of mass destruction."

***** Declassification:**

E.O. 12958, as amended, provides specific guidance on procedures related to Classification Management. Section 3.3(b) of that order permits a classification authority to exempt material for more than 25 years from declassification under the specific criteria cited below. DoS has determined that one or more of these exemptions apply to the subjects listed in Tables IV-1 through IV-8 of this guide. The Declassification Exemption column in the respective tables contains a cross-reference to the applicable criterion cited here:

"**(b)** An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which could be expected to:

(1) reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

(2) reveal information that would assist in the development 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 actual U.S. military war plans that remain in effect;

(6) reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) reveal information that would clearly and demonstrably 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 the national security, are authorized;

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

(9) violate a statute, treaty, or international agreement."

C. Classification Tables

Table IV-1

Subject: **FUNCTIONAL AREAS** *(i.e. room uses and occupants)*	Class'n/ Sensitivity Level	Declass'n Exempt'n	Remarks
Non Site-Specific			
1. Generic Criteria	U		
2. Design Guidelines	U		
Site-Specific			See Appendix for definition of 'Site-Specific'
Design Requirements			
3. Criteria	U		See 'PCC' Table for additional information.
4. Design Guidelines (generic and standardized graphics)	U/SBU/ NOFORN /C	3.3X (3 & 8)	SBU/NOFORN when the graphic depictions are of generic or standard designs for PCCs or functional Core suites that require site adaptation. CONFIDENTIAL when standard designs for PCCs or functional Core suites are prepared for a specific set of projects or will not be modified for site adaptation.
5. Proposed or existing room and space assignments (Note: location of safe havens/areas is Unclassified)	U/SBU/C	3.3X (3 & 8)	SENSITIVE BUT UNCLASSIFIED when there is sufficient information available to ascertain which rooms contain weapons safes. CONFIDENTIAL when Existing or proposed internal layouts of PCC or a Core Suite are delineated. See 'PCC' and 'Treated Environments' Tables for additional guidance.
Design			
6. Office buildings, office suites, CMRs, DCMRs and MSGQs.	U/SBU		SBU when layouts are depicted. (see also PCC and Core Suite discussions below)
7. Weapons safe location (except guard booths)	U/SBU		SENSITIVE BUT UNCLASSIFIED when there is sufficient information available to ascertain the location of a weapons safe.
8. PCC Location	U		See Table IV-2, Post Communications Center.
9. PCC Layout	C	3.3X(3)	CONFIDENTIAL when the internal configuration of the PCC is delineated. See Table IV-2, Post Communications Center.
10.. Core Suite Location	U		Core Suite defines those other functional areas located within the Core area of the Controlled Access Area (CAA).
11.. Core Suite Layout	C	3.3X (1, 3 , 8)	CONFIDENTIAL when the internal configuration of the Suite is delineated.

Operations			
12. Signage that uses the same terminology as those in an unclassified space program.	U		No space programs or signage using the terms: SIC, weapons safe, safe haven, or safe area, are permitted. Also, no signage using classified terms is permitted.
13. Identification of office spaces.	U/SBU/C	3.3X(8)	UNCLASSIFIED when spaces are identified using the terms office, reception area, corridor, restroom, mechanical spaces, support space, etc. SENSITIVE BUT UNCLASSIFIED when drawn from criteria such as an unclassified spaces requirements program or location of weapons safe. CONFIDENTIAL when an office or space is identified as a Treated Environment or containing specific information about the type of treated environment.

NOTES:

Table IV-2

Subject: **POST COMMUNICATIONS CENTER** *(and other areas as designated in the statement of work)*	Class'n/ Sensitivity Level	Declass'n Exempt'n	Remarks
Non Site-Specific			
1. Generic Criteria (includes layout, assemblies, building support systems)	SBU/ NOFORN		
2. Design Guidelines	U/S	3.3X (3&8)	SECRET when the specifications, models, etc. of prime mission equipment (i.e. processors, transmission devices), power line filters and Motor Generator (MG) sets installed in PCCs are defined.
3. Command and Control Procedures	SBU		e.g. override or emergency procedures.
4. Tests Procedures and Results	U/S	3.3X (3&8)	SECRET when specific tests procedures for PCC-unique assemblies are defined.
Site-Specific			See Appendix for definition of "Site-Specific"
Design Requirements			
5. Criteria	U/C	3.3X (8)	CONFIDENTIAL when the absence or presence of a CSE, RFSE or other treated environment is noted.
5.1. Electrical Components (e.g. Power panels, Isolation Transformers, Power Filters, Wave Guides, motor-generators)	U/C/S	3.3X (3&8)	CONFIDENTIAL when wave guides or Motor Generator sets are prescribed. SECRET where physical location and/or Specifications are prescribed. SECRET where their connectivity is prescribed.
6. Design Guidelines	U/SBU/C/ S		SBU/NOFORN when the graphic depictions are of generic or standard designs for PCCs that require site adaptation. CONFIDENTIAL when standard designs for PCCs are prepared for a specific set of projects or will not be modified for site adaptation. SECRET when the specifications, models, etc. of prime mission equipment (i.e. processors, transmission devices), power line filters and Motor Generator (MG) sets installed in PCCs are defined.
7. Proposed or Existing PCC	U/C/S	3.3X (3&8)	CONFIDENTIAL when the internal configuration of the PCC is delineated (except vault walls).

			SECRET when vulnerabilities that would render the electrical or AIS systems inoperable are disclosed. SECRET when PCC-unique details, assemblies, Prime Mission Equipment and other equipment (to include attributes of Treated Environments or mission critical equipment) are noted.
7.1 Technical Security Protection	U/S	3.3X(8)	See Table IV – 7 Technical Security.
7.2 Treated Environment Protection	U/S	3.3X(8)	See Table IV – 3 Treated Environments.
Design			
8. The design and details of PCC functions and layouts.	U/C/S	3.3X (3&8)	CONFIDENTIAL when the absence or presence of a CSE or RFSE is disclosed. Also, CONFIDENTIAL when layout of PCC is delineated (except vault walls). SECRET when details of penetrations into Treated Environments are described.
8.1 Vaulted Construction	U		
8.2 Interior Design and Furnishings	U/C	3.3X (8)	CONFIDENTIAL when items are identified as destined for the PCC.
8.3 Emergency Exits	U		
8.4 Facility Support Systems: Mechanical and Electrical (including calculations, specifications, designs, etc.)	U/C	3.3X (3&8)	CONFIDENTIAL for systems supported by dedicated PCC support systems.
8.5 Mechanical and Electrical systems (including calculations, specifications, designs, etc.) exclusively dedicated to the PCC.	C	3.3X (3&8)	
8.6 Dedicated Emergency Power systems.			See Table IV-4 'Emergency Power Systems'
8.7 Treated Environments.			See Table IV-3 'Treated Environments'
8.8 Technical Security.			See Table IV-7 'Technical Security'
8.9 Telecommunications Systems.			See Table IV-8 'Telecommunications'
8.10 Roof Penetrations and Facilities (e.g. Sheds).	U/C/S	3.3X (3&8)	UNCLASSIFIED for roof drains, scuppers, elevator and HVAC control rooms not associated with the PCC. CONFIDENTIAL when other specified use is identified. SECRET if PCC unique details are identified.

Operations			
9. Operations, Maintenance and Repair Manuals.	U/SBU/ NOFORN	3.3X (3&8)	SBU/NOFORN for systems unique to the Core.
10.Tests and Inspection Procedures and Results for systems within the PCC.	C/S	3.3X (3&8)	CONFIDENTIAL when specific systems are described or vulnerabilities documented. SECRET when those items include quantified information.
11. Command and Control Procedures	C	3.3X(3)	CONFIDENTIAL for installed PCC unique equipment

NOTES:

Table IV-3

Subject: **TREATED ENVIRONMENTS (TE)** *(Acoustic and Electromagnetic Radiation, including parent rooms)*	Class'n/ Sensitivity Level	Declass'n Exempt'n	Remarks
Non Site-Specific			
1. Generic Criteria (includes layout, assemblies, building support systems)	U		
2. Design Guidelines	U		
3. Tests Procedures and Results	U/S	3.3X (3&8)	UNCLASSIFIED for commercially available procedures for Treated Environments. **(**e.g. ASTM standards) SECRET for USG designed test procedures and results.
Site-Specific			See Appendix for definition of "Site-Specific"
Design Requirements			
4. Criteria	U/C	3.3X (3&8)	CONFIDENTIAL when the absence or presence of a CSE or RFSE is noted.
4.1 Electrical Components (e.g. Isolation Transformers, Power Filters, Wave Guides, Motor-Generators)	SBU/ NOFORN/ C/S	3.3X(3)	SBU/NOFORN when it is noted that these components will be used on a project but not specific to a Treated Environment. CONFIDENTIAL when wave guides or Motor Generator sets are prescribed. SECRET when physical location and/or specifications are prescribed. SECRET when their connectivity is prescribed.
5. Design Guidelines	U		UNCLASSIFIED for graphic depictions of generic or standard designs which require site adaptation. When little or no site adaptation is anticipated, see 6, "Proposed or Existing TEs".
6. Proposed or Existing TEs **Note: See Table IV-1, 13 above.**	C/S	3.3X (3&8)	CONFIDENTIAL when the location of the Treated Environment is identified. CONFIDENTIAL when the internal configuration or the type of Treated Environment is defined or when the presence or absence of a CSE or RFSE is noted. SECRET when vulnerabilities that would render the Treated Environment inoperable or ineffective are noted. SECRET when details, assemblies, equipment or technical protection of the TE is noted.

Design			
7. The design and details of Treated Environment functions and layouts.	U/C/S	3.3X (3&8)	CONFIDENTIAL when the presence of a CSE or RFSE is disclosed. Also, SECRET when layout of Treated Environment is delineated. SECRET when details of penetrations into Treated Environments are described or when entire Treated Environment design is provided.
7.1 Interior Design and Furnishings	U/C	3.3X(8)	CONFIDENTIAL when items are identified as destined for a TE.
7.2 Facility Support Systems Mechanical and Electrical (including calculations, specifications, designs, etc.)	U/C	3.3X (3&8)	CONFIDENTIAL for details (including loads and capacities of systems within the Treated Environment and Parent Room, when applicable.
7.3 TE-specific Systems	C	3.3X (3&8)	
7.4 Dedicated Emergency Power systems			See Table IV-4 ' Emergency Power Systems'
7.5 Technical Security			See Table IV-7 'Technical Security'
7.6 Telecommunications Systems			See Table IV-8 ' Telecommunications'
Operations			
8. Operations, Maintenance and Repair Manuals	U/SBU/ NOFORN		SBU/NOFORN for commercially published information and/or procedures.
9. Tests and Inspection Procedures and Results for Treated Environment systems.	U/SBU/ NOFORN/ S	3.3X (3&8)	SBU/NOFORN when commercially published test and/or inspection procedures are used. SECRET when test results and/or specific systems vulnerabilities are described. SECRET for USG designed tests and results.

NOTES:

Table IV-4

Subject: **EMERGENCY POWER SYSTEMS** ***(i.e. un-interruptible power supplies and generators)***	Class'n/ Sensitivity Level	Declass'n Exempt'n	Remarks
Non Site-Specific			
1. Generic Criteria	U		
2. Design Guidelines	U		
3. Research Tests and Results	U		
Site-Specific			
Design Requirements			
4. Criteria	U/C	3.3X(8)	CONFIDENTIAL for portion of emergency system exclusively dedicated to PCC
5. Design Guidelines	U/C	3.3X(8)	CONFIDENTIAL for portion of emergency system exclusively dedicated to PCC
6. Proposed or Existing emergency power systems, including discussion of vulnerabilities.	C	3.3X (3&8)	CONFIDENTIAL for portion of emergency system exclusively dedicated to PCC.
Design			
7. Location and/or capacity (i.e. rating) of units. Location of remote controls. Load shedding or similar prioritization strategy details.	U/C	3.3X (3&8)	CONFIDENTIAL for extent of emergency system exclusively dedicated to PCC.
8. Power distribution from UPS or generator to switchgear/power panel.	U/C	3.3X (3&8)	CONFIDENTIAL for extent of emergency system exclusively dedicated to PCC.
Operations			
9. Operations and Maintenance Manuals and parts lists.	U/C	3.3X (3&8)	CONFIDENTIAL for extent of emergency system exclusively dedicated to PCC.
10. Results of acceptance tests and maintenance inspections.	U/C	3.3X (3&8)	CONFIDENTIAL for extent of emergency system exclusively dedicated to PCC.

NOTES:

Table IV-5

Subject: **BLAST RESISTANCE**	Class'n/ Sensitivity Level	Declass'n Exempt'n	Remarks
Non Site-Specific			
1. Generic Criteria	U/SBU/ NOFORN		SBU/NOFORN when a maximum credible event is quantified.
2. Design Guidelines	U		
3. Research Tests and Results	U		
Site-Specific			
Design Requirements			
4. Criteria	U/SBU/ NOFORN		SBU/NOFORN when charge weights are quantified.
5. Design Guidelines	U		
6. Proposed or Existing blast resistant features (to include vulnerability analyses and feasibility studies).	U/SBU/ NOFORN /C	3.3X(8)	SBU/NOFORN when charge weights are quantified. CONFIDENTIAL when vulnerabilities are quantified.
Design			
7. Documentation indicating materials and assemblies of blast resistant features.	U/SBU/ NOFORN /C	3.3X(8)	SBU/NOFORN when charge weights are quantified (e.g. calculations). CONFIDENTIAL when vulnerabilities are quantified.
Operations	N/A		

NOTES:

Table IV-6

Subject: **PHYSICAL SECURITY** *(i.e.* an assembly or assemblies (using building materials and/or site features) that are designed to resist unauthorized or forced entry and attack (by hand tools, firearms or other similar weapons*)*.	Class'n/ Sensitivity Level	Declass'n Exempt'n	Remarks
Non Site-Specific			
1. Generic Criteria	U		
2. Design Guidelines	U		
3. Research Tests and Results	U		
Site-Specific			
Design Requirements			
4. Criteria	U		
5. Design Guidelines	U		
6. Proposed or Existing physical security features.	U/C	3.3X(8)	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.	U/C	3.3X(8)	CONFIDENTIAL when vulnerabilities not visible to the general public are described (e.g. when documented in survey or inspection reports).

NOTES:

Table IV-7

Subject: **TECHNICAL SECURITY** *(i.e. CCTV, Intrusion Detection Systems (IDS), electronic Door Controls. etc.)*	Class'n/ Sensitivity Level	Declass'n Exempt'n	Remarks
Non Site-Specific			
1. Generic Criteria	U/C	3.3X(8)	CONFIDENTIAL for USG- directed modifications to COTS IDS equipment protecting the CAA.
2. Design Guidelines	U		
3. Research Tests and Results	U		
Site-Specific			
Design Requirements			
4. Criteria	U/C	3.3X(8)	CONFIDENTIAL for USG-directed modifications to COTS IDS equipment protecting the CAA.
5. Design Guidelines	U		
6. Proposed or Existing technical security features.	U/C/S	3.3X(8)	CONFIDENTIAL for USG-directed modifications to COTS equipment. CONFIDENTIAL when specific components are not readily visible to the general public and are protecting the CAA. SECRET when system is protecting the Core.
Design			
7. General Power	U/C	3.3X(8)	CONFIDENTIAL for power supply and back-up systems exclusively serving Core areas.
8. Conduit runs including cabling where system or device types (e.g. detection, deterrent, monitoring) are not indicated.	U/C	3.3X8)	CONFIDENTIAL for PCC and Treated Environments, See Table IV-2 'PCC' and Table IV-3 'Treated Environments' for additional guidance.
9. Detection, Deterrent and Monitoring Devices	U/C/S	3.3X(8)	CONFIDENTIAL when location within CAA is not visible to visitors and model is identified, or for USG-directed modifications to COTS equipment. SECRET when model and location in Core are identified.
10. Wiring Diagrams indicating point to point routing to the terminations of individual conductors. (This is to differentiate from cabling plans.)	U/C/S	3.3X(8)	CONFIDENTIAL for CAA. CONFIDENTIAL for USG-directed modifications to COTS equipment. SECRET for Core.
11. Control Panels	U/C	3.3X(8)	CONFIDENTIAL for USG-directed modifications to COTS equipment.

Operations			
12. As-builts	SBU/C/S	3.3X(8)	SBU for chancery/consulate compounds, CONFIDENTIAL for CAAs. SECRET for Core areas.
13. Operations and Repair Manuals	U/SBU/ NOFORN/ C	3.3X(8)	UNCLASSIFIED when data is commercially available in the public domain. SBU/NOFORN for COTS IDS systems unique to the CAA. CONFIDENTIAL for USG-designed IDS equipment or USG-directed modifications to COTS IDS systems protecting the CAA.
14. Results of surveys and inspections	U/S	3.3X(8)	SECRET for description or vulnerabilities of systems located in the CAA. SECRET for description or vulnerabilities of IDS systems protecting the Core.

NOTES:

Table IV-8

Subject: **TELECOMMUNICATIONS** *(i.e. C-LAN, U-LAN, BAS, CATV, Fire Alarm, Intercom, Public Address Telephone, excludes technical security)*	Class'n/ Sensitivity Level	Declass'n Exempt'n	Remarks
Non Site-Specific			
1. Generic Criteria	U		
2. Design Guidelines	U		
3. Research Tests and Results	U		
Site-Specific			
Design Requirements			
4. Criteria	U		
5. Design Guidelines	U		
6. Proposed or Existing telecommunications features	U		
7. Design - Telephones			
7.1 Demarcation point between host country and post. Also between Post service point and main telephone frame room in chancery/consulate.	U		
7.2 Equipment and Distribution systems (e.g., conduit trays, outlet locations, configurations and distribution of station sets).	U/C	3.3X (3&8)	CONFIDENTIAL for any equipment or distribution details located in the functional areas of the Core.
7.3 Telephone connections to main security posts, safe havens/areas, PCC and any other classified communications or computer processing facilities (suite or room).	U/C	3.3X(8)	CONFIDENTIAL during design and construction when specific individual or organizational routing details in the CAA are revealed. UNCLASSIFIED upon occupancy, see also item 13 below.
7.4 Documentation of telephone cable routes and terminal assignments in CAA.	U/SBU/C	3.3X(8)	SENSITIVE BUT UNCLASSIFIED during design and construction when specific individual or organizational details are revealed. SENSITIVE BUT UNCLASSIFIED for terminal assignments upon occupancy, see also item 13 below.

			SENSITIVE BUT UNCLASSIFIED for Telephone cable routes in the restricted area of the CAA upon occupancy CONFIDENTIAL for cable routing in the functional areas of the CORE.
7.5 Details of specific design techniques used to protect any element of the telephone system from technical threat or attack	U/SBU/C/S	3.3X(8)	SBU for technical security systems. CONFIDENTIAL for technical security in the CAA (See Table IV-7- Technical Security). SECRET for telephone components.
7.6 Electrical and mechanical services, architectural furnishings, and details of other facility support systems in the telephone facilities	U		
7.7 Location of emergency telephones	U		
7.8 Acceptance test results and deficiency list	U/S	3.3X(8)	SECRET when tests involves specific countermeasures.
8. Design – C-LAN			
8.1 Plans, details and specifications delineating C-LAN equipment, user terminals and printers, and central processing units.	C	3.3X(8)	CONFIDENTIAL
8.2 Distribution conduits and terminal boxes	U/C	3.3X(8)	CONFIDENTIAL when the function of the design (ie. C-LAN) is revealed.
8.3 Identification of specific models of CLAN mission equipment (e.g., terminals, printers CPUs, or other processing hardware).	U/C	3.3X(8)	CONFIDENTIAL when exact models are identified. CONFIDENTIAL for USG-directed modifications to COTS equipment.
8.4 Acceptance test results and/or deficiency lists.	C/S	3.3X(8)	CONFIDENTIAL when listing models to be used, or when modifications made to any models are revealed. SECRET when deficiencies are identified.
9. Design -Other Classified Computer Systems	C	3.3X(8)	CONFIDENTIAL for project specific documentation.
NOTE: The contractor will be notified in writing of any other classified computer systems on which the contractor must work. This notification will be provided as part of the site-specific government-furnished information (GFI). To avoid an error of omission, the GFI will include a statement that there are no such areas in the project, if such is the case. These instructions will specifically modify the CLAN guidelines for the additional systems. However, as a general rule, any details of the CPU room operation, special electronic distribution closets, or segments in the PCC and any other similarly designated rooms are classified at least CONFIDENTIAL**.**			

10. Design - Unclassified Computer and Telecommunication Systems (U-LAN, Fire Alarm, Internet, CATV, BAS, Public Address and many tenant systems)	U/C	3.3X(8)	CONFIDENTIAL for those portions of wiring diagrams delineating BAS in Core Suites. See Table IV-3, Treated Environments
NOTE: All architectural, electrical, and mechanical design and/or construction documents, BOMs, acceptance tests, emergency restoration plans and details, etc., related to these systems are UNCLASSIFIED unless the U.S. Government provides specific instruction in writing to the contrary.			
Operations			
11. Telephone emergency service restoration plans, diagrams, repairs, parts lists, etc.	U/SBU/C	3.3X(8)	SENSITIVE BUT UNCLASSIFIED for CAA area plans. CONFIDENTIAL for core areas plans.
12. C- LAN emergency service restoration plans, diagrams, repairs, parts lists, etc.	U/S	3.3X(8)	SECRET when referring to results of tests or status of deficiencies throughout the network and/or inside the core.
13. Telephone Lists	U/SBU		UNCLASSIFIED for abbreviated phone listings showing key personnel and organizations or alphabetical listings SENSITIVE BUT UNCLASSIFIED for telephone directories that contain complete phone and organizational listings**.**

NOTES:

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
CIHS – Classified Information Handling System (obsolete term)
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
MSG – Marine Security Guard
MSGQ – Marine Security Guard Quarters
NISP – National Industrial Security Program
NISPOM – National Industrial Security Program Operating Manual
NOB – New Office Building
NOFORN - No Foreign Dissemination
OBO – Overseas Buildings Operations
OADR – Originating Agency Determination Required (obsolete term)
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 Communication Center
PDS – Protected Distribution System
PR - Parent Room
RF – Radio Frequency
RFSE - Radio Frequency Shielded Enclosure
RMS - Roof Maintenance Shed
S – Secret
SBU – Sensitive But Unclassified
SCC – Security Control Center/Console
SIC – Security Interface Cabinet
STE – Secure Terminal Equipment (new equipment, replaces STU)
STU –Secure Telephone Unit
TCR – Treated Conference Room (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
USIS - (obsolete term)

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 Post Communications Center 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 comprising 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).

Standard (ized) 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).

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

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

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. 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
Washington, D.C. 20522
(703) 312 3089

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

Office of Information Systems Programs
Bureau of Diplomatic Security
U.S. Department of State
Washington, D.C. 20522

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/sensitive 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 Contracting Officer, 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. 12958, pursuant to U.S. DOS Security Classification Guide for Design and Construction of Overseas Facilities, dated [*issue date*]"

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 de-classification. 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 Department of State.

2. CLASSIFIED MATERIAL

a. Handling: **Confidential (C) and Secret (S)** material shall be handled in accordance with the provisions in the NISPOM (for contractors) and Department of State 12 FAM policies and procedures (for USG employees). 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 the provisions in the NISPOM (for contractors)and 12 FAM 500 policies and procedures (for government employees). 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 DoS 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.

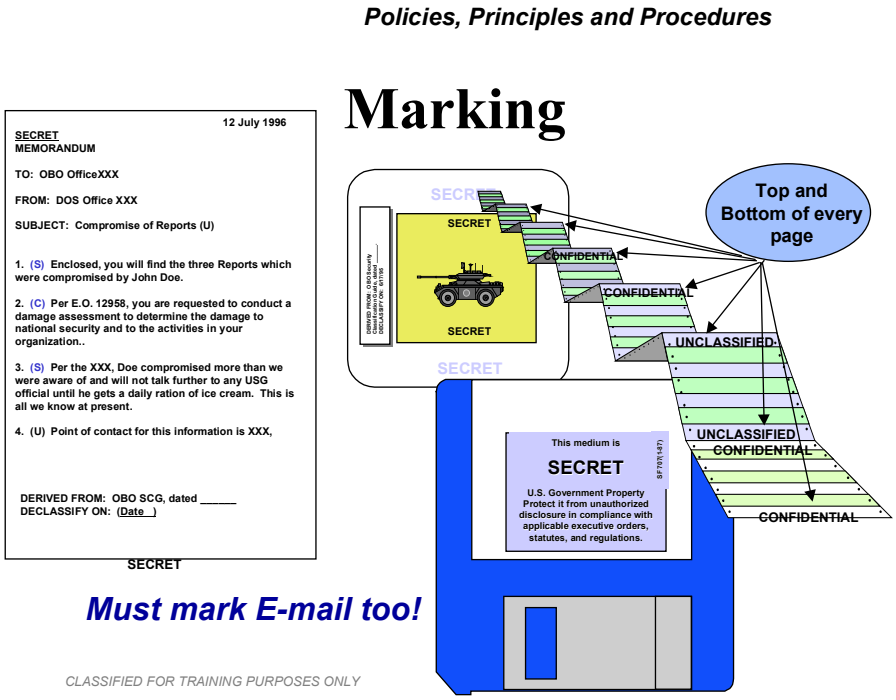

Figure 1.

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 Department of State 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 Program Branch (DS/ISP/INB) 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, USG employees sending classified information to contractors or others should contact DS/ISP/INB 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): Classified information may be sent via: the U.S. Postal Service as express or registered mail. No other regular or express mail services may be used. U.S. Postal Service Express Mail can only be used when it is the most effective means to accomplish a mission within security, time, cost, and accountability constraints. To ensure direct delivery to the addressee, the "Waiver of Signature Indemnity" block on the U.S. Mail label may not be executed under any circumstances. All classified express mail shipments shall be processed through mail distribution centers or delivered directly to a U.S. Postal Service facility or representative. The use of external (street side) express mail collection boxes is prohibited.

(4) Overseas: Classified information shall be sent by diplomatic pouch, diplomatic courier service or defense courier service.

h. Storage: Confidential or Secret information must be stored in a container approved by the facility security officer for the classification level of the material (or higher).

i. Public Release of Classified Information: Information relating to an overseas project is not authorized for release to any non-US 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 Contracting Officer, the documents may also be returned to the Department of State for retention or destruction.

3. SENSITIVE BUT UNCLASSIFIED (SBU) 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 12 FAM 540. Questions regarding this additional marking requirement should be directed to Chief, DS/IS/ISP.

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 Department of State 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"

b. Access: US 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 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 U.S. Postal Service 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 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 non-working 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 Department of State 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

b. Public Release of Unclassified Information: The fact that this guide reflects certain details of project information designated as unclassified does not authorize public release of these details. Furthermore, floor plans and utility routings of USG facilities (as well as plans or photos of emergency generators, tanks with emergency fuel supplies and escape routes) shall not be posted on public Internet web sites (see Department Notice 2001-03-014 for more details). Prior to any release of information:

(1) **Government personnel** shall coordinate with their Agency or Post Public Affairs Officer. (Information regarding the posting of unclassified information on an Internet Web Site is available at http://isc.state.gov/publications/guide.htm).

(2) **Contract personnel** shall coordinate with the Contracting Officer. Proposed public releases of any project information must be processed in accordance with existing contractual requirements as stipulated in item 12 of the Contract Security Classification Specification (DD Form 254).

d. Disposal: When drawings of buildings containing Controlled Access Areas (CAAs) are disposed, they shall be destroyed in the same manner as that required for classified drawings (see Paragraph C.2.j.). This applies to any drawing that shows any portion of a building that contains a CAA, even if the CAA is not shown.

APPENDIX D - Frequently Asked Questions

Topic 1: Classification of Information

Question: I've read the classification guide and have begun to develop site specific designs and 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: 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 3: 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 4: Classified Information versus Secure Procurement

Question: Is the furniture in the PCC classified?

Answer: No. This is a bit of a trick question, however. 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 Controlled Access Areas 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 USG representative (usually OBO, a tenant, or Post). The CSP is approved by the Bureau of Diplomatic Security (DS).

Topic 5: 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 6: Compilation of Information

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

Answer: This is a real example of how classified information was inadvertently disclosed. This edition of the Security Classification Guide closes this particular loophole. Nonetheless, this example is included here to convey the kind of conditions that can result in inadvertent disclosures, and thus, a security violation.

> 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 7: 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 8: 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, if the only purpose of the vault is to provide protection for the storage of classified information such as the pouch vault or the protection of backup power. Yes, If the vault wall is for the PCC.

Question: How about a penetration into a Treated Environment?

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

Topic 9: Treated Environment - Definition

Question: The term "treated environment" is a new concept for 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 Controlled Access Area shall include a sheet of foil- backed gypsum wall board. Is this considered a Treated Environment too?

Answer: No. Foil-backed gypsum board for the perimeter walls/partitions of the CAA does not imply a treated environment. 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.

Question: What about rooms where the walls are to include acoustic insulation to, say, STC 30?

Answer: If the requirement states that the entire room, including all penetrations, are to meet a certain STC rating, then the room qualifies as a Treated Environment and both the criteria and the design would be treated as classified. However, if it is just a statement that the walls shall be filled with STC 30 insulation, or will be constructed to a standard detail/section that meets STC 30, then the answer is no.

Topic 10: Treated Environments

Question: With regard to Treated 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 treated environment.	Does not mention type of Treatment.
b. (C) Room 308 has a Treated Environment.	Provides the location of the Treated Environment.
b. (C) There is a built-in conference room in Room 308.	Implies type of treatment (acoustic).
c. (S) There is a BCR built to STC 45 in Room 308.	Provides treatment performance characteristics.

d. (C) This post has a certified shielded enclosure.	Mentions presence or absence of CSE or RFSE.
e. (S) The CSE is located in Room 410.	Mentions type and location.
f. (S) The CSE in Room 410 is built to NSA Std. XYZ.	Mentions type, location and characteristics.
g. (U) There is a secure phone booth at Post.	Does not mention type of Treatment.
h. (C) That phone booth is located in room 512.	Mentions location.
i. (C) That phone booth is designed for acoustic protection.	Mentions type of Treatment.
j. (C) That phone booth is designed for radio frequency protection.	Mentions type of Treatment.

Topic 11: 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 12: 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 counter measure.
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 13: 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 14: Standard Details

Question: I have a standard partition detail that is used in the General Work Area 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 General Work Area 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 15: Vulnerabilities

Question: The determination of 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 safehaven is not designed to withstand 24 hours Forced-entry or Ballistic attack.	24 hours exceeds Department standard.
2. (U) The door to the Compound Access Control Facility does not shut properly.	Vulnerability is visible to the general public.

3. (C) The PAC hardline is not constructed to meet 15 minute FEBR (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 FEBR standards.	Vulnerability is not identified.
5. (C) Add second layer of 6 mm steel to bring hardline up to 15 minute FEBR stds.	Vulnerability is identified.

Topic 16: 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.