Requirements for SCIF Door Assemblies

By Scott Detienne, RA, CCS, BSCP, CPP, AHC

THIS ARTICLE PROVIDES GENERAL REQUIREments for standard door, frame and hardware components, (door assemblies) and related construction items utilized for SCIF's based on DCID 6/9. It is addressed to architects, engineers, building managers and designers of SCIF facilities and quotes DCID 6/9, which is open for public use and readily available on the Internet.

SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF) AND SENSITIVE CLASSIFIED INFORMATION

SCIF is a "Sensitive Compartmented Information Facility" which is an accredited area where sensitive classified information (SCI) may be handled, stored, used, discussed, and/or processed. S. C. I. is "Sensitive Classified Information" which is required to be handled within SCIFs meeting the requirements of the DCID 6/9.

DCID 6/9

DCID 6/9 is the "Physical Security Standards for Sensitive Compartmented Information Facilities" Manual, as approved by the Director of Central Intelligence (DCI). The current edition is dated 18 November 2002. DCID 6/9 consists of basic requirements and supplemental "annex" requirements. Other SCIF manuals prepared by other military or governmental organizations are available, but most are not open for general public use without a "need to know". Those manuals are not addressed in this Article.

COGNIZANT SECURITY AUTHORITY AND SENIOR OFFICIAL OF THE INTELLIGENCE COMMUNITY

The SOIC is the head of an agency, bureau, or intelligence element identified in Executive Order 12333. The SOIC will accredit the SCIF according to the DCID 6/9 standard checklist and additional security needs based on SOIC, military or other government generated threat assessment requirements specific to the SCIF. All SCIF's must be accredited by the SOIC prior to conducting any SCI activities.

The Cognizant Security Authority (CSA) is the single principal designated by the Senior Official of the Intelligence Community (SOIC) to serve as the official who is responsible for all aspects of the SCIF security program management with respect to the protection of intelligence sources and methods under SOIC responsibility. The CSA is typically a senior member of the organization that owns the SCIF.

BASIC SCIF REQUIREMENTS PER DCID 6/9

The four basic SCIF Requirements per DCID 6/9, for a "Closed Storage" Classification, and within the USA, are as follows:

- "Permanent Dry Wall Construction", as defined in "General Construction Requirements" below.
- The SCIF must be alarmed with an electronic intrusion detection system (IDS).
- SCI must be stored in General Service Administration (GSA) approved security containers for "Closed Storage Classifications".
- There must be a response force capable of responding to an alarm within 15 minutes after annunciation and a reserve response force available to assist the responding force.

GENERAL CONSTRUCTION REQUIREMENTS PER DCID 6/9 AND RECOMMENDATIONS

The general construction requirements for a SCIF per DCID 6/9, with emphasis on door assemblies, are quoted. DCID 6/9 requirements are often performance based without offering specifics. Therefore, my schematic level recommendations are also indicated.

- "The SCIF perimeter walls, floors and ceiling, must be permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, to include above the false ceiling and below raised floor, must be done in such a manor as to provide visual evidence of unauthorized penetration." (Section 3.3.1 of DCID 6/9).
- SCIF walls are typically recommended to consist of the following minimum requirements:
  1. Walls are full height "drywall" partitions, secured to the structural concrete floor slab assembly and structural concrete ceiling slab assembly. The walls consist of metal studs and gypsum board panels.
  2. The metal studs are standard 3-5/8-inch deep, 20-gauge, studs spaced 16-inches on-center, with bottom runner and slip-type header runner. The studs are recommended to comply with ASTM C 645 and have G40 (Z120), hot-dip galvanized zinc coated finish.
  3. The wall panels are two layers of ½-inch thick or 5/8-inch thick standard gypsum board secured on the outside of the metal studs and one layer of ½-inch or 5/8-inch thick standard gypsum board secured on the SCIF side of the metal studs. The wall panels comply with ASTM C 36C or 36M and ASTM C 1396C or 1396M, and include standard trim accessories, joint treatment materials and standard steel drill screws complying with ASTM C 954. Installation should match standard building specification for typical double layered gypsum board applications. Finishes may include paint or vinyl wall coverings matching typical standard building finishes and should meet local fire code requirements for Class A materials.

ENTRANCE, EXIT, AND ACCESS DOOR REQUIREMENTS

- "Primary entrance doors into SCIFs shall be limited to one. If circumstances require more than one entrance, this must be approved by the CSA. In cases where local fire regulations are more stringent, they will be complied with. All perimeter SCIF doors must be closed when not in use, with the exception of emergency circumstances." (3.3.3.1)
- "All SCIF primary entrance doors must be equipped with an automatic door closer, a GSA-approved combination lock and an access control device" (3.3.3.3).The "X-09" combination dead bolt lock, as manufactured by Kaba-Mas, is currently the only GSA approved combination dead bolt lock available. This lock meets GSA requirements for compliance with Federal Specification FF-L-2740A, dated 1/12/97.
- "Solid wood core door, a minimum of 1-3/4 inches thick or, 16-gauge metal cladding over wood, a minimum of 1-3/4 inches thick or, metal fire or acoustical protection doors, a minimum of 1-3/4 inches thick required." (3.3.3.6)
- "Specifications of doors, combination locks, access control devices and other related hardware may be obtained from the CSA" (3.3.3.6)
- SCIF doors are recommended to be 3-foot wide, single, swing, flush face doors. These doors should be without louvers, unusual undercuts, vision lights, transoms or side lights. Door pairs and exterior door assemblies should also be avoided.
- SCIF door assembly STC ratings are not established but are recommended to match adjoining wall STC ratings. In addition, appropriate UL sound-rated gasketing, including UL sound-rated threshold and/or automatic door bottoms are recommended.
- SCIF door assemblies are recommended to match the general building door and frame style, size, appearance, color and finish to the extent possible. This includes paint finishes as well as wood door species, grain and stain.
- SCIF door frames are recommended to be standard 2-inch wide metal frames, fully welded type (in lieu of knocked-down type), and installed prior to stud installation. The abutting studs are recommended to be anchored to the door frames. Frame styles can include all readily available welded types such as wrap-around (masonry or drywall) to masonry abutting frames for existing masonry conditions.
- SCIF door frames are recommended to be grout filled, even at stud walls, and the lockset or electric strike should include a strike "mortar guard" that is installed on the back side of the frame to prevent grout spilling out the strike opening. In addition, jamb supporting studs are recommended to be doubled and horizontally braced with 16-gauge metal plates or metal studs, to adjacent studs to prevent "pry-open" opportunities. Grout fill of the frames also improves sound isolation. Grout fill may require a special consideration to field drill a ¾-inch hole at the top of the jamb to allow grout injection, followed by a cap secured over the hole. This

requirement should be coordinated with the frame manufacturer.

- SCIF doors may be out-swing or in-swing. Out-swing doors (a.k.a.; "reverse" swing doors that swing in the direction of the public corridor or key side, and also known as "seated pressure" doors) typically provide better forced entry and blast resistance given the continuous door frame stop. In fact, door assemblies required to offer the highest levels of forced entry protection, such as "Miami-Dade County" hurricane resistance door assemblies and blast resistance door assemblies, typically are out-swing doors that rely on the frame stop to obtain additional strength from outside generated pressures or forces. Out-swing doors must be equipped with hinges that have non-removable pins (NRP) although hinge studs are not uncommon. Out-swing doors should also have "latch guard plates" to prevent manipulation of the door latch at the strike. In-swing doors, however, are probably utilized more than out-swing doors for access to SCIF's, offer "more than adequate" overall protection, do not have strike or electric strike manipulation opportunities and may be required for code reasons, such as to prevent out-swing door interference or encroachment into the adjoining corridor. However, most building codes require doors to be out-swinging (swing in the direction of the means of egress) if the room that the door serves has an occupancy load greater than 50 people.
- SCIF doors are recommended to be meet ANSI/SDI A250.8 for level and model and ANSI/SDI A250.4 for physical performance level, be at least Level 2 and Physical Performance Level B (Heavy Duty), full flush or seamless, with the door manufacturer's standard core construction. Frames are recommended to be at least 0.053-inch thick, full profile welded, with stud-wall type anchors.
- SCIF door assembly hardware is recommended to meet Builders Hardware Manufacturer's Association (BHMA) Grade 1 requirements. In general, the door hardware should match the general building hardware to the extent practical. This includes butt-hinge style, closer type and style, door signage, stops, lock set lever style and trim style. Generally, stainless steel or coated steel is the recommended surface finish and base material.
- SCIF doors are recommended to have lever locksets with "store-room function". This set has inside and outside lever handles. The outside lever handle is always locked and requires a key from the outside to allow entry. Removal of the key reverts the outside lever to the locked position. The inside lever always allows free existing. This lockset works with the card reader and electric strike system in that the card reader retracts the electronic strike and only requires pushing (or pulling) the locked lever to open the door. The levers should also meet ADA-AG accessibility configuration requirements.
- SCIF doors are recommended to have closers and stops. Closers should have functions meeting ADA-AG accessibility force-to-open requirements and should be installed on the protected side. Closers should not be equipped with hold open devices. In addition, the door stop should be simple floor or wall bumpers and not be equipped with hold open devices. Overhead stops should be avoided, but if provided, must be coordinated with the closer to ensure proper operation. They should also not have hold open devices.
- SCIF door locksets are recommended to have removable lock cylinders for quick change of the cylinder, should the integrity of the cylinder be in question. The government's personnel (not the contractor's) are recommended to obtain lock cylinders directly from the manufacturer and install these cylinders. High security cylinders are also possible, but standard cylinders are common on SCIF doors as the overall locking strategy relies on the dead bolt.
- SCIF lockset cylinders are recommended to have unique "change keys." Keying is NOT recommended to be part of the building's overall master key system. In addition, keys should indicated "DO NOT DUPLICATE," be numbered and only assigned to designated officials.
- SCIF door sequence of operation is recommended as follows
  1. Activation of the X-09 combination deadbolt.
  2. Activation of the card reader, which electronically deactivates (opens) the electric strike and "shunts" (turns off) the door contact (aka: balanced magnetic switch).
  3. Push (or pull) of the locked lever, without use of the key.
  4. Entry is also possible by activation of the combination deadbolt and use of the lockset key without activation of the card reader, but this

should cause an alarm. Entry without activation of the card reader should cause activation of the door contact and signals an alarm.

5. Exiting requires turn of the "thumb turn" on the inside face of the X-09 combination deadbolt and turning the lever. The electric strike remains in the locked position and the lockset allows "free existing."

INTRUSION DETECTION SYSTEMS

- "The CSA shall approve IDS proposals and plans prior to installation within a SCIF. IDS consist of four phases; detection phase, reporting phase, assessment phase, response phase. IDS shall detect unauthorized human entry into the SCIF. Motion detection sensor shall be provided in the SCIF. Door contacts are recommended to be part of the IDS. The PCU ("panel control unit" or arm/disarm panel) shall be inside SCIF. Stringent cabling and host computer are required. IDS must comply with UL Standard 2050." (3.1.6)
- "IDS shall be connected to emergency power." (19.0)

ACOUSTICAL CONTROL AND SOUND MASKING

- "The current edition of Architectural Graphic Standards (AGS) describes various types of sound control, isolation requirements and office planning. The AGS establishes Sound Groups 1 through 4, of which Groups 3 and 4 are considered adequate for specific acoustical security requirements of SCIF construction." (Annex—E 1.2)
- "All SCIF perimeter walls shall meet Sound Group 3 unless additional protection is required of amplified sound." (Annex E—2.1)
- "Sound Group 3—STC of 45 or better. Loud speech can be heard, but is hardly intelligible. Normal speech is unintelligible." (Annex E—1.2.3)
- "If compartmentation is required within a SCIF, the dividing walls must meet "Sound Group 3" (STC sound rating of 45 or better)." (Annex E—2.2)
- "When normal construction and baffling measures have been determined to be inadequate for meeting Sound Group 3 or 4, as appropriate, sound masking shall be employed." (Annex E—3.1)
- "To be effective, the masking device must produce sound at a higher volume on the exterior of the SCIF than the voice conversation within the SCIF. Speakers should be placed close to or mounted on any path which would allow audio to leave the area. Sound masking devices placed on exterior of SCIF." (Annex E—4.0)
- "The introduction of electronic systems that have components outside the SCIF should be avoided. Speakers or other transducers, which are part of a system that is not wholly contained in the SCIF, are sometimes required to be in the SCIF by safety or fire regulations. In such instances, the system can be introduced if protected as follows: All incoming wiring shall breach the SCIF perimeter at one point. TEMPEST or TSCM concerns may require electronic isolation. In systems that require notification only, the system shall have electronic isolation. In systems that require two-way communication, the system shall have electronic isolation. SCIF occupants should be alerted when the system is activated. All electronic isolation components shall be installed within the SCIF as near to the point of SCIF egress as possible." (Annex E—7.0)

PERSONNEL ACCESS CONTROL

- "All SCIF's shall have personnel access control systems. SCIF entrances must be under visual control OR have automatic access control system. Visual control consists of employees or guards. CCTV systems acceptable if continually monitored, or automated access control system consists of ID cards and card reader access may be used in lieu of visual controls." (Annex F - 1.0)
- "Automated personnel access control system shall authenticate an individual's authorization to enter the SCIF" (Annex F—2.2)
- "Transmission line protection required. (electronic integral line signal supervision as part of the card reader system)" (Annex F—2.5)
- "Electric strikes installed for use in personnel access control systems shall be heavy-duty industrial grade." (Annex F—2.6)
- "Locations where authorized data, card encoded data, and personnel identification or verification data is input, stored, or recoded must be protected within a SCIF or an alarmed area controlled at the SECRET level." (Annex F—2.7).
- "Card readers, keypads, communication, or interface devices located outside the entrance to the SCIF, shall have tamper resistant enclosures and be securely fastened to a wall or other structure." (Annex F- 2.8)

generally engineered to specific threat needs and is beyond the scope of this article.

- The SCIF walls may require EMP (electromagnetic protection), HEMP (high altitude electromagnetic pulse), RF (radio frequency) or TEMPEST (Transient Electromagnetic Pulse Surveillance Technology) protection. TEMPEST Shielding refers to the specific shielding that prevents the emanation of unintentional intelligence-bearing signals that if intercepted and analyzed outside the SCIF, may disclose classified information, and prevents outside signals that could damage electronic components inside the SCIF. Protection requires steel, lead, aluminum, copper or copper fabric shielding. Generally, protection to address specific EMP, HEMP, RF or TEMPEST threats requires specialty engineers.
- The SCIF walls may require additional fire and life safety protection. For example, an auditorium use group may need one or two hour fire separation from the remainder of building and may require unique fire exit device door hardware.
- The SCIF floors may need special recess to accommodate TEMPEST shielding and recessed TEMPEST door frame and threshold details.

ADDITIONAL SOUND ATTENUATION REQUIREMENTS

- The SCIF walls may utilize unconventional sound attenuation components. For example, several gypsum board manufacturers have developed improved sound-rated wall systems that utilize sound-absorbing gypsum board or cement boards (typically used for tile backing board). Providing several different gypsum board thicknesses or mixing the types of panel materials improves overall sound ratings. In addition, the cement board offers additional hardened wall protection.

ADDITIONAL ENTRANCE, EXIT, AND ACCESS DOOR REQUIREMENTS

- An entry vestibule, consisting of one door between the public corridor and vestibule and a second door between the vestibule and the SCIF, may be required. This "man-trap" system may utilize interconnected electronic entry door hardware that prevents "piggy back" entry or access card "pass back" entry. One door within the vestibule cannot be opened until the other door is latched shut.
- The SCIF door assembly may require additional "forced entry" protection. Forced entry attacks relate to burglaries and civil disturbance threats. HP White Specification 02: TP-05000.02, dated September, 1993, indicates five levels of force entry protection against various types of attacks. Attacks include blunt impact (hammers), sharp impact (chisels), thermal stress (torches), and chemical deterioration (solvents). The levels of protection relate to either the number of impacts a forced entry protected assembly will withstand or the time, in minutes, required to bypass a forced entry protected assembly with the use of torches or chemical agents. Level I offer the least amount of resistance protection; Level V offers the most amount of resistance protection. Levels of protection are measured in terms of resistance time; 5-minutes, 15-minutes and 60-minutes. Typically, a 5-minute or 15-minute forced entry resistant door assembly is recommended for office environments. Higher levels should be considered if the door assembly presents unusual vulnerabilities. The surrounding walls that abut the door assembly should also receive the same level of protection, and should be strengthened to support the additional door assembly loading. In addition, the hardware, including the hinges and latches, must offer the same level of resistance. Often, manufacturers provide a complete door assembly, including the hardware that has been tested and certified to offer various levels of forced entry protection.
- The SCIF door assembly may require additional ballistic protection, particularly doors that offer protection to personnel of critical positions. UL 752 "Standards for Bullet Resisting Equipment" defines requirements for protection against penetration, passage of fragments and spalling or fragmentation of the protective materials. Bullet resistant levels range from Level 1 (lowest level of protection) to Level 8 (highest level of protection). Level 3 offers protection against three shots from a high powered handgun, while Level 4—protected door assemblies offer protection against commercially available rifles. Typically, a Level 3 bullet resistant door assembly is recommended for office environments. Higher levels should be considered if the door assembly presents unusual vulnerabilities. NIJ 0801.01 offers similar ranges of bullet resistance levels. The surrounding walls that abut the door assembly should also receive the same level of protection, and should be strengthened to support the additional door assembly

loading. In addition, the hardware, including the hinges and latches, must offer the same level of ballistic resistance. Often, manufacturers provide a complete door assembly, including the hardware that has been tested and certified to offer various levels of ballistic protection.

- The SCIF door assembly may require additional "pressure resistant" protection to resist environmental or blast events. Environmental-resistant doors (i.e., hurricane-resistant doors) should be considered for exposed exterior conditions; however, every effort should be made to prevent extreme environmental exposures on a SCIF door assembly. Blast protection categories, ranging from Class A (lowest level of protection) to Class D (highest level of protection), as well as blast resistance, ranging from low range (1 PSI) to high range (12 PSI) or special military applications, should be considered. Considerations should include definition of overpressure, duration, maximum allowable deflection, rebound requirements single or multiple incidents, resistance to penetrations, etc. Typically, Class A blast resistant door assemblies offer adequate protection for typical interior office environments. Higher levels should be considered if the door assembly presents unusual vulnerabilities. The surrounding walls that abut the door assembly should receive the same level of protection, and should be strengthened to support the additional door assembly loading. In addition, the hardware, including the hinges and latches, must offer the same level of pressure resistance. Often, manufacturers provide a complete assembly, including the hardware that has been tested and certified to offer various levels and ranges of blast protection.
- The SCIF door assembly may require EMP, HEMP, TEMPEST or RF shielding. These types of doors are highly specialized and should be part of a vestibule system with the RF shielded door separating the vestibule from the SCIF and the typical SCIF door separating the vestibule from the public corridor.
  1. The typical minimum attenuation versus frequency characteristics for an RF Shielded doors are as follows: [NOTE ** Retain the following for NMR/MRI Nuclear Magnetic Resonance/ Magnetic Resonance Imagery facilities.]
     a. Magnetic Field Attenuation: 90 dB at 200 MHz.
     b. Electric Field Attenuation: 100 dB from 10 MHz through 50 MHz.
     c. Plane Wave Attenuation: 100 dB from 50 MHz through 1 GHz.
  2. The typical references design standards are as follows:
     a. MIL-E-4957A—Enclosure for Electromagnetic Shielding, Demountable, Prefabricated for Electronic Test Purposes.
     b. MIL-STD-220A—Method of Insertion Loss for Radio Frequency Filters.
     c. MIL-STD-285—Method of Attenuation Measurements for Electromagnetic Shielding Enclosures for Electronic Test Purposes.
     d. NSA 65-6—National Security Agency Specification for RF Shielded Enclosures for Communication Equipment.
     e. NSA 73-2A—National Security Agency Specification for RF Shielding of Large Architectural Areas.
     f. IEEE-STD-299.
  3. The typical RF Shielded Door Assemblies are constructed as follows:
     a. Door: Custom metal reinforced, nominal 1-inch thick, by 3-feet wide by 7-feet tall, with plywood core construction and integral ¼-inch thick RF stainless steel shielding.
     b. Frame: Stainless steel frame, ¼-inch thick, fully welded, with single knife door and frame mated construction.
     c. Single Knife Door and Frame Mated Construction: Heavy-duty metal door fingerstock mating components, 1/8-inch thick. Clip-in-place beryllium copper fingerstock around the perimeter of receiver with a removal channel for easy replacement. Provide fingerstock and mating components on all four sides of door (jambs, head and sill).
     d. Thresholds: Typically match the jambs, need to be recessed and have heights that do NOT meet ADA-AG compliance, due to their unique mating requirements with the door edge.
     e. Sign: Provide two precautionary professionally printed, plastic signs, with 1-inch tall red letters on white background, indicating "DO NOT ALLOW WEIGHT EXCEEDING 250 POUNDS ON THRESHOLD," and mounted on both sides of the door.

f. Door and Frame 4Finish: Shop prime finish suitable for field painting.
g. Door and Frame Weight: Nominal 650-pound door assembly.
h. Cam Latch Set: Passage heavy duty, aluminum cam latch set that allows free entry or exiting without keys. Provide custom handle that activates two or three point cam latch. Provide plastic ball at end of handle. Provide cam roller and cam block. Provide clear anodized aluminum finish.
i. Operation: Door is latched and unlatched using a simple bar handle on either side of the door leaf. This action raises and lowers an external double cam roller assembly, engaging or freeing the knife edge.
j. Hinges: Three, extra-heavy duty, adjustable, ball bearing, swing-clear, aluminum, surface mounted, type hinges made of non-ferrous metal. Provide clear anodized aluminum finish.
k. Floor Stop: BHMA Grade 1, stainless steel, wall mounted with anchors that do not pass thru copper shielding.
l. Door Assembly Preparation: Prepare door assembly in RF Shielding Manufacturer's shop and deliver completed door assembly ready for installation. Prepare door and frame to accept all hardware components and meet specified requirements.
m. Coordination of the Door Shielding and Overall Grounding: Careful detailing is required to insure the door assembly is properly grounded and that contact between the door assembly and RF shielding does not come in contact with metal studs, metal mesh or other metal components that may interfere or disrupt the planned grounding of the RF shielding.
n. Fire Rating: Due to the size, weight and configuration of a RF shielded door assembly, it is unlikely that it can achieve a fire rating and meet NFPA 101 and 80 requirements to be 'self-latching and self-closing'. This further justifies the need for a vestibule arrangement with the out door planned as the fire rated door assembly.
o. Gasketing: Careful consideration is required to select perimeter gasketing materials that maintain grounding between the door, frame, abutting wall and the grounding source. These gaskets are typically made of aluminum, copper, monel (nickel-copper alloy) or stainless steel, combined with silicone coatings.
p. ADA-AG Compliance: The force to open typical RF shielded doors, the force to turn the door bar handle and the threshold heights, typically do not meet ADA-AG requirements. If ADA compliance is mandatory for SCIF, special engineering considerations, as well as coordination of manufacturer's capabilities, is required to modify these components.
q. Abutting Walls: The surrounding walls that abut the door assembly should receive the same level of protection, and should be strengthened to support the additional door assembly loading. Deddd

- The SCIF door assembly may require additional door hardware including an aiphones system (an audio and visual CCTV intercom system that allows insiders to view requested entries), a door viewer (peep-hole), door bell system, protection plates (kick plates or plates tailored to cart movement), extra-heavy hardware, lead-lined hardware, and other special components.
- Aiphones present unusual concerns for RF shielded doors which include the following:
  1. An Aiphone is considered a telephone device and therefore may not be allowed within the SCIF.
  2. An Aiphone is a "transmitting" device that could be manipulated for devious purposes.
  3. The Aiphone should receive cabling filtering acceptable to the CSA, Aiphone manufacturer, and SCIF Shielding manufacturer.
  4. The Aiphone should be place on the outer-most vestibule door and not the door between the vestibule and the SCIF.
  5. A simple door wide-angle peephole should be considered for the vestibule door and maybe even the SCIF door, in lieu of an Aiphone. If used for the SCIF door, the SCIF shielding manufacturer must be consulted to verify the peephole assembly does not violate the RF shielding capabilities.
  6. A simple door bell system, acceptable to the CSA, and placed outside the vestibule door with a bell in the vestibule that can be heard within the SCIF, should also be considered.

7. Alternative protocols can be developed for individuals entering or leaving the SCIF. For example, one protocol may indicate that only authorized individuals may enter the SCIF. These individual may act as escorts to ensure authorized entries, proper passage of equipment and supplies, and limit "piggy back" entries.
8. The SCIF doors may be observed with outside CCTV systems and alarm devices,

- The SCIF door assembly may require code compliant fire resistance ratings, and possibly smoke protection.
- The SCIF door assembly may require GSA approved Vault Doors classification.
- The SCIF door assembly may occur in situations where corrosive compounds, salty environments, or hygienic issues are a concern. If so, a stainless steel door assembly should be considered; however, every effort should be made to prevent these exposures.
- The SICF door assembly may occur in situations where thermal extremes of cold and heat are a concern. If so, a thermal door assembly should be considered; however, every effort should be made to prevent these exposures.
- Electromagnetic locks may be required, however, electromagnetic locks are NOT recommended due to the code requirement to interface the lock with the fire alarm system in a manor that required the lock to "fail-safe" (fail in the unlocked position) with fire alarm activation or loss of electrical power. Both vulnerabilities offer simple and tempting methods to gain unauthorized entry into the SCIF.
- A card-to-exit system may be required. The card-to-exit system utilizes a second card reader on the inside door face. An individual utilizes the card on the card-to-exit reader for an "authorized" exit. A card-to-exit system provides additional audit trail information, such as recording "who left when". It must be understood that current code requirements do not allow card-to-exit systems to deny "free entry". The card-to-exit system is "voluntary", but may be interfaced with an alarm system to indicate that an individual has conducted an "unauthorized" exit and left the room without utilizing the card-to-exit system. In addition, this system may also be tied into a CCTV camera that records an individual leaving the room without use of the card-to-exit system (by interface with the door contact).

ADDITIONAL INTRUSION DETECTION SYSTEMS

- Stringent cabling and host computer requirement may be required.
- "Code Red" strobe light systems may be required.
- The IDS might be deactivated with the card reader to allow bypass of the PCU once in the SCIF. This point however may not be allowed by the CSA.
- Alarms might be silent (without notifying the entering person that they activated the IDS system). This point however may not be allowed by the CSA.
- The door contact might be connected to the IDS system, in lieu of a separate stand alone electronic security system. This point however may not be allowed by the CSA.

ADDITIONAL PERSONNEL ACCESS CONTROL

- The card reader system may be required to provide an audit trail for individuals entering and exiting the SCIF. This audit trail may be used in lieu of hard-copy, hand written sign-in sheets as required for typical SCIF protocols. The audit trail is typically a function of the software of the computer system dedicated to the electronic entry control.
- The security room requirements, including requirements of the head-end equipment, integration of the access control system with the intrusion detection system, CCTV requirements, and other electronic security requirements requires careful consideration form the CSA.

In conclusion, this article offers typical construction recommendations for SCFI door assemblies. This article does not address all building issues identified in the DCID 6/9, and does not address related protocol issues, such as personnel controls and inspections procedures. In summary, the CSA and SOIC must be active participants with all SCIF directions and design decisions.

About the Author: *Scott Detienne, RA, CPP, CCS, BSCP, AHC, is a senior project architect with the URS Corporation and has been involved in renovation, rehabilitation and design issues for government facilities, with focus on security integration and building hardware upgrades, for the past 25 years. He can be contacted at Scott_Detienne@URSCorp.com.*