Special Access Program - SA501

TEFLONRABBIT ARTICLE No.217

Unique Identifier:c1934f12-2e40-413c-97e5-86b7039a143a

ICD705 SA501 compliant SCIF

ICD 705 Physical Security Construction Requirements for SAP

Monday, February 27, 2023 - 22:21

PDF Version
Aroma
Image not found or type unknown
50
Rumness
Image not found or type unknown
60
Subscription Only
Off
£
2999

Welcome to the SAPF Physical Security Construction Requirements course. This course covers the minimum 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 DOD and Intelligence Community directives.
This course places you in a scenario as the Special Access Program Facility Accrediting Official, or SAO, for a SAPF that is under construction. You will be guided through an accredited facility to learn the construction specifications and then placed in your newly constructed SAPF to evaluate construction requirements.

Repository Military Industrial Complex SCIF SAPF CIA DoD Course

Course Scenario

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

Sam: Good afternoon and thank you for joining this meeting. I know that you have just been assigned to this organization and assigned the SAO position. 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 me introduce everyone. As you know, I'm the organization's Director. Starting over here on the left is Ruben, our PSO and Jeff is our sister facility SAO.

Now, we need to get you trained on your SAO responsibilities and the accreditation requirements for our new facility. Ruben will work with you on your SAO responsibilities. Jeff will be your trainer for SAPF accreditation requirements.

Ruben: Jeff, since you 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 — 9 AM in my office. I will meet you in the lobby and escort you through security processing.

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

1

Jeff: Here are the training objectives.
Student will select the document:

SAO Training Objectives
o Recognize Intelligence Community Standard (ICS) and DOD guidance for the construction, accreditation, and inspection of SAPFs
o Inspect SAPF doors for compliance with DOD physical security criteria
o Analyze SAPF windows, ducts, ventilation, and view ports for compliance with DOD physical security criteria
o Verify that SAPF ceilings, walls, and floors are compliant with DOD physical security criteria
o Evaluate SAPF intrusion detection systems (IDS) for compliance with DOD physical security criteria
o Evaluate SAPF telecommunications for compliance with DOD physical security criteria
o Evaluate SAPF classified destruction methods for compliance with DOD physical security criteria

Course References

You have returned to your office.

Student will select the email icon:
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 ICD/ICS 705
ICD 705-1
ICS 705-2

Here is the resources link so that you can view these policy documents.
We will begin by reviewing the purpose of each of these documents tomorrow.

-Jeff

CDSE

Lesson: Physical Security Construction Requirements

SAPF Construction and Inspection Guidance

Jeff: Good morning, you're right on time. Our goal for this morning is to identify the Department of Defense, or DOD guidance and Intelligence Community Standards, also known as ICS, that covers the construction of a Special Access Program Facility, or SAPF, describe SAPF inspection and review requirements, and explain 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.

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.

Guidance for the Construction and Inspection of SAPFs

Policy guidance that we routinely use include DOD Manual 5105.21, Volume 2; DOD Manual 5200.01, Volume 3; DOD Manual 5205.07, Volume 3; ICD/ICS 705 Technical Specifications for Construction; ICS 705.02; and standard operating procedures, or SOPs. Let's review the purpose of each of these documents.

Student selects each reference:
DODM 5105.21, Volume 2: Sensitive Compartmented Information (SCI)
Administrative Security Manual: Administration of Physical Security, Visitor Control and Technical Security
- Covers the administration of physical security, visitor control, and technical security for SAPFs
- Applicable to all military departments, DOD agencies and field agencies, DOD components, and contractors in facilities accredited by the Defense intelligence Agency (DIA)

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 security procedures for physical security at DOD SAPFs

Applicable to:
- All Military departments
- DOD agencies and field agencies
- DOD components and component contractors and consultants
- Not-DOD U.S. government entities that require access to DOD SAPFs

SAO responsibilities for SAPF construction:
- 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 Security Assistance Policy Coordinating Office (CA SAPCO)
- Approve and document mitigations
- Recommend waivers APF of physical security safeguards
- Ensure mitigating strategies are implemented and documented in the Construction Security Plan CSP)

ICD/ICS 705: Technical Specifications for Construction
- Established 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 705-2: Standards of the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities
- Establishes criteria for accreditation of Sensitive Compartmented Information Facilities 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) were developed by each organization to:
- Address specific areas that may not be covered in the DOD or of policy guidance.
- Identify specific areas of security concern.
- Address specific facility mission requirements.

Accreditation and Inspections
CDSE

Let's look at the inspection 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 inspect any SAP area before accreditation. There are other inspections and reviews that must be accomplished as outlined in the IC Tech Spec for ICD and ICS 705. These include re-inspection and periodic inspections.

Re-inspections will be conducted based on threat, physical modification, sensitivity of SAPs, and past security performance.

Periodic inspections will be conducted based on threat, physical modification, sensitivity of SAPs, and past security performance, but will be conducted no less frequently than every 3 years for SAPFs.

The Fixed Facility Checklist

The Fixed Facility Checklist, also known as the FFC, is used to inspect SAPFs for the initial accreditation, re-inspection, and periodic inspections. The FFC documents physical, technical, and procedural security information including facility entrances and emergency exits, intrusion detection systems, telecommunications systems, equipment baseline, acoustical protection, classified destruction methods, and information systems.

The FFC documents physical, technical, and procedural security information including facility entrances and emergency exits, intrusion detection systems, telecommunications systems, equipment baseline, acoustical protection, classified destruction methods, and information systems.

The completed FFC will include floor plans, diagrams of electrical and communications wiring; heating, ventilation, and air conditioning connections; security equipment layout, to include the location of intrusion detection equipment and security in depth, or SID. All diagrams or drawings must be submitted on legible and reproducible media.

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. The host Cognizant Security Authority or CSA maintains oversight of the facility unless all parties agree to transfer CSA 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 SCI-related SAPs must meet the physical security requirements of ICD 705-1. Any physical security measures above those described in ICD 705-2 that are required by SAP managers should be negotiated between the SAO and AO.

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

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

Knowledge Check 1

Which of these policy documents should you consult if you want to verify the SAO responsibilities for construction of SAPFs? Select the best response.

- o DODD 5200.01
- o DODM 5205.07, Volume 3
- o DODM 5205.21, Volume 3

o DODD 5102.21

Answer: DODM 5205.07, Volume 3

Knowledge Check 2
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?
o ICD 731
o DODM 5205.07, Volume 2
o DODM 5205.21, Volume 3
o ICD/ICS 705

Answer: ICD/ICS 705

Knowledge Check 3
Which of the following inspections should the SAO perform for a SAPF? Select all that apply.
? Pre-contract inspection
? Initial accreditation inspection
? Re-inspection
? Periodic inspection

Answer: Initial accreditation inspection; Re-inspection; Periodic inspection

Knowledge Check 4
What is the purpose of conducting periodic inspections at SAPFs? Select all that apply.

? Ensure the efficiency of facility operations
? Document periodic maintenance
? Identify deficiencies
? Re-accredit the facility

Answer: Ensure the efficiency of facility operations; Identify deficiencies

Knowledge Check 5
The Fixed Facility Checklist (FFC) is used to inspect SAPFs for the initial accreditation, re-inspection, and periodic inspections. Select the best answer.
o True
o False

Answer: True

Knowledge Check 6
How does co-utilization of existing SAPFs benefit the DOD? Select all that apply.
? Promotes efficiency
? Achieves financial savings
? Identifies operational deficiencies
? Allows agencies to mirror operations

Answer: Promotes efficiency; Achieves financial savings

Lesson Summary

We have identified the DOD and ICS guidance that covers the construction of SAPF, described the SAPF inspection and review requirements, and explained reciprocity for these facilities.

Lesson: Doors

Doors Introduction

Now we will talk about the main points of entry for a Special Access Program Facility, or 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. To start, we will look at the criteria for primary and secondary doors. We will also review the requirements for emergency doors.

Doors Types – Steel and Wood Doors

When we inspect SAPF doors, we need to inspect every door and its components to ensure they match the requirements of policy. These components include the door itself, the doorframe, CDSE

---

locking devices, and hardware such as hinges, push bars, floor sweep, and automatic, non-hold door-closers.

Student selects the steel door:
Steel doors, like wood 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, door-closers, and lock areas.

Steel Doors
- 1 ¾-inch thick
- 18-gauge face steel
- Lock area predrilled and/or reinforced to 10-gauge

Student selects the right arrow and the wooden door:
Our entry doors are made of steel but the door to the breakroom is wood and meets the criteria we would be looking for. Wood doors must be 1 ¾-inch 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 outsides for dimensional stability.

Wood Doors
- 1 ¾ inch thick, solid wood core (wood stave)

Door Types – Roll-up Doors

A roll-up door in a SAPF can be a little more difficult to meet construction requirements.

Student selects the roll-up door:
They have the same 18-gauge requirement as steel doors, and these doors must be secured on either side with a deadbolt. Normally, roll-up doors are only authorized for use in non-discussion areas because they cannot be treated for acoustics. However, being 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.

Roll-up doors
- 18-guage steel or greater

- Secured inside using deadbolts on both left and right sides
- Additional locking devices such as pad locks may be used on roll-up doors.
- Located in designated not-discussion area

Door Types – Double Doors

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

Student selects the double doors:
The differences are that each door requires its own independent security switch if it is used as an entry into the SAPF, and one of the doors must be fixed with deadbolts placed on the top and
CDSE

---

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. Preventing unwanted peaking is good, but we also need to prevent unwanted listening as well.

Double doors
- Independent high-security switch
- One of the doors secured with deadbolts at top and bottom
- Astragal strip
- Door sweep

Door Acoustical Protections

The ability of a SAPF to retain sound within its perimeter is rated using a value called the Sound Transmission Class or STC. To satisfy normal security standards of SAPF transmission, attenuation groups have been established in sound groups you see here.

Door Criteria
- Sound Group 3 - STC 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 - STC 50 or better. Very loud sounds within the SAPF, such as loud singing, brass music, or a radio at full volume, can be heard with the human ear faintly or not at all outside of the SAPF.

Door Acoustical Protections (cont.)

So, we need to have ways to mitigate sound transmissions emanating from our facility – especially the doors.
One way to do this is to incorporate a vestibule. For the most part, it’s a room that separates the controlled and uncontrolled areas. It is good for keeping unwanted eyes and ears from accessing the information the SAPF was built to protect. We also need to meet the acoustic requirements as listed in ICD/ICS 705.

Sound Transmission Mitigations

Technical Specifications for Construction and Management of Sensitive Compartmented

Information Facilities IC Tech Spec?for ICD/ICS 705.

Chapter 3, Section E requirements:
- When practical, entrance doors should incorporate a vestibule to preclude visual observation and enhance acoustic protection.
- SAPF doors and frame assemblies shall meet acoustic requirements as described

in Chapter 9 unless declared a not-discussion area.

Door Acoustical Protections (cont.)

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. Chapter 9 lists

---

some ways to mitigate those issues by adding structural enhancements to the building, sound-source generators, or sound masking devices. We have covered the door types and acoustical protection, so now we can move on to the SAPF door locking devices.

Door Locking Devices

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 a GSA-approved lock that meets federal specifications. Fortunately, the 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, and troubleshooting of equipment failures.

The DOD Lock Program
Designated as the DOD technical authority for locks, safes, vaults, seals, and containers used to protect national security information (NSI) and arms, ammunitions, and explosives (AA&E), the DOD Lock Program is divided into three branches. The DOD Lock Program is divided into three branches:
1. Field Support
2. Research, Development, Testing & Evaluation (RDT&E)
3. Physical Security Equipment (PSE) Testing

Door Locking Devices (cont.)

What locking devices should a SAPF entry door have? The IC Tech Spec for ICD/ICS 705 lists the door's locking criteria.

Student selects the steel door:
The next locks you will encounter frequently are the ones that meet the FF-L-2740 federal specification. Combination locks approved under this specification are used on new and existing GSA-approved security containers, vault doors and pedestrian door deadbolts. You can refer to the DOD Approved Locks Job Aid if you are unsure which lock is required for the application you are inspecting. So, let's start with the pedestrian combination door deadbolt.

FF-L-2890 approved pedestrian door deadbolt devices come with a lock that meets Federal Specification FF-L-2740. These locks are intended for use on pedestrian doors to secure rooms and SAPFs.

SAPF Door Criteria
- Primary entrance doors shall be equipped with the following:
- A GSA-approved pedestrian door deadbolt meeting Federal Specification FF-L-2890
- A combination lock meeting Federal Specification FF-L 2740
- An approved access-control device
- May be equipped with a high-security keyway for use in the event of an access control system failure

DOD Approved Locks Job Aid is linked on this screen.

Door Locking Devices (cont.)

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, or ACS, and guidelines.

Student selects the door locking device:
SAPF access shall be controlled by SAP-indoctrinated personnel or by an 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 you see listed. If a SAPF has a low number of people that require access, the SAO may approve the use of non-automated access control devices.

SAPF Door Criteria
Primary entrance doors shall be equipped with an approved access-control device:
- 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.
- Biometric personal identity verification using unique personal characteristics such as fingerprint, iris scan, palm print.

Door Locking Devices (cont.)

Our doors may be equipped with a high-security keyway for emergency access or in the event of a system failure. These are not required but may be needed in some situations. Well, I think that just about covers the door locking devices. Let's see is there anything else I need to tell you about doors? Oh! I almost forgot to tell you about the hardware.
SAPF Door Criteria
Primary entrance doors shall be equipped with the following:
- A GSA-approved pedestrian door deadbolt meeting Federal Specification FF-L-2890
- A combination lock meeting Federal Specification FF-L 2740
- An approved access-control device

May be equipped with a High-Security keyway for use in the event of an access control system failure.
1. X09 Inside and Outside
2. High-Security Keyway

Door Hardware

For the most part, the hardware that we use on our SAPF perimeter doors look a lot like the hardware on any door. The hinges must have the ability to secure the hinge pins from being removed. Also, every perimeter door must have an automatic door-closer that does not have a hold-open feature.
CDSE

Perimeter Door Hardware Requirements
- Hinge pins that are accessible from outside of the SAPF door shall be modified to prevent

removal of the door (e.g., welded or set screw, etc.).
• All perimeter SAPF doors shall be equipped with an automatic, non-hold door-closer which shall be installed internal to the SAPF, if possible.

Emergency Doors

The construction standards for emergency doors used on SAPFs are similar to any other perimeter doors. However, there are differences in the types of hardware used on emergency doors. Like other perimeter doors, emergency doors must meet the criteria for the type of door you have, wood or steel.

Hinges must have the ability to secure the hinge pins from being removed and the door must have an automatic door-closer that does not have a hold-open feature. 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 and safety codes just like any other perimeter door.

Emergency Door Requirements
• All door type criteria apply
• Accessible door hinge pins shall be modified to prevent removal of the door
• Equipped with an automatic, non-hold door-closer
• SAPF doors and frame assemblies shall meet acoustic requirements
• Complies with applicable building, safety, and accessibility codes and requirements

---

Specific Emergency Door Hardware

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.

Student selects the door:
Emergency exit doors will have no exterior hardware and 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.

Emergency Door Requirements
• Be alarmed 24/7
• Have no exterior hardware
• Must be secured with deadlocking panic hardware on the inside
• Provide a local audible annunciation when opened

Knowledge Check 1
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.
o Astragal strip
o 180-degree peep hole
o Local audible annunciation device
o 24/7 video surveillance

Answer: Astragal strip

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

Answer: No. Emergency exit doors must not have exterior hardware.

Lesson Summary

It's been a busy morning. So far, we discussed the criteria for primary, secondary, and emergency doors. 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 Objectives
? Examine primary and secondary doors
? Check emergency doors

Lesson: Windows, Ducts, and Ventilation

Lesson Introduction

Doors may be one of the easiest points to enter a facility, but they are not the only way to access a SAPF. Windows and ventilation systems can be used to gain unauthorized access to the classified information within. It is our job as SAOs, to mitigate that risk; verifying the construction techniques and materials used to meet the requirements listed in ICD/ICS 705. Keeping with our goal of ensuring you are as prepared as possible to get your facility accredited without too many hiccups, let’s have a look at the criteria for windows and ventilation systems.

Lesson Objectives
• Evaluate window construction
• Inspect ducts and ventilation areas

Windows

When we inspect SAPF windows, we need to refer to the criteria listed in ICD/ICS 705, 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 of the ground or a platform must be protected by security alarms. So, let's say a 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 platform, it would require security alarm protection.

Windows (cont.)

Windows in a SAPF must provide visual and acoustic surveillance protection. We add visual protection to windows by making the window opaque or with the SAOs 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 RF protection to your windows when recommended by the Certified TEMPEST Technical Authority or CTTA.
CDSE

This can be accomplished by applying an RF shielding film to the glass.

The last window requirement we need to discuss is protecting 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.

Vents and Ducts

Now that we are 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 ICD/ICS 705, Chapter 3. 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. Heat, Ventilation, and Air Conditioning or HVAC vents and ducts will also need to meet these criteria but have additional requirements.

Vents and Ducts Criteria
ICD/ICS 705 v1.4, Chapter 3, Section G 7
- All penetrations of perimeter walls shall be kept to a minimum.
- Electrical Utilities should enter the SAPF at a single point.
- All utility (power and signal) distribution on the interior of a perimeter wall treated for acoustics or RF shall be surface mounted, contained in a raceway, or an additional wall shall be constructed using furring strips as stand-off from the existing wall assembly.

Vents and Ducts (cont.)

Let's go up the ladder and open the duct inspection port.

Student selects the ladder.

Vents and Ducts (cont.)

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 that there is no direct sound path through the duct. SAPF walls above the false ceiling must be finished in the same 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 CDSE

---

finished and sealed so gaps or openings are eliminated around the entire duct.

Vent Bars and Grilles

So, 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 six 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 (cont.)

Bars and grilles in the SAPF duct system 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 an SAO and annotated on the Fixed Facility Checklist.

Vent Bars and Grilles (cont.)

Bars, if installed, must have half inch diameter steel that is welded on all sides. The bars must be placed six inches on center and 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 Bars and Grilles (cont.)

Grille material can be purchased commercially and must meet one of the criteria listed here. 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.

Vent Grille Criteria
If grilles are used, they shall be one of the following:
- ¾-inch-mesh, #9 (10-gauge), case-hardened, expanded metal
- Expanded metal diamond mesh, 1-1/2” #10 (1-3/8” by 3” openings, 0.093” thickness, with at least 80% open design) tamperproof
- Welded wire fabric (WWF) 4x4 W2.9xW2.9 (6-gauge smooth steel wire welded vertically and horizontally four inches o.c.)

Knowledge Check 1
To warrant protection from forced entry, the bottom of SAPF windows must be placed _____ from the ground or adjacent platform.
o 14 feet
CDSE

17

---

o 16 feet
o 18 feet
o 20 feet

Answer: 18 feet

Knowledge Check 2
If one dimension of the (duct work) penetration measures less than _____ inches, bars or grilles are not required.
o Six
o Five
o Eight
o Four

Answer: Six

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 ventilation systems to ensure the risk of unauthorized individuals gaining access to classified materials is mitigated.

Lesson Objectives
? Evaluate window construction
? Inspect ducts and ventilation areas

CDSE

18

Lesson: Walls, Ceilings, and Floors

Lesson Introduction

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 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. Have a look at our objectives. So, let's look into the criteria for ceilings, walls, and floors.

Lesson Objectives
• Contrast open and closed storage area construction requirements
• Verify that walls meet acoustical protection standards

SAP Compartmented Area (CA)

Before we get into the specifics of wall construction, you must understand that 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." As you can see from the definition, these areas are used to separate or segregate information, systems, and programs within a single SAPF. 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
- A SAP Compartmented Area is an area, room, or a set of rooms within a SAPF that provides controlled separation between control systems, compartments, sub-compartments, or Controlled Access Programs.
- The SAP Compartmented Area shall be approved by the SAO.
- The SAP Compartmented Area FFC shall be used to request approval.

SAP Compartmented Area (CA) (cont.)

Because a SAPF Compartmented Area 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/electronic access control devices. However, there is no need for a high-security lock like a CDX-09 or a CDX-10, or independent alarms systems.

SAP Compartmented Area (CA) (cont.)

If compartmented information will be displayed on a computer terminal or a group of terminals in an area where everyone is not accessed to the program, you may have to include some or all of the visual protection measures you see here to reduce the ability of "shoulder surfing" or inadvertent viewing of SAP Compartmented information.

If you know during the planning stage that your facility will include several SAP Compartmented Areas, you may be able incorporate walls that provide permanent protection and

---

separation of controlled systems, compartments, sub-compartments, or controlled access programs in the design phase of construction.

SAP Compartmented Area Visual Protection
- Position the computer screen away from doorway/cubicle opening
- Use a polarizing privacy screen
- Use partitions and/or signs
- Existing private offices or rooms may be used but may not be a mandatory requirement

SAP Compartmented Area (CA) (cont.)

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

SAP Compartmented Area Acoustic Protection
All TEMPEST, administrative telephone, and technical surveillance countermeasure (TSCM) requirements for the parent SAPF shall apply to the compartmented area and shall be reciprocally accepted.

When compartmented discussions are required, the following apply:
- Use existing rooms that have been accredited for SAP discussions.
- Use administrative procedures to restrict access to the room during conversations.

SAP Compartmented Area (CA) (cont.)

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

Wall Acoustic Protection Criteria
- Construction of walls as described in IC Tech Spec for ICD/ICS 705, Chapter 3 (Wall types A, B, and C) or with brick, concrete, or other substantive material and acoustically treating penetrations, walls and doors should provide the necessary acoustic protection for Sound group 3.
- When Sound Group 3 or 4 cannot be met with normal construction, incorporate supplemental mitigations to protect classified discussions from being overheard by unauthorized persons.

Closed/Open Storage

Now that we know a SAPF can be divided into compartmented areas, let's talk about how to categorize these areas and the facility. SAP areas can have one of two storage designations: Closed Storage or Open Storage.
CDSE

Closed storage means that users must secure all classified information in a 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. However, all the access controls and visual protections for SAP areas we discussed previously apply.
Closed Storage
The storage of classified information in properly secured General Services Administration (GSA) approved security containers.

When the storage, processing, and use of compartmented information, product, or deliverables is required, and all information shall be stored while not in use, then all of the following shall apply:
- Access and visual controls identified for compartmented areas shall be the standard safeguard.
- Compartmented information shall be physically stored in a GSA approved security container.

Closed/Open Storage (cont.)

In an open storage area or facility, classified information does not need to be stored in a 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 information or documents.

The requirements for an open storage SAP Compartmented Area are not as stringent if located in an open storage SAPF. If the SAPF is accredited as open storage, the SAP Compartmented Area could be a private office or room with the standard access controls we discussed earlier. If accredited as closed storage, the perimeter of the open storage SAP Compartmented Area will need to meet open storage standards. This may require the construction of new walls or doors.

Open Storage
Storage of classified information within an approved facility where securing classified information in GSA-approved storage containers while the facility is not occupied by authorized

personnel is not required.

In rare instances when open storage of information is required, the following apply:
• If the parent SAPF has been built and accredited for closed storage, then the SAPF CA perimeter shall be constructed and accredited to open storage standards.
• 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.
• The SAPF SAO may approve open or closed storage within the SAPF. Storage requirements shall be noted in the Fixed Facility Checklist (FFC) and, if appropriate, in a Memorandum of Understanding (MOU) or CUA.

Closed/Open Storage (cont.)

Because we have different types of storage areas, we have multiple wall types to accommodate the activities within. But before we get into the different wall types, let's gauge your knowledge with a few questions.

Knowledge Check 1

Which methods of access control should be used for a compartmented area (CA) accredited for closed storage? Select the best response.
o Visual recognition or mechanical/electronic access control devices
o Spin-dial combination locks and internal dead bolt
o Independent alarm systems and motion sensors
o The CA Perimeter shall be constructed and accredited to open storage standards

Answer: Visual recognition or mechanical/electronic access control devices

Knowledge Check 2

As a best practice, when would classified information be stored in a GSA approved storage container within an open storage area? Select the best answer.
o When the facility is not occupied by authorized personnel
o When it is maintained in a private office with access control
o Anytime the information is not being actively used, it must be stored properly
o When the open storage area is within a closed storage SAPF

Answer: Anytime the information is not being actively used, it must be stored properly

Perimeter Wall Criteria

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.

There are four types of walls we normally use.

Let's start with perimeter walls. Perimeter walls outline the confines, floors, ceilings, doors, windows and penetrations by ductwork, pipes, and conduit. These walls must meet the standards described within ICS 705-1, for SAPF perimeters, but the general construction criteria are listed here. As you can see, 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. Have a look at the SAPF Wall Type document and keep it open as we explain each wall.
CDSE

22

Student selects SAPF Wall Types hyperlink for access to a printable pdf diagram of Wall Type A and Wall Type B.

Wall Type A

If your SAPF will be closed storage, contain a secure working area or SWA, have continuous operation, or be open storage with SID, then the standard acoustic wall or wall Type A may meet your needs. This wall normally requires three layers of 5/8-inch 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 board on the uncontrolled side.

For SAPF wall construction, we will use 3 5/8-inch 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.

Wall Type A (cont.)

The next layer of sound protection is adding the sound attenuation material. The material needs to be 3 1/2" 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 have to 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 ceiling 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

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. Let's look at a Type B wall or an expanded metal wall. As you can see, all the Type A wall requirements are the same for a Type B wall.

The difference between wall Type A and wall Type B is the addition of a layer of expanded metal mesh on the controlled side under the 2 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 FFC. If spot welding is not an option, the expanded
CDSE

23

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.

Wall Type B Criteria
• Wallboard shall be attached to 3 ?-inch wide 16-gauge metal studs or wooden 2x4 studs placed no less than 16” on center (o.c.)
• Acoustic fill 3 ½” (89mm) sound attenuation material, fastened to prevent sliding down and leaving void at the top
• The top and bottom of each wall shall be sealed with an acoustic sealant where it meets the slab
• Fire safe non-shrink grout or acoustic sealant in all voids above/below track both sides of partition
• Entire wall assembly shall be finished and painted from true floor to true ceiling
• ¾” mesh, #9 (10-guage) expanded metal shall be affixed to the interior side of all SAPF perimeter wall studs

Wall Type C

Jeff: Wall Type C or a plywood wall like wall Type B can be used for an open storage facility or have an open storage area without SID. As you can see, 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 1/2-inch 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.

Keep in mind that if Certified TEMPEST Technical Authorities, or CTTA, recommend a layer of approved Ultra Radiant R-Foil be installed to provide Radio Frequency shielding, the foil shall be placed between the layer of plywood and gypsum wallboard on the controlled side.
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-taping 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. However, there are two features of our facility that we still need to discuss; the floor and the ceiling.

Wall Type C Criteria
• Wallboard shall be attached to 3 ? inch-wide 16-gauge metal studs or wooden 2x4 studs placed no less than 16” on center (o.c.)
• Acoustic fill 3 ½” (89mm) sound attenuation material, fastened to prevent sliding down

and leaving void at the top
• The top and bottom of each wall shall be sealed with an acoustic sealant where it meets the slab
• Fire safe non-shrink grout or acoustic sealant in all voids above/below track both sides of partition
• Entire wall assembly shall be finished and painted from true floor to true ceiling

• Three layers of 5/8 inch-thick GWB: two layers on the uncontrolled side and one-layer GWB over minimum ½” plywood on the controlled side.
• ½” Plywood affixed 8’ vertical by 4’ horizontal to 16-gauge studs using glue and #10 steel tapping screws at 12” o.c.

Floors and Ceilings

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. It wouldn't make sense to build walls that are rated for Sound Group 4 if the ceiling doesn't meet Sound Group 3. As it is with our SAPF walls, floor and ceiling penetrations need to be kept to a minimum.

Knowledge Check 3
Which of the following types of SAPF walls contains only three layers of gypsum wallboard, one layer on the uncontrolled side, and two on the controlled side? Select the best response.
o Wall Type A
o Wall Type B
o Wall Type C
o Perimeter Wall

Answer: Wall Type A

Knowledge Check 4
Which wall type contains three layers of ? inch-thick gypsum wallboard, two layers on the uncontrolled side and one-layer gypsum wallboard on the controlled side of the SAPF? Select the best response.
o Wall Type A
o Wall Type B
o Wall Type C
o Perimeter Wall

Answer: Wall Type C

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 opened and closed storage area requirements and the construction techniques used to build walls that meet acoustical protection standards.
CDSE

Lesson: Intrusion Detection Systems

Lesson Introduction

Let's face it, no matter how strong you make the doors and walls in your 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, or IDS, to alert the security team that someone or something is trying to break in to your SAPF. You are better prepared to ensure your facility gets accredited. But we still have plenty to cover before you are ready. Have a look at our objectives before we dive into the criteria for SAPF Intrusion Detection Systems.

Lesson 5 Objectives

- Recognize system requirements
- Inspect system components

What is IDS?

Before we get too far, let's make sure we know what an IDS is. As the definition states, it is an automated system that detects intrusions. We use these systems to alert us to movement, temperature changes, vibrations, the opening of doors, and breaking windows so we can protect the information within our SAPF from break-ins and theft.

IDS 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 many analysts don't like very much, but it is crucial to have contingency plans in the event of a system failure. Mechanical and electrical components breakdown; 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 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.

System Requirements

Now that we know what an IDS is and what it is supposed to protect, let's talk about the specific system requirements that an IDS must meet. There are system component and installation standards outlined in UL 2050. You will find the Extent 3 requirements for installation. 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.

System Requirements (cont.)

The high-security switches and sensors we use in our IDS must comply with UL standards 634 and 639 respectively. A recent change requires that new SAPF construction use UL Level II high-security switches. In existing facilities, the use of existing UL Level I high-security switches are authorized until major IDS modifications/upgrades are made. On the other side of this wall is our breakroom, which is an unsecured area. Because this is a common wall that could be used to gain access, it must be protected.

System Requirements
- IDS installation-related components and monitoring stations shall comply with Underwriters Laboratories (UL) Standard for National Industrial Security Systems for the Protection of Classified Material, UL 2050.

• Installation shall comply with an Extent 4 installation as referenced in UL 2050.

Areas of a SAPF through which reasonable access could be gained, including walls common to areas not protected at the SAP level, shall be protected by IDS consisting of UL 639 listed High-Security Switches (HSS) that meet UL Level II requirements and/or other SAO-approved equivalent sensors.

System Requirements (cont.)

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 or EMT. If those conduits need to run through a service or pull box, then the box must be secured with a GSA- or SAO-approved lock.

IDE cabling that extends beyond the SAPF perimeter shall employ the following requirements:

• Encrypted Line Security should be installed in a closed and sealed metal conveyance defined as a pipe, tube or the like constructed of ferrous Electrical Metallic Tubing (EMT), ferrous pipe conduit or ferrous rigid sheet metal ducting.

• All joints and connections shall be permanently sealed completely around all surfaces (e.g. welding, epoxy, fusion, etc.). Set screws shall not be used.

• The seal shall provide a continuous bond between the components of the conveyance. If a service or pull box must be utilized, it must be secured with a GSA approved combination padlock or SAO-approved key lock.

System Requirements (cont.)

The IDS must be completely separate from other systems such as fire, smoke, 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 SAO approval. 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.

System 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, premise control units, or PCUs, and integrated IDS with remote terminal access. Let’s start with sensors.

System Components, Sensors (cont.)

Sensors are the eyes and ears of the IDS. Depending on the type of sensor, they can detect movement, sound, temperature changes, 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 ICD/ICS 705 or be approved by the SAO. However, for facilities outside the U.S. and in Category I or 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 premise control unit requirements next.

System Components, Premise Control Unit (PCU)

Before we get into the requirements of a Premise Control Unit, or PCU, let's define what a PCU is. It 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.

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.

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, or CNSS, standards. This one kind of goes along with the first requirement. We want to ensure the PCU is kept safe from prying eyes or casual or unauthorized observers. That's why we placed this one in the alarm room.

The PCU must put out a persistent alarm if any one of the conditions shown here occurs. Finally, any IDS cabling or transmission lines that extend past the SAPF perimeter need to meet National Institute of Standards and Technology FIPS Standards 197 and 140-2. The FIPS standard employed must be noted on the UL 2050/CRZH Certificate or other certificate employed. PCUs certified under UL 1610 must meet FIPS 197 or FIPS 140-2 encryption certification and methods. For PCUs certified under UL 1076, only FIPS 140-2 is the acceptable encryption certification and method. If alternative methods are used, they must be approved by the SAO and noted on the IDS Certificate. Now let's look at the requirements for an Integrated IDS and Remote Terminal Access.

PCU Requirements

- Immediate and continuous alarm annunciations shall occur for the following conditions.
  Intrusion Detection
  Failed Sensor
  Tamper Detection
  Maintenance Mode
  IDE Sensor Points shunted or masked during maintenance mode
- IDS transmission lines leaving the SAPF to the monitoring station, must meet National Institute of Standards and Technology, Federal Information Processing Standards (FIPS) for certified encrypted lines

System Components, Integrated IDS

If your IDS is going to be integrated into a networked system, there are physical and software security requirements that must be met. Let's start with the physical requirements.

The host device needs to be placed in a physically protected space. This is defined as a locked room with walls, floor, and ceiling that are fixed in place forming a solid physical boundary to which only SAP-cleared personnel have access. The door to that space must use Commercial Grade 1 hardware, high-security key cylinders, and if not manned 24 hours a day, a UL Extent 3

burglar alarm system and access control. If remotely programmable components are included in the IDS, continuous network monitoring is required. This includes auditing and reporting of network intrusion detection and prevention systems.

System Components, Integrated IDS (cont.)

Now let's look at the software requirements for an integrated IDS. As with the IDS wiring, the IDS components and equipment need to be segregated from the rest of the network by using CDSE

---

features that are configured to allow secure and private data transfers only between the PCU, host computer, remote terminal and monitoring station. A secondary communications path, if utilized, may only be wireless if approved by the SAO in consultation with the CTTA and/or the appropriate technical authority. The passwords need to meet the minimum length and character standard and be changed every six months. A U.S. Government Personal Identity Verification Card or Common Access Card with two factor certificate authentication are acceptable methods of access.

System Components, Remote Terminal Access

Remote terminal access needs to be strictly controlled and limited to a select few. To do that we use role-based user permissions to grant capabilities to a small number of individuals. All U.S. Government installations need to comply with paragraph 7.A.3.c.1 and prohibit non-SCI cleared personnel from modifying the IDS.

The Remote Terminal Access passwords need to meet the same minimum length, character types, and time standards, as we mentioned earlier or utilize U.S. Government Personal Identity Verification Card or Common Access Card with two factor certificate authentication if supported by the application. The host system must record all log in attempts and that information must be documented and accessible to the SAO upon request. Finally, the system must be configured to apply the latest firmware and security updates. It must also comply with Information Assurance Vulnerability Alert guidance.

That was a lot of information to take in. Let’s test your knowledge with a few questions.

Knowledge Check 1
Which UL rating must IDS installations, related components, and monitoring stations comply with? Select the best response.
o UL 2048
o UL 2050
o UL 2639
o UL 2634

Answer: UL 2050

Knowledge Check 2
Which activity or activities are not used when evaluating the risks associated with new technologies? Select all that apply.
? Be dedicated to the system
? Comply with national and local electric codes and CNSS standards
? Be shielded from RF interference
? Be contained within the SAPF

Answer: Be dedicated to the system; Comply with national and local electric codes and CNSS standards; Be contained within the SAPF

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 5 Objectives
? Recognize system requirements
? Inspect system components

Lesson: Telecommunications

Lesson Introduction

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. Before we dive into the criteria for SAPF telecommunications systems, let's review our objectives for this lesson.

Lesson 6 Objectives
- Describe physical and software access controls for unclassified phones
- Evaluate unclassified information systems and cable control

Unclassified Telephones

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 that you are in compliance. The configuration of unclassified telephone systems used in SAPFs need to be baselined and documented in the Fixed Facility Checklist. 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 eavesdrop on our conversations. We must ensure the unclassified telephone systems used in a SAPF are set up 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. We also need to ensure the equipment meets on-hook and off-hook audio protection requirements by verifying it’s listed in one of the three references you see listed. If we discover telephones or instruments not type-accepted, they will be presumed to have on-hook audio available at the monitoring 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 Telephone Requirements
• A baseline configuration of all unclassified telephone systems, devices, features, and software shall be established, documented, and included in the SAPF FFC.
• 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.
• Unclassified telephone systems shall incorporate physical and software access controls to prevent disclosure or manipulation of system programming and data.
CDSE

• On-hook and off-hook audio protection shall be provided by equipment identified by the National Telephone Security Working Group within TSG-6/CNSSI 5006, National Instruction for Approved Telephone Equipment, or an equivalent TSG 2/CNSSI 5002.

Unclassified Information System Requirements

One of the best ways to keep classified or sensitive information safe is by segregating it from the 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 those that maintain the system only.

You may recall that our Intrusion Detection System 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.

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 SAO 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 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

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 Fixed Facility Checklist needs to document if the facility contains any environmental infrastructure 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.

Now that we know the requirements for environmental infrastructure systems you may encounter, let's talk about the emergency notification systems utilized in a SAPF.

Emergency Notification Systems

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, 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 communications system that send 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 communications 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.

The proper use and handling of the SAPF wires and cables can go a long way in keeping our facility and information secure.

Unclassified Cable Control

As we stated previously, the fewer holes you have in a bucket, the easier it is to contain water within it. Well, that philosophy has been applied 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 telecommunications requirements; how about we test some of your new knowledge.

Knowledge Check 1
Which system shall not transmit audio and shall be configured to prevent external control or activation, technical exploitation, or penetration when not in use? Select the best response.
- o CCTV System
- o Unclassified Telephone System
- o Unclassified Information System
- o Emergency Notification System

Answer: Unclassified Telephone System

Knowledge Check 2
Which system, if installed, shall present no technical security hazard to the SAPF? Select the best response.
- o CCTV System
- o Unclassified Telephone System
- o Unclassified Information System
- o Emergency Notification System

Answer: CCTV System

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 these systems secure ensures the information keeps flowing without compromising the data's security.

Lesson 6 Objectives
? Described physical and software access controls for unclassified phones
? Evaluated unclassified information systems and cable control

---

Lesson: Classified Material Destruction Methods

Lesson Introduction

Classified materials, or at least copies of these materials, outlive their usefulness and need to be destroyed versus taking up space in a classified storage container. To accomplish this, we must follow certain destruction methods to ensure these materials are destroyed. We are here to discuss those methods. Before we dive into the criteria for classified material destruction methods, review our objective for this lesson.

Lesson 7 Objective
• Describe authorized methods and equipment used for destruction of classified/sensitive material

Classified Information in Open Storage Areas

Let's talk about the open storage area security and construction requirements first. As we stated previously, in an open storage area, compartmented or classified information doesn't need to be stored in a GSA-approved storage container when the facility isn't physically occupied by authorized personnel. This means the security procedures for these areas are less strict than closed storage areas.

Open storage area entrances 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.

Destruction Equipment Location

For obvious reasons and as a best practice, our destruction equipment must not be placed close to the entry door. Documents and other material identified for destruction shall continue to be protected as appropriate. We can't have someone just reaching in to take classified materials. Some of the equipment used to destroy classified materials can be extremely heavy. So, we need to ensure the floor is reinforced or strong enough to handle the load. This is especially true if your facility has false floors.

Now that we have some of the specific security and construction requirements under our belt, let's move on to the destruction methods and equipment requirements.

Destruction Methods and Equipment

There are many ways to destroy something, but the end goal of destruction is to change the item's form or function to make it unusable. The destruction of classified information has the same goal regardless of the form it's in. There are two classes of information that we need to have the ability to destroy: classified information and classified IT equipment and media.

When we're speaking of classified information destruction methods, we're mostly speaking about

classified paper products. Regardless of method, the goal is to destroy the information in a manner that will prevent reconstruction.

Regardless of the form that the SCI you need to destroy takes, the equipment required to complete the task must be approved by the NSA and listed on their evaluated products list.

Classified Information Destruction Methods
- Burning
- Crosscut shredding
- Wet pulping
- Mutilation
- Chemical decomposition
- Pulverizing/Disintegrating

Destruction Certificates

We need to account for SCI even after the destruction occurs. When was it destroyed and by who? We do this by using destruction certificates.

Classified Information Destruction Methods
- Destruction certificates are required for accountable SAP material.
- Organization must maintain a master record of accountable SAP material and destruction is recorded in the master record.
- Individual destruction certificates may be destroyed after recording in the master record.

Knowledge Check 1
Which of the following are classes of information that a SAPF must have the ability to destroy? Select the best response.
o Classified information and classified IT equipment and media
o Controlled unclassified information and classified information
o For Official Use information and controlled unclassified IT media
o Paper products and video products

Answer: Classified information and classified IT equipment and media

Lesson Summary

When classified materials outlive their usefulness, they can't just be thrown in the trash. We've discussed the destruction methods we must follow to ensure those materials are accounted for and destroyed.

Well, that pretty much covers everything I needed to tell you about SAPF Physical Security Construction Requirements. I think you're ready. Good luck with your facility accreditation.

Lesson Objectives
? Describe authorized methods and equipment used for destruction of classified/sensitive material.

Lesson: Course Conclusion

Course Summary

Congratulations, you have completed the SAPF Physical Security Construction Requirements course. You should now be able to perform the listed activities.

? Recognize DOD guidance and ICS for the construction, accreditation, and inspection of SAPFs.
? Inspect SAPF doors for compliance with DOD physical security criteria.
? Analyze SAPF windows, ducts, ventilation, and view ports for compliance with DOD physical security criteria.
? Verify that SAPF ceilings, walls, and floors 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.
? Evaluate SAPF classified destruction methods for compliance with DOD physical security criteria.

Original Document
SA501-guide.pdf (652.36 KB)