Physical Security Construction Requirements for SAP

Student Guide

November 2024

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Introduction

Course Welcome

[Narrator] Welcome to the Physical Security Construction Requirements for SAP course. This course covers the physical security construction requirements for Special Access Program Facilities, known as SAPFs.

After completing this course, you will be able to determine compliance or non-compliance of a newly constructed or renovated SAPF in accordance with Department of Defense (DOD) and Intelligence Community Directives (ICD). This course places you in a scenario as the SAPF Accrediting Official (SAO) that has been newly constructed. You will first be guided through an accredited facility to learn the construction specifications and then placed in your newly constructed SAPF to evaluate physical security requirements.

Course Objectives

[Narrator] You have arrived at a meeting in the conference room. There are three attendees seated at the conference room table.

[Kate] Good afternoon and thank you for joining this meeting. I know that you have just been assigned to this organization and assigned as the SAO. We're here to bring everyone up to date on the remodeling of the facility that will be our new SAPF and to plan for the accreditation inspection. The renovations are due to be completed in 90 days. Since you are new to our team, let us introduce ourselves.

As you know, I'm Kate, the organization's director. We are all here to support you and get you trained on your SAO responsibilities and the accreditation requirements for our new facility. I'll let the team introduce themselves.

[Ruben] Hi. My name is Ruben, I am the Program Security Officer, also referred to as the PSO. I will work with you on your SAO responsibilities. Welcome to the team.

[Jeff] Hi, I'm Jeff! I am an SAO at your sister facility. I will be your trainer for the SAPF accreditation requirements. I'm looking forward to working with you.

[Ruben] Jeff, since we are using your accredited SAPF to demonstrate DOD policy construction requirements, we want to work with your availability for scheduling training time with our new SAO.

[Jeff] We can begin training tomorrow morning, at 9 o'clock in my office. I will meet you in the lobby and escort you through visitor control.

[Ruben] I see that you have prepared an outline for the training. Please share that with our new SAO.

[Jeff] Sure, here are the learning objectives.

- Given an instruction, determine DOD guidance and Intelligence Community Standards (ICS) for the construction, accreditation, and inspection of SAPFs.
- Given an immersive environment, a scenario, and the blank Fixed Facility Checklist (FFC):
    - Inspect SAPF doors for compliance with DOD physical security criteria.
    - Analyze SAPF windows, ducts, ventilation, and access/inspection ports for compliance with DOD physical security criteria.
    - Verify that SAPF walls, ceilings, floors, and Special Access Program Compartmented Area (SAPCAs), are compliant with DOD physical security criteria.
    - Evaluate SAPF intrusion detection systems (IDS) for compliance with DOD physical security criteria.
    - Evaluate SAPF telecommunications for compliance with DOD physical security criteria.

Course References

[Narrator] You have returned to your office and you have an email.

Hello,

Here is the list of documents that cover the construction and accreditation of SAPFs:

- DODM 5105.21, Volume 1
- DODM 5105.21, Volume 2
- DODM 5105.21, Volume 3
- DODM 5205.07, Volume 3
- IC Tech Spec for CD/ICS 705
- ICD 705-1
- ICS 705-2

Access the Course Resources to briefly view these policy documents.

We will begin by reviewing the purpose of each of these documents tomorrow.

-Jeff

Lesson 2: SAPF Physical Security Construction Requirements for SAP

Introduction

Lesson Overview

[Narrator] You are meeting with your sister facility's SAO, Jeff, to begin your training.

[Jeff] Good morning. You are right on time. Our goal for this morning is to identify the Department of Defense (DOD) guidance and Intelligence Community Standards, also known as ICS, that covers the construction of Sensitive Compartmented Information Facilities (SCIFs), but we also use as our standards for the construction of SAPFs. In addition, we will review paperwork associated with the accreditation and inspection process and I will explain SAPF inspection and review requirements. Lastly, we will discuss the reciprocity for SAPFs. We will do all of this in my office and then head out to the rest of the facility to view specific components and their construction standards.

Let's start by defining a SAPF. A SAPF is an accredited area, room, group of rooms, building, or installation where SAP materials may be stored, used, discussed, manufactured, or electronically processed. SAPFs may be fixed facilities, mobile platforms, prefabricated structures, containers, modular applications, or other applications and technologies that may meet performance standards for use in SAPF construction.

Policies

Guidance for the Construction and Inspection of SAPFs

Policy guidance that we routinely use includes:

- DOD Manual 5200.01, Volume 3
- DOD Manual 5205.07, Volume 3
- Technical Specification for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec for Intelligence Community Directive/Intelligence Community Standards (ICD/ICS 705), also referred to as IC Tech Spec
- ICS 705-02
- Facility's standard operating procedures (SOPs)

Let’s review the purpose of each of these documents.

Policy Guidance	Purpose
DODM 5200.01, Volume 3 - DOD Information Security Program – Protection of Classified Information	• Provides guidance for safeguarding, storage, destruction, transmission, and transportation of classified information • Applicable to all military departments, DOD agencies and field agencies, and DOD components
DODM 5205.07, Volume 3 - DOD Special Access Program (SAP) Security Manual - Physical Security	• Implements policy established in DOD Directive 5205.07 • Assigns responsibilities • Provides general procedures for physical security at DOD SAPFs Applicable to: • All Military departments • DOD agencies and field agencies • DOD components and component contractors and consultants • Non-DOD U.S. government entities that require access to DOD SAPFs
IC Tech Spec for ICD/ICS 705	• Establishes the physical and technical security specifications and best practices for meeting construction and renovation standards of ICS 705-1 • Facilitates the protection of SAP and SCI against compromising emanations, inadvertent observation and disclosure by unauthorized persons, and the detection of unauthorized entry • Applicable to all Intelligence Community (IC) elements
ICS 705-02 - Standards of the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities	• Establishes criteria for accreditation of Sensitive Compartmented Information Facilities (SCIFs) to enable reciprocal use and information sharing • Applies to the IC and any other department or agency that may be designated a part of the IC
Standard Operating Procedures (SOPs)	• Address specific areas that may not be covered in the DOD or IC policy guidance • Identify specific areas of security concern • Address specific facility mission requirements

SAO and SSM SAPF Responsibilities

DODM 5205.07, Volume 3 also provides the SAPF construction responsibilities of the Special Access Program Facility Accrediting Official (SAO), and the Site Security Manager (SSM).

Role	Responsibilities
Special Access Program Facility Accrediting Official (SAO)	• Review and approve/disapprove the design concept, construction security plan (CSP), and final design for each construction project • Physically inspect facilities before accreditation • Provide construction advice and guidance as required • Inspect facilities at an interval as determined by the Cognizant Authority SAP Central Office (CA SAPCO) • Approve and document mitigations • Recommend waivers of physical security safeguards to the Director, CA SAPCO • Ensure mitigating strategies are implemented and documented in the CSP • Request construction surveillance technicians to supplement site access controls, implement screening and inspection procedures, and monitor construction and personnel
Site Security Manager (SSM)	• Advise the SAO of the potential for variation from the requirements of DODM 5205.07-V3 during construction • Additional duties outlined in DODM 5205.07-V3

Accreditation and Inspection

Types of Inspections

[Narrator] You ask Jeff the following question – "You mentioned that I must inspect the facility before it is accredited. Is that the only inspection that must be accomplished?"

[Jeff] Good question. Let's look at the inspections that must be accomplished. In accordance with DODM 5205.07, Volume 3, SAOs will review physical security pre-construction plans or facility expansion or modification plans to ensure compliance with applicable construction criteria and document any proposed mitigation in the plans. The approval or disapproval of a physical security pre-construction plan will be in writing and retained in the requester's files. The SAO will physically inspect any SAP area before accreditation.

Periodic inspection is another inspection that must be accomplished as outlined in the IC Tech Spec for ICD and ICS 705. Periodic physical security inspections will be conducted based on threat, physical modification, sensitivity of SAPs, and past security performance.

These physical security inspections will be conducted at least every 3 years for SAPFs.

The Fixed Facility Checklist

Let me show you one of the key documents used during inspections. The Fixed Facility Checklist, also known as the FFC, is used to inspect SAPFs for the initial accreditation and periodic inspections.

The FFC documents physical, technical, and procedural security information. For example, when examining doors, you will evaluate physical items listed on the checklist such as "Is an approved access control device installed?"

You will also examine technical security checklist items such as “Do SCIF perimeter doors and frame assemblies meet acoustic requirements unless declared a non-discussion area?” A procedural security item on the checklist includes checking items such as, “Does the SCIF SOP include procedures to ensure all doors are secured at the end of the day?”

Now let’s take a closer look at the FFC. It includes a variety of categories including general information, security-in-depth, SCIF security, doors, intrusion detection systems (IDS), telecommunication systems and equipment baseline, acoustical protection, classified destruction methods, and information systems/TEMPEST/technical security.

The completed FFC will include, but is not limited to floor plans, diagrams of electrical and communications wiring; security equipment layout, to include the location of intrusion detection equipment and security in depth (SID); fire alarm layout; and heating, ventilation, and air conditioning connections. All diagrams or drawings must be submitted on legible and reproducible media.

Access the Course Resources to view an example of a completed Fixed Facility Checklist.

Reciprocal Use

Co-utilization of SAPFs

Co-utilization of existing facilities promotes efficiency and achieves financial savings. Elements desiring to co-utilize a SAPF will accept the host’s current accreditation and any waivers. A co-utilization agreement (CUA) will be established between the host and tenant prior to occupancy. There is an FFC for each SAP Compartmented Area (SAPCA) where there is co-utilization of a SAPF. The SAPCA FFC shall be used to request approval. The host Cognizant Authority (CA) maintains oversight of the facility unless all parties agree to transfer CA responsibility. Co-utilization is considered joint-utilization when the tenant and the host share all of the resources in the facility to accomplish the task and/or mission.

Reciprocity

Reciprocity occurs when there is a requirement to share an accredited SCIF or portion with a compartment, program, or special activity that is sponsored by an IC element or organization other than the current SCIF CUA. Facilities housing Sensitive Compartmented Information (SCI) related SAPs must meet the physical security requirements of ICS 705-1. ICS 705-1 applies to facilities with SCI-related SAPs.

Any physical security measures above those described in ICS 705-02 that are required by SAP managers should be negotiated between the SAO and Accrediting Official (AO). ICS 705-02 is the Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities.

When a SCIF is under a CUA and personnel are not briefed into all the respective programs, the host and tenant activities must establish procedures to prevent unauthorized access to that specific compartment or program. This may include physical, visual, and acoustic security measures.

When IC Technical Specifications have been applied to construction or renovation and operation of SAPFs, those facilities satisfy the standard for reciprocal use across all IC elements for accreditation by IC elements as a SCIF.

Knowledge Checks

Knowledge Check – 1

Which of the following policy documents should you consult when you need to determine the physical security specifications and best practices for meeting SAPF construction and renovation standards?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ ICD 731

○ DODM 5205.07, Volume 2

○ DODM 5205.21, Volume 3

○ IC Tech Spec for ICD/ICS 705

Knowledge Check – 2

Which of the following is used to inspect SAPFs for initial accreditation and periodic inspections?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ Fixed Facility Checklist (FFC)

○ Standard Operating Procedures (SOPs)

○ Physical Security Pre-Construction Plans

○ SAPF Inspection Checklist

Knowledge Check – 3

Which of the following inspections should the SAO perform for a SAPF?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

□ Pre-contract inspection

□ Initial accreditation inspection

□ Post-contract inspection

□ Periodic inspection

Knowledge Check – 4

Which of the following statements are true about reciprocity?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- □ With reciprocity, procedures to prevent unauthorized personnel from accessing compartmented or program information primarily focus on acoustic security measures.
- □ Reciprocity promotes efficiency and helps achieve financial savings.
- □ With reciprocity, procedures must be in place to prevent unauthorized personnel from accessing compartmented or program information.
- □ Reciprocity occurs when there is a requirement to share an accredited SCIF or portion with a compartment, program, or special activity.

Conclusion

Lesson Summary

[Jeff] Well, we had a very productive morning. We have identified the DOD and ICS guidance that covers the construction of SAPFs, we have reviewed paperwork associated with the accreditation and inspection process, described the SAPF inspection and review requirements, and explained reciprocity for these facilities.

Let's take a short break and then come back and start looking at construction requirements for specific items within the facility.

Lesson 3: Doors

Introduction

Lesson Overview

[Jeff] Now we will talk about the main points of entry for a Special Access Program Facility (SAPF). As you may have guessed, the criteria for a SAPF door can be stringent. Keep in mind that this facility was built as a modified construction project. So, we have a mixture of different doors, locks, and hardware in our open storage facility.

Our goal is to ensure you're prepared as much as possible to ensure your facility is accredited without too many hiccups. Take a moment to review the lesson objectives:

- Examine primary and secondary doors
- Evaluate emergency doors
- Describe construction requirements for different door types
- Evaluate door acoustical protections, locking devices, and door hardware

But before we begin our tour and go through any of the doors, it's important to discuss the control of portable electronic devices (PEDs) within a SAPF.

Portable Electronic Devices

Control of Portable Electronic Devices (PEDs)

For guidance on bringing PEDs into a SAPF, refer to the Standard Operating Procedures (SOPs). Designated areas may be identified at the entry point to all SAP areas for the storage of PEDs. Where PED storage areas or containers are allowed by the Program Security Officer (PSO) to be within the SAPF, the PEDs will be turned off. Designated PED storage areas or containers will be confined to "non-discussion" areas.

PEDs without loadable data storage capabilities that are authorized within the SAPF include:

- Electronic calculators
- Spell checkers
- Language translators
- Receive-only pagers
- Audio and video playback devices
- Receive-only radios
- Devices that do not transfer, receive, store, or generate data including text, audio, and video

For additional information on PEDs, refer to the criteria listed in IC Tech Spec, Chapter 10, "Portable Electronic Devices with Recording Capabilities and Embedded Technologies". Now let's go into the facility and talk about the different door types.

Door Types

Door Types

There are three types of doors in the facility.

- The primary door is our SAPF perimeter door that is recognized as the main entrance.
- A secondary door is a SAPF perimeter door employed as both an entry and egress door that is not the primary door.
- An emergency egress-only door is a SAPF perimeter door that is employed as an emergency egress door with no entry capability.

Refer to the criteria listed in IC Tech Spec, Chapter 3, Section E when inspecting SAPF doors.

Steel Doors

When we inspect SAPF doors, we need to inspect every exterior, secondary, and emergency door, and its components to ensure they match the requirements of policy. These components include the door itself, the doorframe, locking devices, and hardware such as hinges, push bars, floor sweep, and automatic, non-hold door-closers. Let's start with steel doors.

Steel Door Requirements

Steel doors must have a thickness of 1 ¾- inches but have a few additional requirements. The face steel must be 18-gauge but reinforcement must be added to the hinges, preferably a lift hinge at 7-gauge, door closers at 12-gauge, and lock areas at 10-gauge.

Wood Doors

Now let's talk about the construction requirements for wood perimeter doors. Wood doors must be one and three quarters inches thick and have a solid or wood stave core. A stave core door uses a core manufactured of a lower grade wood glued together with veneers and edges of a finished door glued on the outside for dimensional stability.

Knowledge Check – 1

You are tasked to examine the primary and secondary doors. What will you need to evaluate?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- □ The doorframe
- □ The hardware on the door
- □ The locking devices on the door
- □ You only need to examine the door construction, not the door components.

Door Styles

Roll-up Doors

Now let’s look at a few different door styles. One of these styles is a roll-up door. In a SAPF, it can be a little more difficult to meet construction requirements for these.

Roll-up Door Requirements

Roll-up doors have the same 18-gauge requirement as steel doors, and these doors must be secured on either side with a dead bolt. Additional locking devices such as pad locks may be used on roll-up doors.

Normally, roll-up doors are only authorized for use in non-discussion areas because they cannot be treated for acoustics. However, since our facility was modified construction, we had to get a waiver for the roll-up and add sound masking devices to meet the acoustic requirements.

Double Doors

All the criteria for wood or steel doors apply to double doors.

Double Door Requirements

What is different with double doors is that each door requires its own independent high-security switch (HSS) if it is used as an entry into the SAPF, and one of the doors must be fixed with a deadbolt placed on the top and bottom of the door.

Also, one of the doors must have an astragal strip installed to prevent anyone from peeking through the crack between the doors. An astragal strip is a piece of hardware or molding that is attached to one of a pair of double doors to cover the gap between the two doors.

Lastly, door sweeps should be included. Keep in mind that door sweeps should be on all doors with the exception of roll up doors.

Door Acoustical Protection, Locking Devices, and Hardware

Sound Transmission Class (STC)

Preventing unwanted peeking is good, but we also need to prevent unwanted listening as well. Let's talk about some door acoustical protections. The ability of a SAPF to retain sound within its perimeter is rated using a value called the Sound Transmission Class (STC). To satisfy normal security standards of SAPF transmission, attenuation groups have been established in sound groups.

- Sound group 3 has an STC of 45 or better. Loud speech from within the SAPF can be faintly heard but not understood outside of the SAPF. Normal speech is unintelligible with the unaided human ear.
- Sound group 4 has an STC of 50 or better. Very loud sounds within the SAPF, such as loud singing, brass instruments, or a radio at full volume, can be heard with the human ear faintly or not at all outside of the SAPF.

SAPFs also need to meet the acoustic requirements as listed in IC Tech Spec, Chapter 9, "Acoustic Protection".

Sound Group Mitigations

There may be times when a facility's doors cannot meet Sound Group 3 or 4, and you will have to come up with a solution. We had that issue with the roll-up door in this facility. IC Tech Spec, Chapter 9, "Acoustic Protection" lists some ways to mitigate those issues, such as:

- Adding structural enhancements to the building
- Using noise generators
- Using sound masking devices
- Having non-discussion areas
- Incorporating a vestibule

We have covered the door types and acoustical protection, so now we can move on to the SAPF door locking devices.

Door Lock Program

A SAPF wouldn't be very effective at protecting our classified information if the doors could not be secured properly. A standard key and lockset just won't cut it. We can only use U.S. General Services Administration (GSA) approved locks that meet federal specification.

Fortunately, the Department of Defense (DOD) has established a lock program that lays out the lock specifications and lists the approved lock types. The program's Technical Support Hotline is staffed to help you with information on security hardware:

- Selection
- Requirements
- Specifications
- National stock numbers
- Purchasing
- Troubleshooting of equipment failures

Door Locking Devices

“What locking devices should a SAPF entry door have?” IC Tech Spec lists the door's locking criteria.

Door Locking Device Requirements

Primary entrance doors must be equipped with the following:

- A combination lock meeting the Federal Specification FF-L-2740,
- A GSA-approved pedestrian door deadbolt meeting Federal Specification FF-L-2890, and
- An approved access-control device.

It may also be equipped with a high-security keyway for use in the event of an access control system failure. You can refer to the DOD Approved Locks Job Aid if you are unsure which lock is required for the application you are inspecting. You can find this document in the Course Resources.

Access Control System (ACS)

The door locks are just the first line of defense when it comes to restriction entry to a SAPF. We also are required to incorporate an approved access control system (ACS) and guidelines.

Access Control System Requirements

SAPF access shall be controlled by SAP-indoctrinated personnel or by a SAPF Accrediting Official (SAO) approved ACS that verifies an individual’s identity before the individual is permitted unescorted access.

If an approved automated ACS is used, it needs to employ two of the three technologies including:

- An identification (ID) badge or card used in conjunction with the access control device that validates the identity of the person to whom the card is issued;
- A personal identification number (PIN) that is entered into the keypad by each individual; or

- A biometric personal identity verification using unique personal characteristics such as fingerprint, iris scan, or palm print.

If a SAPF has a low number of people that require access, such as 25 personnel or less, or as determined by the SAO, the SAO may then approve the use of a non-automated access control devices.

Examples of access control systems include identification (ID) badges used in conjunction with the access control device, a personal identification number (PIN), and a biometric personal identity verification system.

Refer to the criteria listed in IC Tech Spec, Chapter 8 Access Control Systems to learn more.

Perimeter Door Hardware

Now let's talk hardware. For the most part, the hardware that we use on our SAPF perimeter doors look a lot like the hardware on any door. However, the hinges must have the ability to secure the hinge pins from being removed when hinges are on the exterior of SAPF, for example, by using welding or set screws. Also, every perimeter door must have an automatic door-closer that does not have a hold open feature and is installed internal to the SAPF, if possible.

Emergency Door Hardware

Earlier we discussed the construction standards for steel and wood doors used on SAPFs. The construction standards for emergency doors used on SAPFs are similar to any other perimeter door and must meet the criteria for the type of door you have, either wood or steel. Also, the door and frame must meet all acoustic requirements if it is located in an open-discussion area. Lastly, the door must comply with all building, safety, and accessibility codes just like any other perimeter door.

Emergency Door Hardware Requirements

Now, let's talk about what is different about emergency doors. All emergency exit doors must be equipped with deadlocking panic hardware on the inside that meets Federal Specification FF-L-2890, Type III, specifically modified for emergency exit applications. Emergency exit doors will have no exterior hardware and will be alarmed at all times. Finally, the door must be equipped with a local, audible annunciation device so everyone knows when the door has been opened.

Knowledge Check – 2

While inspecting an emergency exit door on a SAPF, you see it has deadlocking panic hardware on the inside and a CDX-10 lock on the outside. Would this door meet the criteria for emergency doors in a SAPF, and why (or why not)?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ No. Emergency exit doors must not have exterior hardware.
○ Yes. This hardware meets Federal Specification FF-L-2890, Type III.
○ No. This hardware does not meet Federal Specification FF-L-2890, Type III.
○ Yes. The exterior hardware is for emergency responders to gain access.

Knowledge Check – 3

What must SAPFs equipped with double doors have installed to prevent individuals from looking between the doors into a classified room?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ 180-degree peep hole
○ Local audible annunciation device
○ 24/7 video surveillance
○ Astragal strip

Knowledge Check – 4

You are evaluating the acoustical protections of the doors in a SAPF. What specifications may be present to ensure that the doors will mitigate sound transmissions?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

□ There was astragal strip added to the door.
□ The SAPF door has an HSS.
□ The SAPF doors and frame assemblies meet acoustic requirements.
□ There were sound-source generators added to the SAPF.

Conclusion

Lesson Summary

It’s been a busy morning. So far, we discussed the criteria for primary, secondary, and emergency doors. In addition, we’ve described the construction requirements for different door types and the requirements for acoustical protections, locking devices, and door hardware.

Since doors are the easiest points to enter a facility, we must ensure the doors that protect classified materials operate smoothly for our cleared employees while preventing unauthorized people from gaining access.

Lesson 4: Windows and Penetrations

Introduction

Lesson Overview

[Jeff] Doors may be one of the easiest points to enter a facility, but they are not the only way to access a Special Access Program Facility (SAPF). Windows and ventilation systems can be used to gain unauthorized access to the classified information within. It is our job as Special Access Program Facility Accrediting Officials (SAOs) to mitigate that risk. We do that by verifying the construction techniques and materials used meet the requirements listed in the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, also referred to as the IC Tech Spec.

Keeping with our goal of ensuring you are as prepared as possible to get your facility accredited without too many hiccups, we will look at the criteria for windows and penetrations. Take a moment to review the lesson objectives.

- Evaluate window height and construction
- Inspect ducts and ventilation areas

Windows

Window Criteria

When we inspect SAPF windows, we need to refer to the criteria listed in the IC Tech Spec, Chapter 3, Section F. Let’s have a look at the criteria so you know what to look for. First, it doesn’t make sense to put windows in a facility that is meant to keep secrets secret. It makes even less sense to place those windows on the ground floor of your facility where anyone walking by could look in.

If we were constructing a new facility, we would make every effort to minimize or eliminate windows during the planning stage of construction. However, when dealing with a modified facility, eliminating all windows may not be an option. So, we must mitigate the risk these windows pose to our security efforts. If you are bailing water out of a boat and the bucket you are using is full of holes, your efforts probably wouldn’t be very effective.

The same can be said about a SAPF. The more windows that can be opened in a facility, the greater risk that classified information can be compromised. We must mitigate that risk by making sure the windows in our facility are non-opening. But just because our windows don’t open, it doesn’t mean they shouldn’t be protected. That’s why every window that is within 18 feet from the ground or an accessible platform must be protected by security alarms.

So, let’s say the bottom of this window is 27 feet from the ground. Due to its height from the ground, this window would not require a security alarm. However, if the window is within 18 feet from an adjacent roof or other accessible platform, it would require security alarm protection.

In addition, we need to protect windows from forced entry. As the requirement states, any window where the bottom of the window is within 18 feet of the ground or other platform that gives access must be protected against forced entry. So how is this done? Well, installing shatter resistant, ballistic proof, or bulletproof glass are some ways to meet this standard. However, these options may not be viable solutions for your SAPF. Installing bars externally over the window may be a more practical solution for your project. There are also commercial films that can be applied to windows that can protect the window from forced entry.

Windows Criteria – Visual and Acoustic Protection

Windows in a SAPF must provide visual and acoustic surveillance protection. Again, you can find the window criteria in the IC Tech Spec, Chapter 3, Section F.

We add visual protection to windows by making the window opaque or—with the SAO's approval—equipping the windows with blinds, drapes or other coverings. Also, windows must meet the acoustic protections level of the sound group rating of your facility. Keep in mind that large windows may require noise generator transducers to achieve the required acoustic protection levels.

If your facility must meet the TEMPEST requirements, you may have to include radio frequency (RF), protection to your windows when recommended by the Certified TEMPEST Technical Authority (CTTA). This can be accomplished by applying RF protection such as RF film or RF curtains.

Penetrations

Penetration Criteria

Now that we have covered the SAPF window criteria, let's have a look at some of the items that penetrate the perimeter of a SAPF. When we inspect SAPF vents and ducts, we need to refer to the perimeter penetrations criteria listed in the IC Tech Spec, Chapter 3, Section H.

Let's have a look at the criteria so you know what to look for. As with windows, penetrations of SAPF perimeter walls should be kept to a minimum. But there is no way to eliminate penetrating the perimeter completely. Items such as electrical and signal utilities should enter the facility at a single point and be constructed to meet acoustic and RF protection standards. We'll be discussing RF protections standards later on.

Heat, Ventilation, and Air Conditioning (HVAC) vents and ducts will also need to meet these criteria but have additional requirements. The HVAC vents and duct work must meet the acoustic protections level of the sound group rating of your facility. Sound baffles may be installed in the ducts to help meet this requirement.

The builder could also install "Z-Ducts" with acoustically lined, thru-wall sheet metal transfer ducts. "Z" ducts are shaped like the letter "Z" and contain two ninety-degree bends that ensure there is no direct sound path through the duct.

SAPF walls above the false ceiling or below a false floor must be finished and painted in a similar manner as the wall below the false ceiling. This is done so unauthorized intrusion or penetration of the perimeter is seen easily. The walls surrounding the ducts must be finished and sealed so gaps or openings are eliminated around the entire duct.

Vent Bars and Grilles - Exceptions

We must protect vents and duct openings that penetrate the perimeter walls of a SAPF and exceed 96 square inches with permanently affixed bars or grilles. But there are some exceptions. If one side or dimension of the vent is less than 6 inches, it doesn't need bars or grilles. The same can be said for vents that have permanently installed sound baffles or wave forms. If they are set no further than six inches apart, bars or grilles are not required.

Vent Bars and Grilles Criteria

Bars and grilles in the SAPF duct systems must be installed inside the perimeter of the facility. The duct may also have an access or inspection port so we can inspect the bars and grilles for proper installation and tampering.

If the inspection port cannot be installed within the facility's secure perimeter and the area outside is controlled to the secret level, an inspection port could be installed outside the perimeter and secured with an approved lock. This would require the approval of the SAO and annotated on the Fixed Facility Checklist.

Vent Bar Criteria

Bars, if installed, must use half-inch diameter steel that is welded on all sides. The bars must be placed six inches on center; a deviation of one-half inch in vertical and/or horizontal spacing is permissible.

The bars must be permanently affixed to the duct. This can be accomplished by welding the bars in a frame, screwing the frame to the duct walls, and welding the screws so they can't be removed. We prefer using bars over grilles because the grille openings are smaller and may restrict airflow.

Vent Grill Criteria

Grille material can be purchased commercially and must be one of the following.

- It can made of three quarter inch mesh, #9, or 10-gauge, case-hardened, expanded metal.
- It can also be made of expanded metal diamond mesh, 1-1/2" #10 and tamperproof. This has 1-3/8" by 3" openings, 0.093" thickness, with at least 80% open design.
- Or it can be made of welded wire fabric (WWF) 4x4 W2.9xW2.9 consisting of six gauge smooth steel wire welded vertically and horizontally four inches on center.

Regardless of the material used, you need to ensure the airflow is not restricted and is adequate for your facility. Like the bars, grilles must be permanently affixed to the duct in the same manner.

Knowledge Check – 1

You are inspecting a window on a modified SAPF. What should you look for?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- □ The window is protected by a security alarm if it is within 18 feet of the ground or accessible platform.
- □ The window can open if it is 27 feet from the ground.
- □ The bottom of the window is placed at least 18 feet from the ground or adjacent platform.
- □ The window is non-opening.

Knowledge Check – 2

You are inspecting the penetrations on a SAPF. What should you look for?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- □ Electrical utilities are entering the SAPF at a single point.
- □ The vents and ducts are protected to meet the acoustic requirements.
- □ Bars and grilles are on vents under 96 square inches.
- □ The walls surrounding duct penetrations are finished to eliminate openings between the duct and the wall.

Conclusion

Lesson Summary

Excellent! Verifying the construction techniques and materials used to meet the requirements is a major part of our job. We have discussed the SAPF criteria for windows and penetrations to ensure the risk of unauthorized individuals gaining access to classified materials is mitigated.

Lesson 5: Walls, Ceilings, Floors, and SAPCAs

Introduction

Lesson Overview

[Jeff] Having secure doors, windows, and vents will surely help protect unauthorized disclosures of sensitive information. But they will be meaningless if the walls of your Special Access Program Facility (SAPF), are not constructed to prevent forced entry or meet acoustic standards. Our goal is to ensure you are as prepared as possible to ensure your facility gets accredited. Take a moment to review the lesson objectives:

- Describe open and closed storage area construction requirements
- Verify that walls, ceilings, floors, and SAPCAs meet standards

So, let’s look into the criteria for walls, ceilings, floors, and SAP Compartmented Areas (SAPCAs).

Storage Designations

Closed/Open Storage

Before reviewing the construction requirements for the facility, it’s important to understand the storage designations for SAP areas. These storage designations can impact the construction requirements. SAP areas can have one of two storage designations:

- Closed storage
- Open storage

Closed Storage

Closed storage means that users must secure all classified information in a General Services Administration (GSA) approved storage container when not in active use. The security requirements for a closed storage facility are more rigid than an open storage facility or area. Access controls and visual protections are the standard safeguard for closed storage and will be discussed later in this lesson.

Open Storage

In an open storage area or facility, classified information does not need to be stored in a General Services Administration (GSA) approved storage container when the facility is not physically occupied by authorized personnel. However, it is a best practice to secure classified information in a GSA-approved storage container when you are not actively using the program information.

Walls

Walls Overview

If you want to protect a resource, then surrounding that item with walls is a time-tested solution. The more valuable the resource, the stronger the walls should be. Now, I think most would agree that our compartmented or classified information is an extremely valuable resource. Therefore, the walls that we use to protect that information need to be built to prevent forced entry and meet acoustic standards. Because we have different types of storage areas, we have multiple wall types to accommodate the activities within.

Perimeter Wall Construction

Perimeter walls outline the confines of the SAPF. On perimeter walls, power and signal distribution receptacles must be surface mounted. This includes power outlets, switches, and network cabling.

There are three types of walls that a perimeter wall would be constructed of: Wall Type A, Wall Type B, and Wall Type C. We will describe the specifications for these wall types later in the lesson. When inspecting SAPF perimeter walls, you will refer to the criteria in the IC Tech Spec, Chapter 3, Section C. In addition, perimeter walls must meet the standards described within ICS 705-1 for SAPF perimeters.

Perimeter Wall Construction Criteria

The type of perimeter wall needed for a SAPF depends on the type of storage mandated and discussion areas required within. Keep in mind, if your facility has existing walls made from materials that meet or exceed the perimeter wall construction standards, those walls may be used.

- If the space is designated for closed storage, there will not be any forced entry or acoustic requirements.
- If the space is designated for open storage, it will require additional protection against forced and unauthorized entry.

Please note that on any of the wall types the Certified TEMPEST Technical Authorities (CTTA), could recommend the countermeasure of Radio Frequency (RF) shielding via foil backed Gypsum Wallboard (GWB), or a layer of approved Ultra Radiant R-Foil on the secure side of SAPF walls.

Wall Types

If your SAPF will be closed storage, contain a Special Access Program Working Area (SAPWA) with continuous operation, or be open storage with Security in Depth (SID), then the standard acoustic wall or wall Type A may meet your needs.

If your SAPF will be an open storage facility or have an open storage area without SID, then wall Type B or C will be what you are looking for.

Access the SAPF/SCIF Wall Types document in the Course Resources and keep it open as we explain each wall.

Wall Type A Criteria

Wall type A normally requires three layers of 5/8" gypsum wallboard to meet the sound Group 3 rating. However, if the wall needs to meet a Sound Group 4 rating, the wall will require a fourth sheet of gypsum wallboard on the uncontrolled side.

For SAPF wall construction, we will use three 5/8" 16-gauge metal studs or standard 2X4 wooden studs placed every 16 inches on center. To meet sound ratings and to ensure there is never a straight gap between the two sheets of gypsum board on the controlled side, the sheets should be staggered so the seams are not directly on top of each other.

Listed below is the order of the wall components for Wall Type A starting from the controlled side (interior) to the uncontrolled side (exterior):

1. Paint
2. Gypsum wallboard
3. Gypsum wallboard
4. Studs/Acoustical filling
5. Gypsum wallboard
6. Paint

Wall Type A Acoustic Protection and Finishing

The next layer of sound protection is adding the sound attenuation material. The material needs to be 3 ½" thick and secured to prevent the material from sliding down the interior of the wall over time. Failing to complete this critical step could result in voids in the top portion of the wall where sound may escape.

You may think that three layers of gypsum board and sound attenuation material would dampen the sound enough to meet our needs but we must ensure these facilities meet a specific sound group rating. Therefore, we need to ensure the 16-gauge continuous tract that holds the wall framing is sealed with a continuous bead of acoustic sealant where it meets the true ceiling and true floor. But we are not done sealing the walls yet. All gaps in where the wall meets the true celling and true floor need to be filled with fire safe non-shrink grout or acoustic sealant on both sides of the wall.

The final requirement for wall type A is ensuring the wall is finished and painted from true ceiling to true floor. That means you should see no screws, tape, seams, or gaps above the acoustical ceiling, wall penetrations or below the false floor.

Wall Type B Criteria

Let's look at a Type B wall or an expanded metal wall. Type B walls have all of the same requirements as Type A walls with one difference: the addition of a layer of expanded metal mesh on the controlled side under the two layers of gypsum wallboard.

The expanded metal layer needs to be secured to the metal studs from the floor to the ceiling. One way to do this is by spot welding it to the studs in 6-inch intervals. If spot welding is used to fasten the expanded metal to the studs, you need to note it in the Fixed Facility Checklist (FFC). If spot welding is not an option, the expanded metal layer can be secured using hardened screws or washers or clips. Screws shall be applied every 6-inches along the length of each vertical stud and at the ceiling and the floor. If screws are used to fasten the expanded metal to the studs, it needs to be noted in the FFC as well.

Listed below is the order of the wall components for Wall Type B starting from the controlled side (interior) to the uncontrolled side (exterior):

1. Paint
2. Gypsum wallboard
3. Gypsum wallboard
4. Expanded metal mesh
5. Studs/Acoustical filling
6. Gypsum wallboard
7. Paint

Wall Type C Criteria

Many of the Type A wall requirements are the same for a Type C wall as well. Let's go over the different criteria for this wall.

One difference between wall Type A and wall Type C is the addition of a layer of one ½" plywood on the controlled side under a single layer of gypsum wallboard. Another is having two layers of gypsum wallboard on the uncontrolled side, rather than a single layer on walls A and B. While on the controlled side there is only one layer of gypsum wallboard.

Keep in mind that if CTTA recommends a layer of RF protection be installed to provide RF shielding, the foil shall be placed between the layer of plywood and gypsum wallboard on the controlled side. The RF material will determine how this is implemented.

The plywood needs to be installed with the long edge positioned vertically and the short edge positioned horizontally. Once placed correctly, the plywood needs to be secured to the 16-gauge studs using glue and steel self-tapping screws every 12 inches. The gypsum wallboard layer on the controlled side will be secured to the plywood and not the studs themselves. This is done to ensure no acoustic flanking path exists in the wall.

As you can see, the criteria you need to follow for your SAPF walls will depend on the information that you need to protect.

Listed below is the order of the wall components for Wall Type C starting from the controlled side (interior) to the uncontrolled side (exterior):

1. Paint
2. Gypsum wallboard
3. RF foil – if recommended by CTTA
4. Plywood
5. Studs/Acoustical filling
6. Gypsum wallboard
7. Gypsum wallboard
8. Paint

Floors and Ceilings

Floors and Ceiling Criteria

There are two features of our facility that we still need to discuss: the floor and the ceiling. The floors and ceilings of a SAPF need to meet the same requirements for forced entry and acoustic protection as the walls that surround it unless the SAPF Accrediting Official (SAO) approved another method. It wouldn’t make sense to build walls that are rated for Sound Group 4 if the ceiling doesn’t even meet Sound Group 3.

As it is with our SAPF walls, floor and ceiling penetrations need to be kept to a minimum. Refer to the criteria listed in the IC Tech Spec, Chapter 3, Section D when inspecting SAPF floors and ceilings.

SAPCAs

SAP Compartmented Area - Defined

There may be additional areas within a SAPF that walls are intended to protect other than the perimeter. We call these areas “SAP Compartmented Areas,” or SAPCAs. These areas are used to separate or segregate information, systems, and programs within a single SAPF or Sensitive Compartmented Information Facility (SCIF).

The area should be approved by the SAO, and the SAP Compartmented Area FFC should be used to request approval. SAP Compartmented areas have specific access control, visual protection, and acoustic protection requirements that may determine the type of wall that is needed.

SAP Compartmented Area - Requirements

Let’s look at the requirements.

SAPCA Access Control

Because a SAPCA is within a SAPF, the access requirements into the area are not as stringent as they are for the facility. Access can be controlled by visual recognition or some form of approved mechanical or electronic access control devices.

However, there is no need for a high security lock like a CDX-09 or a CDX-10. Spin-dial combination locks should not be installed on SAPCA doors, and independent alarm systems should not be installed in a SAPCA.

SAPCA Visual Protection

In a compartmented area, visual protection measures must be considered to reduce the ability of "shoulder surfing" or inadvertent viewing of SAP compartmented information. Some possible protections include:

- Positioning the computer screen away from the doorway or cubicle opening
- Using a polarizing privacy screen
- Using partitions and/or signs
- Using existing private offices or rooms

If you know during the planning stage that your facility will include several SAPCAs, you may be able to incorporate walls that provide permanent protection and separation of controlled systems, compartments, sub-compartments, or controlled access programs in the design phase of construction.

SAPCA Acoustic Protection

Although not a SAPCA-specific requirement, all SAPFs require some form of protection from prying ears outside. A SAPCA will need to meet the same criteria as the SAPF in which it is housed.

All TEMPEST, administrative telephone, and technical surveillance countermeasure (TSCM) requirements for the parent SAPF shall apply to the SAPCA and shall be reciprocally accepted. When compartmented discussions are required, use existing rooms that have been accredited for SAP discussions and use administrative procedures to restrict access to the room during conversations.

SAPCA Wall Acoustic Protection Criteria

As with SAPF doors and windows, SAPCA walls have to meet acoustic and sound group rating standards. This is normally accomplished by using the wall construction techniques listed in the IC Tech Spec. However, we may need to take additional steps to ensure we meet the sound rating required.

When Sound Group 3 or 4 cannot be met with normal construction, incorporate supplemental mitigations, such as those we've discussed earlier, to protect classified discussions from being overheard by unauthorized persons.

SAPCAs with Open Storage

The requirements for an open storage SAPCA are not as stringent if located in an open storage SAPF. In rare instances when open storage of information is required, the following apply. If the parent SAPF has been built and accredited for open storage, the SAPCA could have a private office or room with the standard access controls we discussed earlier. Entrance requirements need to be under the visual control of authorized individuals or have an automated entry control system installed to ensure only authorized individuals can enter the area.

If the parent SAPF has been built and accredited for closed storage, then the SAPF perimeter shall be constructed and accredited to open storage standards. This may require the construction of new walls or doors.

Knowledge Check – 1

If the SAPCA is approved for open storage of information, which of the following apply?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- □ If the parent SAPF has been built and accredited for open storage, a private office with access control on the door is adequate physical security protection.
- □ If the parent SAPF has been built and accredited for closed storage, a private office with access control on the door is adequate physical security protection.
- □ If the parent SAPF has been built and accredited for closed storage, then the SAPCA perimeter shall be constructed and accredited to open storage standards.
- □ If the parent SAPF has been built and accredited for open storage, then the SAPCA perimeter needs to be upgraded to open storage standards.

Knowledge Check – 2

Which of the following types of SAP walls contains only three layers of gypsum wallboard (one layer on the uncontrolled side and two on the controlled side) with no expanded metal?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

- ○ Wall Type A
- ○ Wall Type B
- ○ Wall Type C
- ○ Perimeter Wall

Knowledge Check – 3

Which wall type contains a ½” plywood layer and three layers of ⅝” thick gypsum wallboard—two layers on the uncontrolled side and one layer on the controlled side of the SAPF?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ Wall Type A

○ Wall Type B

○ Wall Type C

○ Perimeter Wall

Conclusion

Lesson Summary

All the security in the world would be meaningless if the walls of your SAPF are not constructed to prevent forced entry or meet acoustic standards. We discussed the differences between open and closed storage area requirements and the criteria for building walls, ceilings, floors, and SAPCAs.

Lesson 6: Intrusion Detection Systems

Introduction

Lesson Overview

[Jeff] Let's face it, no matter how strong you make the doors and walls in your Special Access Program Facility (SAPF) there will always be a risk of a perimeter breach given enough time and the right tools. The mitigation is to alert the security personnel or responders as quickly as possible so the time element of the equation is reduced enough to catch the perpetrators before they are successful.

We use an Intrusion Detection System (IDS) to alert the security team that someone or something is trying to break into your SAPF. You can find the IDS criteria listed in the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (IC Tech Spec), Chapter 7, Intrusion Detection Systems.

Take a moment to review the lesson objectives:

- Determine system requirements
- Inspect system components

IDS Requirements

What is an Intrusion Detection System (IDS)

Before we get too far, let's make sure we know what an IDS is. An IDS is an automated system that detects an intrusion of a specified site, facility, or perimeter and triggers an alarm. It consists of sensors and a premise control unit (PCU). We use these systems to alert us to:

- Movement
- Temperature changes
- Power loss
- Vibrations
- Tampering
- Breaking windows

These alerts can help protect the information within our SAPF from break-ins and theft.

General Protection Requirements

Now that we know what an IDS is, let's look at how it is supposed to protect that information. First, anytime a SAPF is not occupied, the IDS must be armed and working properly. Some areas inside a

SAPF may need a higher level of protection than the rest of the facility perimeter. Having an open storage area within a closed storage facility is an example. The areas adjacent to the open storage area that we feel someone could gain access through will need to be protected by the IDS as well.

What kind of doors are we talking about here? Well, emergency doors would be a good example. These doors have no external hardware or access controls and usually are not under the constant visual observation of cameras and security personnel. Therefore, the IDS must monitor these doors continuously.

This is the part that most security practitioners don't like very much, but it is crucial to have emergency action plans in the event of a system failure. Mechanical and electrical components break down, it's a fact of life. So, to mitigate the risk of a SAPF being left unprotected due to system failure, SAP-indoctrinated personnel will physically occupy the SAPF until the system is functioning again.

The last general requirement we need to discuss for the IDS is ensuring the SAPF alarm emergency action plan lays out the actions that need to be taken in the event of a system failure. It should list individuals that need to be contacted to report and fix the issue and outline the plan to keep the facility occupied until repairs are made.

Installations

Now that we know what an IDS is and what it is supposed to protect, let's talk about the IDS installation-related components and monitoring station requirements that an IDS must meet. There are system component and installation standards outlined in Underwriters Laboratories (UL) 2050, Standard for National Industrial Security Systems for the Protection of Classified Material.

You will find the Extent 3 requirements for installation. Extent 3 requirements are the highest level of security for National Industrial Security Systems. Keep in mind that systems developed and used exclusively by the U.S. Government do not require UL certification but shall nonetheless comply with an Extent 3 installation as referenced in UL 2050.

High Security Switches and Sensors

Areas of a SAPF through which reasonable access could be gained, including walls common to areas not protected at the SAPF level, shall be protected by IDS. The high-security switches (HSS) and sensors we use in our IDS must comply with UL standards 634 and 639 respectively. SAPF construction requirements require the use of UL Level II HSS. In existing facilities, the use of existing UL Level I HSS are authorized until major IDS modifications or upgrades are made.

Cabling

As you may imagine, all of the sensors, switches, and security equipment must be connected to an alarm security panel. This means a lot of wires. If these wires go outside the SAPF perimeter, they need to be protected with encryption or placed in approved conduit called Electrical Metallic Tubing (EMT).

All joints and connections shall be permanently sealed completely around all surfaces using methods such as welding, epoxy and fusion. Set screws shall not be used. The seal shall provide a continuous bond between the components of the conveyance. If those conduits need to run through a service or pull box, then the box must be secured with a U.S. General Services Administration (GSA) approved lock or a SAPF Accrediting Official (SAO) approved lock.

Systems

The IDS must be completely separate from other systems such as fire, smoke, radon, water, or gas detection systems. One reason for this requirement is that it ensures the IDS does not need to be taken off-line for maintenance of the other system. Also, your IDS cannot include audio or video monitoring equipment without adding the appropriate countermeasure and getting approval from the SAPF Accrediting Official (SAO) or the Accrediting Official (AO).

Now that we have talked about the IDS's general and system requirements, let's talk about some of the individual components of an IDS.

IDS Components

Sensors

So you may have figured out some of the equipment but let's go a little more in depth about the IDS's major components. These include sensors and premise control units (PCUs).

Depending on the type of sensor, they can detect movement, opening doors, and breaking windows. Regardless of the type of sensor, they all need to be installed within the SAPF perimeter. You, as the SAO, will need to approve any sensor placed outside the perimeter.

We may employ dual technology sensors in our SAPF, but the technologies must be able to trigger the alarm without input from the other. Some dual technology sensors require both technologies be activated to trigger the alarm, so be sure to check the sensors specifications.

We need to have enough sensors in the system to ensure your SAPF is adequately protected by the IDS. The coverage must meet the requirements listed in IC Tech Spec or be approved by the SAO. However, for facilities outside the U.S. and in Category I and II countries, the SAO may require motion detection sensors above false ceilings and/or below false floors.

All perimeter doors of your SAPF need to be protected by the IDS using HSS and motion sensors. However, if the primary entrance door employs a delay to allow for changing the system mode of access, the delay shall not exceed 30 seconds. Finally, we need to ensure all emergency exits are alarmed 24/7. That pretty much covers sensors. Let's go over the PCU requirements next.

Premise Control Unit (PCU) Defined

Before we get into its requirements, let's define what a PCU is. A PCU is an electronic device that continuously monitors the alarm status of local IDS and transmits alarm conditions to a remote monitoring system. The PCU allows authorized personnel to place the alarm zone in an armed or disarmed status via a local keypad, credential reader, or biometric device.

PCU Overview

Now let's look at the requirements. The first requirement is that the PCU needs to be placed within the confines of the SAPF and only SAPF personnel can make changes to the access modes. Makes sense, right? We wouldn't want our PCU outside of the perimeter. We want to ensure the PCU is kept safe from prying eyes or casual or unauthorized observers.

PCU Cabling

The next requirement is for the cabling between the sensors and the PCU. It must be used only by the IDS, installed all within the SAPF, and comply with all electric codes and Committee on National Security Systems (CNSS) standards.

PCU Alarm

In addition, the PCU must put out a persistent alarm for any one of the following conditions:

- Intrusion detection
- Failed sensor
- Tamper detection
- Maintenance mode
- IDS sensor points shunted or masked during maintenance mode

Finally, any IDS cabling or transmission lines that extend past the SAPF perimeter need to meet National Institute of Standards and Technology Federal Information Processing Standards (FIPS) 197 and 140-2.

Certifications Required

The FIPS employed must be noted on the UL 2050/CRZH Certificate or other certificate employed. CRZH is the category code used by UL to certify that a facility complies with UL 2050 standards for National Industrial Security Systems. Listed below are the certification method requirements.

Certification Method	**Requirements**
PCUs certified under UL 1610	Must meet FIPS 197 or FIPS 140-2 encryption certification and methods
PCUs certified under UL 1076	Only FIPS 140-2 is the acceptable encryption certification and method
Alternative methods	Must be approved by the SAO and noted on the IDS Certificate

Knowledge Check – 1

Which UL rating must IDS installations, related components, and monitoring stations comply with?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ UL 2048

○ UL 2050

○ UL 2639

○ UL 2634

Knowledge Check – 2

When inspecting the sensors for an IDS, what should you look for?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

□ The sensors are located within the SAPF perimeter.

□ The emergency exit doors are alarmed and monitored 24 hours a day.

□ Dual technology sensors require both technologies to be activated to trigger the alarm.

□ The number of motion detection sensors are installed to meet the requirements of the IC Tech Spec.

Conclusion

Lesson Summary

If it can be built, it can be broken. The doors and walls of your SAPF will always be a perimeter breach risk. The IDS reduces that risk by alerting us to the attempted breach before the perpetrator has time to access our critical information. We discussed the IDS requirements and its components to better prepare you for ensuring the IDS in your SAPF is fully functional.

Lesson 7: Telecommunications

Introduction

Lesson Overview

[Jeff] As much as we need to protect classified or sensitive information from falling into the wrong hands, we need to be able to communicate with individuals all over the world. This requires an unclassified telecommunications system that meets security requirements and protects the information from being compromised or intercepted.

You can find the telecommunications technical specification criteria listed in the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (IC Tech Spec), Chapter 11, “Telecommunications Systems”.

Before we dive into the criteria for Special Access Program Facility (SAPF) telecommunications systems, let’s review our objectives for this lesson.

- Determine physical and software access controls for unclassified phones
- Evaluate unclassified information systems and cable
- Evaluate emergency notification systems

Unclassified Telephone Systems

Unclassified Telephone Requirements

I must tell you that the guidance we will cover is compatible with security requirements of other disciplines such as Information Systems Security, Communications Security, Operational Security, or TEMPEST. Be sure to review those disciplines’ guidance and checklists to ensure you are in compliance.

The configuration of unclassified telephone systems used in SAPFs needs to be baselined and documented in the Fixed Facility Checklist (FFC). The baseline needs to include all devices, features, and software used by the system. All the security systems, special doors, and soundproofing would be worthless if someone could externally tap into our unclassified telephone system and turn on our phone’s microphone and eavesdrop on our conversations. When not in use, unclassified telephone systems shall not transmit audio and shall be configured to prevent external control or activation, technical exploitation, or penetration.

One of the ways we prevent anyone from accessing our unclassified telephone system is by limiting access to the system with physical and software access controls, such as a secure communications closet. We also need to ensure the equipment meets on-hook and off-hook audio protection requirements by verifying it’s listed in the references.

If we discover telephones or instruments not type-accepted, they will be presumed to have on-hook audio available at the mounting cord until determined otherwise. Determining telephone stations that don't have on-hook audio hazards requires a technical investigation that may only be conducted by a Technical Surveillance Countermeasures team or National Telephone Security Working Group authorized telephone laboratory.

Unclassified Information Systems and Cable

Unclassified Information Systems Requirements

One of the best ways to keep classified or sensitive information safe is by segregating it from unclassified information. Our information systems are designed to follow the same logic. But, that does not mean the unclassified information systems are left unprotected. These systems have their own protection requirements.

The best way to protect our unclassified information system is to control and limit access to the system's hardware and software. Access to server and telecommunications rooms should be limited to only those that who maintain the system.

You may recall that our Intrusion Detection System (IDS) had to have remote access to the system disabled to prevent tampering. Well, our unclassified information system's telephonic and audio features need to be protected from remote activation as well.

Any unclassified video or teleconferencing equipment that is in the SAPF needs to be turned off and its cables disconnected from the system when it's not being used.

Finally, any video equipment used in a SAPF needs to have a very visible indicator that alerts them when the system is recording or transmitting. While we are discussing video devices, let's talk about Closed Circuit Television (CCTV) systems.

Closed Circuit Television (CCTV) System Requirements

Having a CCTV system is not a requirement for a SAPF, but these systems can supplement your security team by allowing them to monitor areas around your facility that would require additional personnel and expense. Not only can we use them to say, monitor the entrances, but we can also use the recordings to investigate any actions or unauthorized entries that take place.

The CCTV system, if used, cannot pose a threat to the security of our SAPF. Therefore, the CCTV systems require their own computers, cabling, and network access. No part of a CCTV system, if installed, can penetrate the SAPF perimeter. Everything required to operate the system must be installed exterior to the SAPF perimeter walls. However, waivers can be requested by the Special Access Program Facility Accrediting Official (SAO) or the Accrediting Official (AO) for elements of a CCTV system to be internal to the SAPF perimeter.

If we place CCTV cameras around our facility's entry door, we need to ensure the camera's view does not capture any classified information or access control components, such as the keypad where facility employees enter their personal identification number (PIN) to gain entry to the SAPF. There is a chance a facility you manage may utilize a CCTV system, but I can pretty much guarantee that facility will have an environmental infrastructure and an emergency notification system. Let's talk about those next.

Environmental Infrastructure Systems Requirements

Let's start with environmental infrastructure systems. So, what are they? Well, these systems work in the background to monitor and create a workable environment for SAPF employees and ensure continuous operations.

Our FFC needs to document if the facility contains any environmental infrastructure systems, also referred to as building maintenance systems. These systems include premise management systems, environmental control systems, lighting and power control units, and uninterrupted power sources.

Our checklist also needs to include the location of all external connections and describe what countermeasures have been put in place. Some of the reasons your facility may require external connections include remote monitoring, access and external control of features and services, and protection measures taken to prevent malicious activity, intrusion, and exploitation.

Unclassified Cable Control Requirements

As we stated previously, the fewer holes you have in a bucket, the easier it is to contain water within it. Well, that philosophy applies to SAPF construction. The fewer holes that are in the facility's perimeter, the lower the risk of classified information being released. Therefore, our facility's telecommunications wiring and cabling needs to enter the facility through a single opening, if possible. Of course, the bigger the SAPF, the more cabling that will be required, and a single opening may not be practical.

We must know what every cable that enters the facility perimeter is used for, even if it's for future expansion. So, at the point where the cables enter the SAPF, each cable needs to be labeled. We can do this several ways, but they must identify the precise use of every cable through labeling or log entries. Designated spare conductors shall be identified, labeled, and bundled together.

If your SAPF is a modified facility, there is a good chance you may have some unused conductors left over from the previous occupants. These unused conductors need to be removed, but removal may not be an option in all cases. At a minimum, these unused conductors should be stripped, bound, and grounded where they enter or exit the facility. Unused fiber optic cabling is treated in a similar manner, however rather than stripping and grounding, the fiber is capped and labeled as unused fiber. The proper use and handling of the SAPF wires and cables can go a long way in keeping our facility and information secure.

We have discussed a lot of information about SAPF unclassified telephone systems and unclassified information systems and cable; now let's talk about the emergency notification system.

Emergency Notification Systems

Emergency Notification Systems Requirements

Keeping all electronic system components within the SAPF perimeter is probably the best way to ensure that they are secure. However, when it comes to emergency notification systems, there are exceptions. These include systems approved by the SAO, systems required for security purposes, and systems that are required under life safety regulations.

So, our fire alarm system may require some form of speakers or other transducers that are not completely contained within the SAPF perimeter. If it does, the system must meet some additional protection requirements.

As with any system, the emergency notification system's wiring must penetrate the SAPF perimeter at one location. TEMPEST or Technical Security Countermeasures (TSCM), concerns may require electronic isolation and shall require review and approval by the Certified TEMPEST Technical Authorities.

Any one-way communication system that sends audio into the facility will require a high-gain amplifier to amplify the incoming signal. You shouldn't see emergency notification systems that require two-way communication systems in a SAPF very often, but they may be used in the rarest of circumstances. If they are used, they shall be protected so that audio cannot leave the SAPF without the SAPF occupants being alerted when the system is activated.

Finally, any electronic isolation components that make up the system need to be installed within the SAPF perimeter. They also need to be installed in the SAPF as close as possible to the point of entry used by the system's wiring.

These systems utilize a lot of wires and cables to operate properly. There are standards for wire and cabling installation as well. The proper use and handling of the SAPF wires and cables can go a long way in keeping our facility and information secure.

Knowledge Check – 1

What should you look for when evaluating unclassified phones?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- □ They incorporate physical and software access controls to prevent disclosure or manipulation of system programming and data.
- □ They are set up to prevent external control or activation, technical exploitation, or penetration.
- □ They are integrated with the closed circuit television system.
- □ They provide on-hook and off-hook audio protection.

Knowledge Check – 2

You are evaluating unclassified cables in a SAPF. You notice that all telecommunication cabling enters the SAPF through a single opening and allows for visual inspection. Does this meet the standards?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ Yes, all telecommunication cabling should enter the SAPF through a single opening and allow for visual inspection, where possible.

○ It partially meets the standards. All telecommunication cabling should enter the SAPF through a single opening but it does not need to allow for visual inspection.

○ No, telecommunication cabling can enter the SAPF through multiple openings as long as it allows for visual inspection.

○ No, there are no specific requirements for how telecommunication cabling enters the SAPF.

Knowledge Check – 3

You are evaluating the emergency notification systems in a SAPF. You notice that all the electronic system components are not within the SAPF perimeter which is not aligned with specifications. What should you check to determine if there is an exception?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

□ The system was approved by the SAO.

□ The system is required for security purposes.

□ The system is required under life safety regulations.

□ There are no exceptions. All electronic system components need to be kept within the SAPF perimeter.

Conclusion

Lesson Summary

Telecommunication and information systems are the circulatory systems that keep the information age alive. Without them, we would go back to using carrier pigeons.

As you have learned, keeping the unclassified telephones, unclassified information systems and cable, and the emergency notification systems secure, ensures the information keeps flowing without compromising the data’s security.

Lesson 8: Course Conclusion

Conclusion

Lesson Review

[Narrator] Listed below are the lessons in the course.

- Lesson 1: Course Introduction
- Lesson 2: SAPF Physical Security Construction Requirements
- Lesson 3: Doors
- Lesson 4: Windows and Penetrations
- Lesson 5: Walls, Ceilings, Floors, and SAPCAs
- Lesson 6: Intrusion Detection Systems
- Lesson 7: Telecommunications
- Lesson 8: Course Conclusion

Lesson Summary

Congratulations! You have completed the Physical Security Construction Requirements for SAP course. You should now be able to perform the following activities:

- Given an instruction, determine DOD guidance and ICS for the construction, accreditation, and inspection of SAPFs.
- Given an immersive environment, a scenario, and the blank Fixed Facility Checklist (FFC):
  - Inspect SAPF doors for compliance with DOD physical security criteria.
  - Analyze SAPF windows, ducts, ventilation, and access/inspection ports for compliance with DOD physical security criteria.
  - Verify that SAPF walls, ceilings, floors, and SAPCAs are compliant with DOD physical security criteria.
  - Evaluate SAPF intrusion detection systems (IDS) for compliance with DOD physical security criteria.
  - Evaluate SAPF telecommunications for compliance with DOD physical security criteria.

To receive course credit, you MUST take the Physical Security Construction Requirements for SAP practical exercise. Please use the STEPP system from the Center for Development of Security Excellence to access the online practical exercise.

Appendix A: Answer Key

Lesson 2 Review Activities

Knowledge Check – 1

Which of the following policy documents should you consult when you need to determine the physical security specifications and best practices for meeting SAPF construction and renovation standards?

○ ICD 731

○ DODM 5205.07, Volume 2

○ DODM 5205.21, Volume 3

● IC Tech Spec for ICD/ICS 705 (correct response)

***Feedback**: IC Tech Spec for ICD/ICS 705 is the policy document you should consult when you need to determine the physical security specifications and best practices for meeting SAPF construction and renovation standards.*

Knowledge Check – 2

Which of the following is used to inspect SAPFs for initial accreditation and periodic inspections?

● Fixed Facility Checklist (FFC) (correct response)

○ Standard Operating Procedures (SOPs)

○ Physical Security Pre-Construction Plans

○ SAPF Inspection Checklist

***Feedback**: The Fixed Facility Checklist is used to inspect SAPFs for initial accreditation and periodic inspections.*

Knowledge Check – 3

Which of the following inspections should the SAO perform for a SAPF?

□ Pre-contract inspection

☑ Initial accreditation inspection (correct response)

□ Post-contract inspection

☑ Periodic inspection (correct response)

***Feedback**: Initial accreditation inspection and periodic inspection are both inspections that the SAO should perform for a SAPF.*

Knowledge Check – 4

Which of the following statements are true about reciprocity?

- □ With reciprocity, procedures to prevent unauthorized personnel from accessing compartmented or program information primarily focus on acoustic security measures.
- ☑ Reciprocity promotes efficiency and helps achieve financial savings. (correct response)
- ☑ With reciprocity, procedures must be in place to prevent unauthorized personnel from accessing compartmented or program information. (correct response)
- ☑ Reciprocity occurs when there is a requirement to share an accredited SCIF or portion with a compartment, program, or special activity. (correct response)

Feedback*: Reciprocity promotes efficiency and helps achieve financial savings, with reciprocity, procedures must be in place to prevent unauthorized personnel from accessing compartmented or program information, and reciprocity occurs when there is a requirement to share an accredited SCIF or portion with a compartment, program, or special activity.*

Lesson 3 Review Activities

Knowledge Check 1

You are tasked to examine the primary and secondary doors. What will you need to evaluate?

- ☑ The doorframe (correct response)
- ☑ The hardware on the door (correct response)
- ☑ The locking devices on the door (correct response)
- □ You only need to examine the door construction, not the door components.

Feedback*: When examining primary and secondary doors you will examine the doorframe, the hardware on the door, and the locking devices on the door.*

Knowledge Check 2

While inspecting an emergency exit door on a SAPF, you see it has deadlocking panic hardware on the inside and a CDX-10 lock on the outside. Would this door meet the criteria for emergency doors in a SAPF, and why (or why not)?

- ⦿ No. Emergency exit doors must not have exterior hardware. (correct response)
- ○ Yes. This hardware meets Federal Specification FF-L-2890, Type III.
- ○ No. This hardware does not meet Federal Specification FF-L-2890, Type III.
- ○ Yes. The exterior hardware is for emergency responders to gain access.

Feedback*: This door would not meet the criteria for emergency doors in a SAPF because it must not have exterior hardware.*

Knowledge Check 3

What must SAPFs equipped with double doors have installed to prevent individuals from looking between the doors into a classified room?

○ 180-degree peep hole

○ Local audible annunciation device

○ 24/7 video surveillance

◉ Astragal strip (correct response)

***Feedback**: SAPFs equipped with double doors must install astragal strip to prevent individuals from looking between the doors into a classified room.*

Knowledge Check 4

You are evaluating the acoustical protections of the doors in a SAPF. What specifications may be present to ensure that the doors will mitigate sound transmissions?

□ There was astragal strip added to the door.

□ The SAPF door has an HSS.

☑ The SAPF doors and frame assemblies meet acoustic requirements. (correct response)

☑ There were sound-source generators added to the SAPF. (correct response)

***Feedback**: Ensuring the SAPF doors and frame assemblies meet acoustic requirements and adding sound source generators to the SAPF will all help mitigate sound transmissions.*

Lesson 4 Review Activities

Knowledge Check – 1

You are inspecting a window on a modified SAPF. What should you look for?

☑ The window is protected by a security alarm if it is within 18 feet of the ground or accessible platform. (correct response)

□ The window can open if it is 27 feet from the ground.

☑ The bottom of the window is placed at least 18 feet from the ground or adjacent platform. (correct response)

☑ The window is non-opening. (correct response)

***Feedback**: When inspecting a window on a modified SAPF you would look to ensure the window is protected by a security alarm if it is within 18 feet of the ground or accessible platform, the bottom of the window is placed at least 18 feet from the ground or adjacent platform, and the window is non-opening.*

Knowledge Check – 2

You are inspecting the penetrations on a SAPF. What should you look for?

- ☑ Electrical utilities are entering the SAPF at a single point. (correct response)
- ☑ The vents and ducts are protected to meet the acoustic requirements. (correct response)
- □ Bars and grilles are on vents under 96 square inches.
- ☑ The walls surrounding duct penetrations are finished to eliminate openings between the duct and the wall. (correct response)

Feedback*: When inspecting penetrations from a SAPF you should look to ensure electrical utilities are entering the SAPF at a single point, the vents and ducts are protected to meet the acoustic requirements, and the walls surrounding duct penetrations are finished to eliminate openings between the duct and the wall.*

Lesson 5 Review Activities

Knowledge Check – 1

If the SAPCA is approved for open storage of information, which of the following apply?

- ☑ If the parent SAPF has been built and accredited for open storage, a private office with access control on the door is adequate physical security protection. (correct response)
- □ If the parent SAPF has been built and accredited for closed storage, a private office with access control on the door is adequate physical security protection.
- ☑ If the parent SAPF has been built and accredited for closed storage, then the SAPCA perimeter shall be constructed and accredited to open storage standards. (correct response)
- □ If the parent SAPF has been built and accredited for open storage, then the SAPCA perimeter needs to be upgraded to open storage standards.

Feedback*: If the SAPCA is approved for open storage of information and the parent SAPF has been built and accredited for open storage, a private office with access control on the door is adequate physical security protection. If the parent SAPF has been built and accredited for closed storage, then the SAPCA perimeter shall be constructed and accredited to open storage standards.*

Knowledge Check – 2

Which of the following types of SAP walls contains only three layers of gypsum wallboard (one layer on the uncontrolled side and two on the controlled side) with no expanded metal?

◉ Wall Type A (correct response)
○ Wall Type B
○ Wall Type C
○ Perimeter Wall

***Feedback**: Wall type A contains only three layers of gypsum wallboard, one layer on the uncontrolled side and two on the controlled side, with no expanded metal.*

Knowledge Check – 3

Which wall type contains a ½" plywood layer and three layers of ⅝" thick gypsum wallboard—two layers on the uncontrolled side and one layer on the controlled side of the SAPF?

○ Wall Type A
○ Wall Type B
◉ Wall Type C (correct response)
○ Perimeter Wall

***Feedback**: Wall type C contains a ½" plywood layer and three layers of ⅝" thick gypsum wallboard: two layers on the uncontrolled side and one layer on the controlled side of the SAPF.*

Lesson 6 Review Activities

Knowledge Check – 1

Which UL rating must IDS installations, related components, and monitoring stations comply with?

○ UL 2048
◉ UL 2050 (correct response)
○ UL 2639
○ UL 2634

***Feedback**: UL 2050 is the UL rating that IDS installations, related components, and monitoring stations must comply with.*

Knowledge Check – 2

When inspecting the sensors for an IDS, what should you look for?

☑ The sensors are located within the SAPF perimeter. (correct response)

☑ The emergency exit doors are alarmed and monitored 24 hours a day. (correct response)

□ Dual technology sensors require both technologies to be activated to trigger the alarm.

☑ The number of motion detection sensors are installed to meet the requirements of the IC Tech Spec. (correct response)

Feedback*: When inspecting sensors for an IDS, you should look to ensure the sensors are located within the SAPF perimeter, the emergency exit doors are alarmed and monitored 24 hours a day, and the number of motion detection sensors are installed to meet the requirements of IC Tech Spec.*

Lesson 7 Review Activities

Knowledge Check – 1

What should you look for when evaluating unclassified phones?

☑ They incorporate physical and software access controls to prevent disclosure or manipulation of system programming and data. (correct response)

☑ They are set up to prevent external control or activation, technical exploitation, or penetration. (correct response)

□ They are integrated with the closed circuit television system.

☑ They provide on-hook and off-hook audio protection. (correct response)

Feedback*: When evaluating unclassified phones, you should ensure they incorporate physical and software access controls, they prevent external control or activation, technical exploitation, or penetration, and they provide on-hook and off-hook audio protection.*

Knowledge Check – 2

You are evaluating unclassified cables in a SAPF. You notice that all telecommunication cabling enters the SAPF through a single opening and allows for visual inspection. Does this meet the standards?

● Yes, all telecommunication cabling should enter the SAPF through a single opening and allow for visual inspection, where possible. (correct response)

○ It partially meets the standards. All telecommunication cabling should enter the SAPF through a single opening but it does not need to allow for visual inspection.

○ No, telecommunication cabling can enter the SAPF through multiple openings as long as it allows for visual inspection.

○ No, there are no specific requirements for how telecommunication cabling enters the SAPF.

Feedback*: All telecommunication cabling should enter the SAPF through a single opening and allow for visual inspection, where possible.*

Knowledge Check – 3

You are evaluating the emergency notification systems in a SAPF. You notice that all the electronic system components are not within the SAPF perimeter which is not aligned with specifications. What should you check to determine if there is an exception?

- ☑ The system was approved by the SAO. (correct response)
- ☑ The system is required for security purposes. (correct response)
- ☑ The system is required under life safety regulations. (correct response)
- □ There are no exceptions. All electronic system components need to be kept within the SAPF perimeter.

Feedback*: There may be exceptions if the emergency notification system is required for security purposes, the system is required under life safety regulations, or the system was approved by the SAO.*