

HEALTH FACILITIES ADVISORY COMMITTEE (HFAC)
MEETING MINUTES

July 17, 2008, 12:00 P.M. (Eastern Time)

Roll Call:

Chairman: Mr. Tommy Bowman X

Vice-Chairman: CAPT Keith Shortall X

Members: CAPT Jose Cuzme () CAPT Dale Mossefin X
Mr. James Biasco X CDR Brian Hroch X
Mr. Ken Harper X CDR Mat Martinson X

Alternates: Mr. Kevin D'Amanda, CAPT Rick Wermers,
CAPT Michael Weaver, and Mr. Howard Wellspring

Guests: Mr. Joe Bermes and CDR Michael Young

Quorum Requirement per Technical Handbook Chapter 4-1: "A quorum consists of at least 50 percent of the HFAC voting membership. A person attending as sit-in representative of another member shall not be counted in determining the quorum requirement and cannot vote."

A moment of silence to remember CAPT Gary Gefroh was held. CDR Hroch stated an article featuring CAPT Gefroh will be published in the August issue of the Commissioned Officer Association's "Frontline" newsletter. This is available at <http://www.coausphs.org/members/membersdocs/frontline/Frontline0808.pdf>.

Approval of the previous meeting minutes: Brian motioned to approve meeting minutes of April 17, 2008, without revision. James seconded motion. **Motion passed without objection.** (Atch. 1)

Old Business:

- Technical Handbook Chapter 21-15 Security. (Atch. 2)
 - Michael W. suggested review of chapter paragraph-by-paragraph with the person making the comment to explain rationale for the comment. The committee agreed.
 - After much discussion as to the intended readership audience and the information this chapter was to communicate, Ken suggested to abandoned the current proposed draft and return to the original proposed chapter draft. James agreed and suggested the deletion of Appendix A – Facility Security Table.

- James and Howard suggested that FEMA 426 “Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings” be added to the proposed original chapter draft. Table 1-7: Selected Extracts – Recommended Standards Chart in FEMA 426 would replace the deleted Appendix A referenced above. A statement would be included in Chapter 21-15 to emphasize that the requirements in FEMA 426 (i.e., Table 1-7) are the minimum standards and if a higher standard is required, then it will be stated in the POR.
 - Michael W. volunteered to re-edit the original proposed chapter draft by deleting Appendix A and adding reference to FEMA 426.
 - Brian requested a link to FEMA 426. Michael W. agreed to send it to him.
 - Keith asked if security guidance will be written for existing facilities. Michael replied that Chapter 21-15 applies only to new construction. James suggested that the Area consult with their local security manager for guidance on existing facilities.
- International Property Maintenance Code (IPMC) Task Force (TF) Report (Atch. 3)
 - James stated he will take the issue of property maintenance back to the Facility Managers because the TF recommended not to adopt the IPMC or parts of it. Mat expressed concerns that several portions of the IPMC were not applicable to IHS facilities.
 - James volunteered to draft a new chapter regarding property maintenance.
 - Kevin and Ken debated the difference between “guidance” and “code” and the manner of enforcing each.
 - Mat suggested to James to draft the new chapter with the minimum standards required.
 - James re-stated he will take the TF’s recommendation back to the Facility Managers.
 - Ken suggested that Kevin should write the new property maintenance chapter and forward it to the Facility Managers for comment before bringing it to the HFAC.
 - Tommy asked if there was a motion to accept the TF’s recommendation. James motioned to accept the TF’s recommendation; Dale seconded this motion. Tommy asked if there were any dissenting vote. There were none; therefore, **motion was approved**. The following is quoted from the TF’s conclusion paragraph that clarifies the above motion:

“The need to provide standardized maintenance practices across IHS is justified; however the challenge lies with implementation. While the PMC contains some noteworthy items, the document as a whole does not fully meet the IHS’ needs. Therefore, it is recommended that IHS provide guidance to Area Offices and Service Units by way of a new chapter in the OEHE Technical Handbook.”

New Business:

- Mat announced that CAPT Rick Wermers is his alternate. Michael W. informed the committee that Michael Y. had updated the HFAC membership webpage except for Brian's alternate. Brian stated that CDR David McMahon, who will report in October 1 as the Institutional Environmental Health Program Manager, will be his alternate.
- Discuss Technical Handbook Chapter 4-1 HFAC. (Atch. 4)
 - Ken informed the committee that some proposed Technical Handbook chapters have by-passed the HFAC for approval which is not in accordance with the current Chapter 4-1. Therefore, Ken suggested that Chapter 4-1 needs to be modified to identify the chapters or type of information that does not need HFAC approval.
 - James explained that most of the proposed chapters that by-passed the HFAC were a matter of policy rather than of a technical nature (i.e., reality).
 - Mat suggested that Technical Handbook Chapter 2-1 Technical Handbook Implementation may require editing.
 - James and Mat volunteered to draft revision to Chapter 4-1 to identify chapters that do not require HFAC approval
- Michael W. added another new business agenda item – status of technical handbook updates.
 - Chapter 24-2 Applicability of Codes, Construction Codes, and Standards has been posted.
 - Chapter 21-5 Electrical Guidelines, Lee Robison to review and post.
 - Chapter 21-15 Security, discussed above.
 - Chapter 21-4.10 Pharmacy Environmental. Lee Robison returned for review of his edits (per post-meeting e-mail from James).
 - Added Chapters 2-1 and 4-1 per above discussion.

Action Items:

- Michael W. will re-edit the original proposed chapter draft by deleting Appendix A and adding reference to FEMA 426. He will distribute draft no later than July 18.
- Kevin will draft a new chapter in the OEHE Technical Handbook to provide guidance to the Area Offices and Service Units regarding standardized maintenance practices for IHS. This draft will be forward it to the Facility Managers for comment before bringing it to the HFAC. Draft is due by mid-August.
- James and Mat will draft revision to Chapters 2-1 and 4-1 to identify chapters that do not require HFAC approval. Drafts are due by mid-September.

Next Meeting: October 9, 2008 at 12:00 p.m. (Eastern Time)

Adjournment: Mat motioned to adjourn; Keith seconded motion. **Motion passed without dissent.**

Attachments:

ATTACHMENT 1 Link to Approved April Meeting Minutes

ATTACHMENT 2 Draft Technical Handbook Chapter 21-15 – Security Level

ATTACHMENT 3 Task Force Report on the International Property Maintenance Code

ATTACHMENT 4 Technical Handbook Chapter 4-1 – Health Facility Advisory
Committee

ATTACHMENT 1 [Link to Approved April Meeting Minutes](#)

ATTACHMENT 2 Draft Technical Handbook Chapter 21-15 – Security Level

CHAPTER 21-15 – SECURITY LEVEL SELECTION FOR USE IN THE DESIGN OF NEW FEDERAL FACILITIES

21-15.1 INTRODUCTION.....Error! Bookmark not defined.
 21-15.2 GUIDELINES.....Error! Bookmark not defined.
 21-15.3 REFERENCE STANDARDS.....Error! Bookmark not defined.
 21-15A Appendix A. Facility Security Standards..... x

Comment [BEH1]: Greg Heck “There appears to be several gaps as they relate to healthcare facilities as you (Brian Hroch) have indicated. “

21-15.1 INTRODUCTION

A. Purpose

The purpose of this chapter is to provide a guideline to the project architect/engineer (A/E) designers, Indian Health Service (IHS) staff, and tribal staff for determining a security level and security design standards for IHS health care facilities.

Comment [MRW2]: Greg Heck commented that “Be sure to involve several of the senior and more qualified security personnel at the Service Units in putting together this chapter. We have several from our Area. I would assume other Areas have some outstanding Security personnel. The Security personnel from Phoenix Area would recommend the Security Chiefs at PIMC and Hopi as part of the process in developing this Chapter.”

B. Scope

This chapter applies to construction of all new IHS health facilities and staff quarters and could apply to renovation and/or alteration of IHS healthcare facilities and staff quarters.

Comment [MRW3]: This should specify that these standards are homeland security as it appears to only address homeland security preparedness and neglects considering non-terrorism security threats. These non-terrorism security threats are significant, more common and probably more threatening. I would recommend that if there are not already included in this guideline or the OEHE technical handbook, that they be considered and developed. Brian Hroch

It addresses only the required minimum-security standards and their application to the determined security levels of new IHS facilities renovated and leased facilities.

C. Minimum Security Standards

The Office of Emergency Services (OES) has established a process, based on an accredited format, to conduct security surveys at Agency structures to include Critical Infrastructures and Key Assets. Based upon the assets to be protected and sound security practices, OES has identified various types of security measures which could be used to counter potential vulnerabilities.

Comment [MRW4]: This should be defined somewhere. Who is OES? Joe Bermes

Comment [MRW5]: Need to go with OES so we don’t confuse Es with DES. James B.

This minimum set of standards can be applied to various facilities. The standards cover the subjects of security personnel, perimeter, entry, interior security, and security planning. Because of the considerable differences among facilities and their security needs, four separate security categories were developed to determine which minimum standards are appropriate for which level of security.

21-15.2 GUIDELINES

A. Process

The IHS Security Specialist should conduct a security review as a part of the planning process for each new facility or quarters project and, where applicable, for each renovation and/or alteration project or leased space. A security assessment, which contains the Security Specialist's determination of the final security level for the facility, will be included as part of each planning document (i.e., Site Selection and Evaluation Report (SSER), Program Justification Document (PJD), Program of Requirements (POR), etc.). The Area and Service Unit must comply with all approved provisions of the latest security review report and incorporate all recommendations in this guideline as applicable.

B. Risk Assessment

Risk analysis is principally concerned with investigating the risks surrounding physical plant (or some other object), its design and operations. Such analyses tend to focus on causes and the direct consequences for the studied object. Vulnerability analyses, on the other hand, focus both on consequences for the object itself and on primary and secondary consequences for the surrounding environment. It also concerns itself with the possibilities of reducing such consequences and of improving the capacity to manage future incidents.

IHS OES will conduct a vulnerability assessment as a process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a facility or system. Examples of facilities and systems for which vulnerability assessments are performed include, but are not limited to, hospitals, clinics, office space, information technology systems, energy supply systems, water supply systems, transportation systems, communication systems, staff quarters, and supply and service centers. Vulnerability assessments will be conducted for various scales of infrastructure.

Vulnerability assessments have many things in common with risk assessment.

Assessments are performed according to the following steps:

1. Cataloging assets and capabilities (resources) in a system
2. Assigning quantifiable value (or at least rank order) and importance to those resources
3. Identifying the vulnerabilities or potential threats to each resource
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources

Risk analysis is principally concerned with investigating the risks surrounding physical plant (or some other object), its design and operations. Such analyses tend to focus on causes and the direct consequences for the studied object. Vulnerability analyses, on the other hand, focus both on consequences for the object itself and on primary and secondary consequences for the surrounding environment. It also concerns itself with the possibilities of reducing such consequences and of improving the capacity to manage future incidents.

Comment [MRW6]: Should be defined. What Office/OPDIV does this position belong to? Joe Bernes

Comment [MRW7]: Is this the same as a Security Assessment? Joe Bernes

Comment [MRW8]: Is this THE IHS Security Specialist within Office of ES. Brian Hroch

Comment [MRW9]: What is the criteria for determining when this is applicable? Tribes operating IHS owned facilities will now need IHS Security Specialist Approval for renovations and alteration projects. This will need to be negotiated into Title I and V compacts. No such language now exists. The criteria for when Tribes make the determination of when a project is "applicable" needs to be defined. Dale M.

Comment [MRW10]: Who conducts the assessment and how is this funded? 638 Tribes will want to know. Tribes will see this as an unfunded mandate. Dale M.

Comment [MRW11]: This is another term which should be clarified in context with the Risk, Vulnerability, and Threat Assessments discussed below. (See next comment)

Does the Security Assessment include the following?:

... [1]

Comment [MRW12]: I.Greg Heck Comments: "HVA process appears to be a HQ driven with little Area and local input. There must be a process that

... [2]

Comment [MRW13]: A number of terms used here seem to be talking about the same thing: Risk Assessment, Vulnerability Assessment, Risk A

... [3]

Comment [MRW14]: See comment above. Joe Bernes

Comment [MRW15]: These are mentioned previously or are they beyond the scope of the HFAC? Would GSA requirements cover supply service

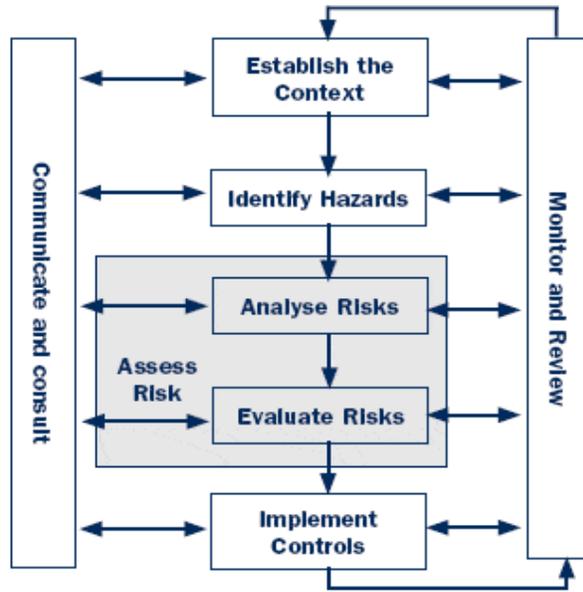
... [4]

Comment [MRW16]: i.e. the Regional Supply and Service Centers (such as Gallup and Ada) Brian Hroch

Comment [MRW17]: Is there a reference document that describes how to conduct this assessment? There does not seem to be enough information here

... [5]

Comment [JEB18]: See comment above.



C. **Threat Assessment**

A threat is the means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifested and is therefore a potential violation of security.

A comprehensive Threat Assessment Process of formally evaluating the degree of threat to a facility, system, or process will help define and describe the nature of the threat or threats (threat agent). A threat agent is a method or occurrence used to exploit a specific or general vulnerability in a facility, system, or operation. Fire, earthquakes, floods, and other natural disasters as well as man-made threats should be included in the Threat Assessment Process.

Comment [MRW19]: Greg Heck "Again, local input is needed."

Comment [MRW20]: Yet another term and another evaluation Joe Bernes

Comment [MRW21]: Not sure how this fits in to the process. James B.

Comment [MRW22]: Is there a reference document that describes how to conduct this assessment? There does not seem to be enough information here. Joe Bernes

D. **Defining the Minimum Security Standards**

Security standards were developed as design criteria for IHS facilities. The standards are listed in Appendix A. They fall into the following categories.

1. **Security Personnel**

Security Personnel standards refer to the level of qualification, desired type of enforcement, and communications equipment used by facility security personnel and other law enforcement that may work in the facility.

The elements of security personnel are:

- Facility Security Personnel
- Other Law Enforcement in Facility

Comment [MRW23]: Greg Heck asked the question about how staffing is calculated when designing a facility? What program or process oversees the staffing of a new healthcare facility, such as evaluation, determination and authorization of the staff composition. Also, "Training of personnel in general does not address some of hospital specific concerns such as de-escalation training, training of staff working in sensitive areas, etc. I also feel the policy is very vague as to training adequacy for security personnel. I strongly suggest they become familiar with the role of health care security both from the JC and International Association for Healthcare Security and Safety to ensure health care related issues are adequately addressed."

2. Perimeter Security

Perimeter security standards pertain to the areas outside of the facility and therefore may extend outside of government control. Depending on the facility type, the perimeter may include sidewalks, parking lots, outside walls of the facility, a hallway, or simply an office door.

The elements of perimeter security are:

- Parking
- Closed Circuit Video Monitoring
- Lighting
- Physical Barriers

3. Entry Security

Entry security standards refer to security issues related to the entry of persons and packages into a facility.

The elements of entry security are:

- Receiving/Shipping
- Access Control
- Entrances/Exits

4. Interior Security

Interior security standards refer to security issues associated with prevention of criminal or terrorist activity within the facility. This area concerns secondary levels of control after people or items have entered the facility.

The elements of interior security are:

- Employee/Visitor Identification
- Utilities
- Occupant Emergency Plans
- Day Care Centers
- Cyber Issues
- Fire Rescue/Life Safety

5. Security Planning

Security planning standards refer to recommendations requiring long-term planning and commitment, as well security standards addressing broader issues with implications beyond security at a particular facility.

The elements of security planning are:

- Intelligence Sharing
- Training
- Tenant Assignment
- Administrative Procedures
- Construction/Renovation

Comment [MRW24]: Greg Heck "It should include **sensitive areas** similar to what JC uses: may include (my recommendation is to include all) emergency departments; pharmacies; nurseries and pediatric wards; medical records"

21-15.3 REFERENCE STANDARDS

A. Security Levels for Indian Health Service Facilities

Since there are vast differences in types of facilities and their security needs, the facilities were divided into four security levels (levels I – IV). These security levels are described below. The listed security levels have been based on the following criteria:

NOTE: Final assignment of a security level to a facility will be adjusted based on designation, risk assessment, threat assessment and intelligence, crime statistics, agency mission, proximity to higher risk facilities, etc.

Comment [MRW25]: If a facility meets all the criteria for any given level, but meets one criteria from the next higher level, which level will it be assessed at?

See note below for “significant crime area” example.
Joe Bermes

Comment [MRW26]: What about the Vulnerability Assessment, or is that part of the Risk Assessment?
Joe Bermes

Level I

- The total number of employees working at the facility is less than 11.
- The facility/location does not have multi-agency risk considerations.
- The facility has a low volume of public contact.
- The facility is not located in a significant crime area.
- The occupants of the facility do not produce or develop critically sensitive and/or classified information or projects on a regular basis.
- The facility does not have a laboratory or storage area containing biological/chemical/radiological or other hazardous agents (that are not commercially available to the general public).
- The economic/social impact caused by the loss of this facility by the government/private sector would be minimal.
- The loss of this facility would not cause or be a factor in other catastrophes.
- The facility/structure does not contain Agency critical systems.
- The facility/structure has not been designated as a “Critical Infrastructure/Key Asset.”

Level II

- The total number of employees working at the facility is between 11 and 150.
- The facility/location does not have multi-agency risk considerations.
- The facility has a moderate volume of public contact.
- **The facility is not located in a significant crime area.**
- The occupants of the facility do not produce or develop critically sensitive and/or classified information or projects on a regular basis.
- The facility may have a laboratory or storage area containing a **small** amount of biological/chemical/radiological or other hazardous agents (that are not commercially available to the general public).
- The economic/social impact caused by the loss of this facility by the government/private sector would be at a localized level.
- The loss of this facility would not be a determining factor of other catastrophes.
- The facility/structure does not contain Agency critical systems.
- The facility/structure has not been designated as a “Critical Infrastructure/Key Asset.”

Comment [MRW27]: If a facility meets all of the other criteria for Level II but is located in a significant crime area, will it be rated Level II or something higher?

NOTE: This type of question could be asked about any of the criteria at any level.
Joe Bermes

Comment [MRW28]: Define small – John L.

Level III

- The total number of employees working at the facility is between 151 and 450.
- The facility/location may have multi-agency risk considerations.
- The facility has a moderate to significant amount of public contact.
- The facility may be located in a significant crime area.
- The occupants of the facility may produce or develop critically sensitive and/or classified information or projects on a regular basis.
- The facility may have a laboratory or storage area containing a moderate amount of biological/chemical/radiological or other hazardous agents (that are not commercially available to the general public).
- The economic/social impact caused by the loss of this facility by the government/private sector would be at a regional level.
- The loss of this facility may be a factor in other catastrophes.
- The facility/structure does not contain Agency critical systems.
- The facility/structure has not been designated as a “Critical Infrastructure/Key Asset.”

Comment [MRW29]: Define moderate amount – John L.

Level IV

- The total number of employees working at the facility is greater than 450.
- The facility/location may have multi-agency risk considerations.
- The facility has a significant amount of public contact.
- The facility may be located in a significant crime area.
- The occupants of the facility produce or develop critically sensitive and/or classified information or projects on a regular basis.
- The facility has a laboratory or storage area containing a significant amount of biological/chemical/radiological or other hazardous agents (that are not commercially available to the general public).
- The economic/social impact caused by the loss of this facility by the government/private sector would be at a national level.
- The loss of this facility could cause or be a factor in other catastrophes.
- The facility/structure may contain Agency critical systems.
- The facility/structure has not been designated as a “Critical Infrastructure/Key Asset.”

B. Application of Recommended Minimum Security Standards

The recommended minimum-security standards applicable to each of the four security levels are covered in Appendix A. *Facility Security Standards*

Seems like we need to include guidance on design standards for meeting the items to be constructed. Is there a guide that would specifically indicate what the setbacks from the building we want for parking? Is there a guide that indicates designing buildings without spots hidden from view? Is there a guide that tells us what is ‘security fencing’? James B.

General comments:

- good start and I think with some editing will definitely work.

- this does tend to mix operations with design. While the operations may only work with an appropriate design this will require, for best operations, working closely with the facility staff to ensure the two mesh. James B.

- my comments do not go into detail. I only reviewed this to make general comments. James B.

- we may need to be specific to say the 1995 Levels have been adjusted for the IHS unique situation. I'm afraid if we don't we will continue to run into conflicts. James B.

Overall, the document seems better than previous versions but still needs work to provide clear direction to an A/E or IHS staff in determining the security requirements for a health care facility. Keith S.

In general, it appears to me that this policy will place increased burdens on IHS owned facilities that are operated by PL 93-638 Tribes under Title I or Title V. If these Tribes are to comply with these requirements it will need to be negotiated into their Funding Agreement or compacts. The law which requires them to comply with these requirements would need to be cited and the Tribes would likely ask where the additional funding will come from to comply with the requirements. Dale M.

I have a hard imagining 638 Tribes going through a review process with Headquarters security staff on ever renovation/alteration project they do. Need the law cited in the policy which would require this. Dale M.

I still think that the Security Standards Appendix needs to be focused on healthcare facilities. Is anyone aware of such an assessment? I found one via ASHE, but it needs work, particularly if it would be applicable to security specs for the design and construction of health care facilities. Brian Hroch.

Tell me if I correctly understand the process laid out in this document: A Security Assessment will be conducted during the planning phase of every new construction project or renovation. The Security Assessment includes a Risk Assessment, Vulnerability Assessment, and Threat Assessment. The Security Assessment will result in the classification of the building as a Level I, II, III, or IV. Appendix A identifies the Facility Security Standards for each Level which must be incorporated into the design.

Joe Bermes

APPENDIX A. – FACILITY SECURITY STANDARDS

M - MINIMUM STANDARD

S - STANDARD BASED ON FACILITY EVALUATION

D – DESIRABLE

N/A - NOT APPLICABLE

FACILITY LEVEL		I	II	III	IV
<u>SECURITY PERSONNEL</u>					
1	FACILITY SECURITY PERSONNEL				
	Dedicated Trained Security Force	D	D	S	S
	Dedicated Armed Security Force	N/A	N/A	N/A	N/A
	Posts at all accessible entrances/exits	D	D	S	S
	Roving Patrols	D	D	S	S
	Armed Officers at all Magnetometer Screening Points	N/A	N/A	N/A	N/A
	Access to EOD K-9 on a 24 hours basis	N/A	N/A	N/A	N/A
	Reliable 24 hour Communication System for Security Personnel (ONLY)	D	S	S	M
	Interoperable Communications with other Law Enforcement or Security Organizations	D	S	S	M
<u>PERIMETER SECURITY</u>					
1	PARKING				
	Control of facility parking.	D	D	S	S
	Control of adjacent parking.	D	D	D	S
	Avoid leases where parking cannot be controlled.	D	D	D	D
	Leases should provide security control for adjacent parking.	D	D	D	D
	Post signs and arrange for towing unauthorized vehicles.	M	M	M	M

Comment [MRW30]: As I commented before, I think it would be appropriate to have the table further defined by the healthcare departments, particularly for high risk locations. I also suggest that greater consideration be given to the facility's specific characteristics, such as existing community threats, property crime risk, violent crime risk, as well as location (rural, vs. urban). I realize this will expand the table substantially, but locations such as Pharmacy, labor/delivery, post partum, peds, ER, general services, all have unique security considerations. And some have greater requirements than other locations. Types of controls, familiar to healthcare facilities, such as HUGS/KISS should also be referenced in this design criteria. AHSE has some materials that may be used to refine/edit existing healthcare specific security assessments. Brian Hroch

Comment [MRW31]: What does this mean? Required or not? Joe Bernes

Comment [MRW32]: What do these mean? What is required, suggested, not required, optional? Kevin D.

Comment [MRW33]: What about non-leased parking? Kevin D.

Comment [MRW34]: What about non-leased parking? Kevin D.

Comment [MRW35]: I have difficulty accepting that will be a requirement for all small IHS clinics in remote areas of Alaska. Is this the intent? Dale M.

	ID system and procedures for authorized parking (placard, decal, card key, etc.).	D	M	M	M
	Adequate lighting for parking areas.	M	M	M	M
	Employee Parking separated from Public Parking	NA	D	M	M
	Bollards preventing unauthorized access	S	S	D	D
2	CLOSED CIRCUIT TELEVISION (CCTV) MONITORING				
	CCTV surveillance cameras with time-lapse video recording.	D	S	S	M
	Security Room for monitoring the CCTV System	D	S	S	M
	Post signs advising of 24-hour video surveillance.	D	S	S	M
3	LIGHTING				
	Exterior lighting with 360 degree coverage around facility	M	M	M	M
	Parking Area Lighting	M	M	M	M
	Lighting meets minimum standard for CCTV use.	D	S	S	M
	Lighting with emergency battery power backup.	M	M	M	M
4	PHYSICAL BARRIERS				
	Extend physical perimeter with barriers (concrete and/or steel composition).	NA	D	D	S
	Rated or Landscape barriers separating drop off/parking area from facility	D	D	D	S
<u>ENTRY SECURITY</u>					
1	RECEIVING/SHIPPING				
	Review receiving/shipping procedures (current).	M	M	M	M
	Implement receiving/shipping procedures (modified).	M	M	M	M
	Sort all mail in a closed vessel or downdraft table	D	M	M	M
	Restrict delivery access to authorized vehicles/personnel	M	M	M	M
2	ACCESS CONTROL				
	Evaluate facility for security guard requirements.	M	M	M	M
	Security guard patrol.	D	D	S	S
	Intrusion detection system with central monitoring capability.	D	S	M	M
	Design to current life safety standards (fire detection, fire suppression systems, etc.).	M	M	M	M
3	ENTRANCES/EXITS				
	X-ray and magnetometer at public entrances.	NA	S	S	S
	Require screening of all mail/packages.	M	M	M	M
	Peep holes	S	S	S	S

Comment [MRW36]: I have difficulty accepting that will be a requirement for all small Level 1 IHS clinics in remote areas of Alaska. Increased Utility and O&M costs as a result of the requirement will be passed on to Tribes operating IHS facilities under P.L. 93-638. Is this the intent? Dale M.

Comment [MRW37]: Same comment as above. Dale M.

Comment [MRW38]: Lighting with emergency battery power backup" Does this mean we have to have emergency power or battery backup on all exterior lights at a facility or just some? It is listed as Minimum Standard on all types of facilities. This seems to be overkill for a small facility and is going to add a lot to the cost of lighting.

Comment [MRW39]: x-ray and magnetometer at public entrances" Is this the direction we are heading in all but the small facilities? If so, this will be expensive and require a trained security staff to operate the equipment. We would need multiple units to cover the Emergency Entrance as well as the Main Entrance. Keith S.

The use of "desirable" seems to leave a lot up to interpretation. If something is not mandated, it probably has little chance of being implemented especially with tight budgets. Keith S.

I didn't see anything in the document that addresses "access control systems". How are areas of the building secured and do we use the new HSPD 12 compliant ID cards to gain access to secure areas of a building? Keith S.

	Intercom	S	S	S	S
	Entry control w/CCTV and door strikes.	D	S	S	M
	High security locks.	M	M	M	M
<u>INTERIOR SECURITY</u>					
1	EMPLOYEE/VISITOR IDENTIFICATION				
	Agency photo ID for all personnel displayed at all times.	M	M	M	M
	Visitor control/screening system.	D	M	M	M
	Visitor identification accountability system.	D	M	M	M
	Establish ID issuing authority.	M	M	M	M
2	UTILITIES				
	Provide security locks to prevent unauthorized access to utility areas.	M	M	M	M
	Provide emergency power to critical systems (alarm systems, radio communications, computer facilities, etc.).	M	M	M	M
	Ability and procedures to close air intake system	M	M	M	M
	Dedicated HVAC system for lobbies, mailrooms, and loading dock (receiving) areas	D	D	D	M
3	OCCUPANT EMERGENCY PLANS				
	Examine occupant emergency plans (OEP) and contingency procedures based on threats.	M	M	M	M
	OEPs in place, updated annually, periodic testing exercise.	M	M	M	M
	Assign and train OEP officials (assignment based on largest tenant in facility).	M	M	M	M
	Annual tenant training.	M	M	M	M
4	DAYCARE CENTERS				
	Evaluate whether to locate daycare facilities in buildings with high threat activities.	NA	M	M	M
	Compare feasibility of locating daycare in facilities outside locations.	NA	M	M	M
<u>SECURITY PLANNING</u>					
1	INTELLIGENCE SHARING				
	Establish law enforcement/security liaisons.	M	M	M	M
	Review/establish procedures for intelligence receipt/dissemination.	M	M	M	M
	Establish uniform security/threat nomenclature.	M	M	M	M
2	TRAINING				
		M	M	M	M

Comment [MRW40]: Does IHS have any Day Care Centers within its inventory? If not, delete this element as it would suggest that this is IHS supportable space. Dale M.

Comment [MRW41]: How do Tribes operating IHS owned facilities under PL93-638 comply with these requirements? Dale M.

Comment [MRW42]: How does this apply to Tribes operating IHS owned facilities under 638 Title I and Title V? Who pays for the additional training costs when not negotiated in the funding agreements with the Tribe. What is the law or regulation that makes it mandatory for Tribes to comply with this requirement? Dale M.

	Conduct annual security awareness training.	M	M	M	M
	Establish standardized unarmed guard qualifications/training requirements.	M	M	M	M
	Establish standardized armed guard qualifications/training requirements.	M	M	M	M
3	TENANT ASSIGNMENT				
	Co-locate agencies with similar security needs	D	D	D	D
	Do not co-locate high/low risk agencies.	D	D	D	D
4	ADMINISTRATIVE PROCEDURES				
	Establish flexible work schedule in high threat/high risk areas to minimize employee vulnerability to criminal activity.	S	S	D	D
	Arrange for employee parking in/near building after normal work hours.	S	S	S	S
	Conduct background security checks and/or establish security control procedures for service contract personnel.	M	M	M	M
5	CONSTRUCTION/RENOVATION				
	Install mylar film on all exterior windows (shatter protection).	D	D	D	D
	Review current projects for blast standards.	M	M	M	M
	Review/establish uniform standards for construction.	M	M	M	M
	Review new design standard for blast resistance.	M	M	M	M
	Establish street setback for new construction.	D	D	S	M
	Review projects for Fire Safety Code	M	M	M	M

ATTACHMENT 3 [Task Force Report on the International Property Maintenance Code](#)

ATTACHMENT 4 [Technical Handbook Chapter 4-1 – Health Facility Advisory Committee](#)

Page 7: [1] Comment [MRW11] Mweaver 12/17/2009 9:26:00 AM

This is another term which should be clarified in context with the Risk, Vulnerability, and Threat Assessments discussed below. (See next comment)

Does the Security Assessment include the following?:

1. Risk Assessment
2. Vulnerability Assessment
3. Threat Assessment

Joe Bermes

Page 7: [2] Comment [MRW12] Mweaver 12/17/2009 9:26:00 AM

1. Greg Heck Comments: “HVA process appears to be a HQ driven with little Area and local input. There must be a process that includes local input, etc. in order to get appropriate buy-in. I recommend a planning model similar to that statistics (incidents, security survey data, police activity and/or crime grid statistics), all level of employee/managerial involvement, setting of objectives, evaluation, etc.). “

Page 7: [3] Comment [MRW13] Mweaver 12/17/2009 9:26:00 AM

A number of terms used here seem to be talking about the same thing: Risk Assessment, Vulnerability Assessment, Risk Analysis. The last paragraph in this section attempts to define the difference between Risk and Vulnerability Assessments, but throws in yet another term, “analysis.” Paragraph B ought to be revised to be consistent in language and provide clarity in definition.

Joe Bermes

Page 7: [4] Comment [MRW15] Mweaver 12/17/2009 9:26:00 AM

These are mentioned previously or are they beyond the scope of the HFAC? Would GSA requirements cover supply service centers? I believe quarters were covered in previous chapters or HFAC decisions. Brian Hroch.

Page 7: [5] Comment [MRW17] Mweaver 12/17/2009 9:26:00 AM

Is there a reference document that describes how to conduct this assessment? There does not seem to be enough information here. Joe Bermes