

HEALTH FACILITIES ADVISORY COMMITTEE (HFAC)
MEETING MINUTES

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

Roll Call:

Chairman: Mr. Tommy Bowman X

Vice-Chairman: CAPT Keith Shortall ()

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

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

Guests: CAPT Kevin Malloy, Mr. Dean Ross, Mr. Ray Cooke, CDR Michael
Young

Approval of the previous meeting minutes. Ken requested the following phrase, "*for Tribally owned and/or operated facility.*" be added to the end of the last sentence on page 3. Jim motioned to approve meeting minutes of Feb 29, 2008 as amended by Ken; Brian seconded motion. **Motion passed without objection.**

Old Business:

- Discuss Technical Handbook Chapter 21-15 Security Level Selection For Use in the Design of New Federal Facilities.
 - Tommy opened the discussion by stating the intention was to identify concerns related to incorporating security issues into the design of new facilities. He asked Michael if he had received everyone's comments to Draft Chapter 21-15. Michael responded that he received only 2 comments and stated the prevailing sentiment by some members was that the draft was not ready for editing pending discussion with Sid Caesar on the next HFAC conference call on April 17.
 - Representing Sid were guests: Dean Ross, IHS/HQS and CAPT Kevin Malloy, Office of Assistant Secretary for Preparedness and Readiness (ASPR). They introduced themselves and their respective mission. Dean emphasized that his office is not responsible to implement HSPD-12 except for infrastructure issue such as card readers.
 - Tommy asked Dean what was the overall security intent and the security game plan. Dean responded the game plan was to assess

existing facilities regarding the current state of security. To date they have surveyed the Albuquerque Area Office, Phoenix Area Office, and PIMC. The intent this year is to survey all 12 Area offices and 4 largest clinics and to train IHS staff to conduct security surveys.

- Jim stated he was expecting guidance on the process to determine the level of security that would determine the design requirements of facilities but not “the actual distance of light poles”.
- Tommy and Ken expressed their expectation was the development of security guidance that may be given to the A/E to incorporate into the design.
- Dean re-drafted Chapter 21-15 with an overview of the threat assessment process. At this time Jim e-mailed all the HFAC members a copy of this re-draft. A copy is attached to this meeting minutes.
- Ken stated the security assessment should be conducted during the planning phase and the results documented in the Site Selection Evaluation Reports (SSER), Program Justification Document (PJD), and the Program of Requirements (POR).
- Michael Weaver asked Dean and Kevin Malloy why their draft included Security Level IV for IHS because a loss would not meet the standard of affecting national security or national public health. Dean and Malloy disagreed and stated a loss would affect national public health – “health of the people”. Ken reinforced Michael’s position stating our current construction standard does not support a facility being self- sustaining beyond 3 to 5 days (i.e., generator, fuel storage, etc.). Ken used Anchorage as an example. But Brian stated loss of PHS staff would adversely affect national health.
- Kevin Malloy stated security concerns needed to be considered during the planning phase and guidance needed to be developed to design and staff a new facility.
- Dean agreed with earlier comments that the security assessment needed to be accomplished during the development of the PJD and POR. He stated specific security design requirements for the proposed new facility needed to be included in the POR.
- Dean and Tommy summarized the security process. IHS HQS would be responsible to perform the security assessment for the new facility and document the security design requirements in a report or directly added to the PJD and POR. During the design phase, the design submittals are reviewed by the Area Office. The Area Office would be responsible to coordinate with all their Area stakeholders to include the Area Security Officer to review the design submittal. Hence, no additional design submittal package would be necessary for distribution by the A/E.
- Ken asked if the security requirements of Chapter 21-15 apply to GSA leases. Dean responded stating the Area Security Officer would visit the existing building proposed for a GSA lease. However, existing conditions may be too onerous to change and the added risk may be

acceptable. Hence, some requirements of Chapter 21-15 would be waived.

- Tommy asked Jose for those projects that have already completed the PJD and POR, how will those projects be reviewed for security requirements. Jose said that Sid's staff has been involved in the review of those projects. Ken asked about projects "looking further". Jose said he will review the process.
 - Brian asked Dean if he has reviewed the Chinle Expansion project which is under construction now. Dean replied he will review it when he gets the drawings. Jim asked Dean if he is the Point of Contact (POC) for submission of drawings and that Dean will coordinate with the Area Security Officer. Dean replied yes.
 - Jose expressed concern that the security design requirements may adversely impact the current funding budgets. Dean said of the 7 surveys they have conducted, most of their recommendations cost \$20 - \$25 per item. These were the "low hanging fruits".
 - Ken expressed concerned that reviews by security staff would not be timely and used Barrow as an example because the security comments have not yet been received. Kevin Malloy stated they completed their review on Barrows in just a couple of hours. Ray Cooke offered to check with Ed Cayous if the security comments have not been forwarded to Seattle.
 - Kevin D'Amanda said that Jose will forward an editable copy of Chapter 21-15. The attachment sent during this call by Jim was in .pdf format.
 - Tommy established a deadline for comments to Chapter 21-15 be submitted to Michael Weaver no later than May 2, 2008.
- Report from the Task Force regarding adoption of the International Property Maintenance Code (IPMC).
 - Michael Young briefed the HFAC on the status of the Task Force's review of the IPMC. The Task Force had its first conference call on March 12 with 5 of 7 members participating.
 - The Task Force agreed that many of the codes were not relevant to IHS but other portions of the IPMC had merit. Task Force explored 4 courses of action:
 - Issue an addendum to the IPMC to select those portions of the code that applied or did not apply. Task Force dropped this course of action from further consideration.
 - Create a separate IHS code. Task Force considered this not to be an acceptable course of action.
 - Explore other codes. Task Force members expressed no interest in doing this.
 - Take no action.

- A second conference call was held on April 3 with 6 of 7 members to respond to rejection of their report as being incomplete.
 - Michael provided several examples of conflict if the IPMC is adopted in whole.
 - Michael stated the Task Force members are to submit their comments to Dwight Packer by April 23.
 - Michael summarized stating the Task Force is leaning to not adopt IPMC in whole; therefore, the challenge is to determine how to adopt parts.
 - Kevin D’Amanda stated the objections are not based on code conflicts but on cost, practicality, and opinions. Kevin commented that the Task Force members have a hesitation of being “open-mind”; some members are rejecting the Code before developing a detailed list of conflicts as requested by the HFAC.
 - Jim stated no other code is out there and that the IPMC is not a residential code. He reminded the HFAC that IHS currently has no code in this area. Jim rhetorically asked, “if not this (IPMC), then what?”. Jim said the IPMC has value.
 - Michael said another conference call with the Task Force will be scheduled. He estimated that by the week of May 12 the report will be completed.
 - Ken challenged the workgroup to arrive at a consensus recommendation in their report and that consensus means all workgroup members may not totally agree with the final recommendation, but can live with it.
 - Tommy established a deadline of May 14 for the completed report.
- Discuss how HFAC will ask Facility Managers’ input to the Condition Index statement of work.
 - Jim stated the scope of work referred to the Facility Condition Survey not the Condition Index. Jim recommended tabling this item. He will re-think this issue and may raise it during the monthly Facility Managers’ conference call.
- Brian stated his alternate, John Smart, has accepted a job with ASPR. Brian inquired how he should appoint a successor. Ken suggested Brian consult with Kelly Taylor on appointing his alternate.
 - Brian announced effective July 21 he will laterally transfer to Albuquerque Area Office. This transfer will not affect his membership on the HFAC.
 - Ken stated the technical handbook chapter on USP 797 has been sent out and asked Tommy if he distributed it to everyone. Tommy responded he sent it to Lee Robinson and a select few.

- Michael Weaver gave update on the other technical handbook chapters. He stated Chapters 21-5 Electrical Guidance, 24-2 Applicability of Codes, Construction Codes and Standards, and the new chapter for USP 797 were in for signature with Lee.

New Business: None.

Action Items:

- Jose will distribute a MSWord Document version of Chapter 21-15 for the HFAC to edit with comments.
- HFAC members to submit their comments on Technical Handbook Chapter 21-15 Security to Michael Weaver no later than May 2. Michael will compile comments and distribute prior to the next HFAC call on July 17.
- The Task Force for the International Property Maintenance Code will submit their completed report to the HFAC Chairman no later than May 14. HFAC Chairman will distribute the report to the other HFAC members.

Next Conference Call: July 17, 2008 at 12:00 p.m. (Eastern Time)

Adjournment: Jim motioned to adjourn; Brian seconded motion. **Motion passed without dissent.**

Attachments:

ATTACHMENT 1 Agenda for April 2008

ATTACHMENT 2 DRAFT Handbook Chapter: Security Level

ATTACHMENT 3 Link to February 2008 Minutes

ATTACHMENT 1 Agenda for April 2008

HEALTH FACILITIES ADVISORY COMMITTEE (HFAC)

AGENDA

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

Conference Call: # 888-282-9627

Pass Code: 59140

Roll Call:

Chairman: Mr. Tommy Bowman ()

Vice-Chairman: CAPT Keith Shortall ()

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

Alternates:

Guests:

Approval of the previous meeting minutes (Feb 29, 2008 see attachment)

Old Business:

- Discuss Technical Handbook Chapter 21-15 Security Level Selection For Use in the Design of New Federal Facilities – Guest – Sid Caesar
- Report from the Task Force regarding adoption of the International Property Maintenance Code
- Discuss how HFAC will ask Facility Managers' input to the Condition Index statement of work

New Business: None

Next Meeting: To be Determined

Attachments:

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 selecting a security level and security design standards for IHS health care facilities.

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.

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

C. Recommended Minimum Security Standards

The Office of Emergency Services (ES) 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, ES has identified various types of security measures which could be used to counter potential vulnerabilities.

This minimum set of standards can be applied to various facilities. The standards cover the subjects of security personnel, perimeter, entry, and 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. 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 designer must comply with all approved provisions of the latest security review report and incorporate all recommendations in this guideline as applicable.

B. Risk Assessment

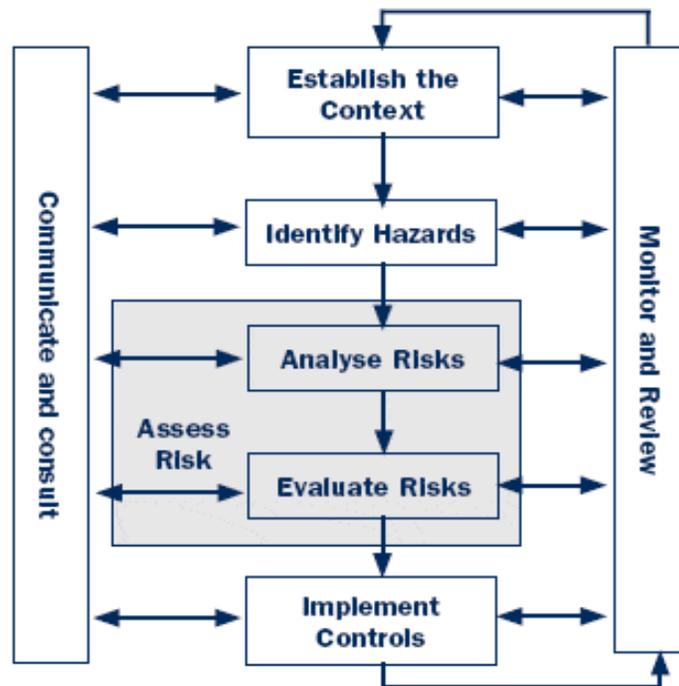
IHS ES will conduct a vulnerability assessment as a process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a facility or system. Examples of facilities and systems for which vulnerability assessments are performed for include, but are not limited to, hospitals, clinics,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



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.

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

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

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.

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.”

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.”

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*

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
	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	N/A	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
	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.	N/A	M	M	M
	Compare feasibility of locating daycare in facilities outside locations.	N/A	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				
	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 [Link to February 2008 Minutes](#)