
**PHYSICAL SECURITY ASSESSMENT
FOR DEPARTMENT OF
VETERANS AFFAIRS FACILITIES**

**RECOMMENDATIONS OF THE
NATIONAL INSTITUTE OF
BUILDING SCIENCES
TASK GROUP**

**TO THE
DEPARTMENT OF VETERANS AFFAIRS**

6 September 2002



**PHYSICAL SECURITY ASSESSMENT
FOR DEPARTMENT OF
VETERANS AFFAIRS FACILITIES**

**RECOMMENDATIONS OF THE
NATIONAL INSTITUTE OF
BUILDING SCIENCES
TASK GROUP**

**TO THE
DEPARTMENT OF VETERANS AFFAIRS**

6 September 2002



PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES

Task Group

Curt P. Betts, PE
US Army Corps of Engineers
Tri-Service Protective Design Center
Omaha, NE 68144-3869

William H. Choquette
Senior Vice President
Gilbane Building Company
Bethesda, MD 20814

James G. Haughton, MD, MPH
Medical Director of Public Health
LA County Department of Health
Services
Los Angeles, CA 90012

Stuart L. Knoop, FAIA
Principal
Oudens + Knoop Architects
Chevy Chase, MD 20815

Richard McClintock
Director of Security
Dartmouth-Hitchcock Medical Center
One Medical Center
Lebanon, NH 03756

Robert Ted Nuckolls, CCE
Baltimore Area Executive for Baltimore
Cemeteries
Baltimore, MD 21212

Michael Rawson, CHSP, HEM
Director of Safety, Security and Support
Services
Intermountain Health Care Inc.
Salt Lake City, UT 84111

Terri Rebmann, RN, MSN, CIC
Center for the Study of Bioterrorism
and Emerging Infections
Saint Louis University
St. Louis, MO 63104

Charles Thornton, PhD, PE
Chairman
Thornton-Tomasetti Group
Washington, DC 20036

Pax Williams
Senior Research Scientist
Battelle Edgewood Operations
Bel Air, MD 21015

James E. Woods, PhD, PE
Executive Director
The Building Diagnostics Research
Institute, Inc.
Bethesda, MD 20814

Project Team

Earle Kennett
Vice President
National Institute of Building Sciences
Washington, DC 20005

Michael Chipley, PhD
Vice President
UTD Inc.
Manassas, VA 20109

Robert Cizmadia, CPP, FSO
Director Corporate Security
Gage-Babcock & Associates
Chantilly, VA 20151

Charles Meyer, PE, FACEC
President
Henry Adams, Inc.
Baltimore, MD 21204

Robert Smilowitz, PhD, PE
Principal
Weidlinger Associates
New York, NY 10014

Russell Weber, AIA
Leo A. Daly Company
Washington, DC 20036

Department of Veterans Affairs

Lloyd H. Siegel, FAIA
Associate Chief Facilities Management
Officer for Strategic Management
Office of Facilities Management
Department of Veterans Affairs
Washington, DC 20420

Kurt D. Knight, PE
Director, Facilities Quality Service
Strategic Management Office
Department of Veterans Affairs
Washington, DC 20420

Marcelle Habibion, EdD
Office of Policy & Planning
Department of Veterans Affairs
Washington, DC 20420

James W. Dudley
Director
Hunter Holmes McGuire
VA Medical Center
Richmond, VA 23249

William B. Harper
Director, Police and Security Service
Department of Veterans Affairs
Washington, DC 20420

Richard Iafolla
Chief, Facilities and Engineering
Service
VA Maryland Health Care System
Baltimore, MD 21201

Mike Elliott
Director, Project Support Service
National Cemetery Administration
Department of Veterans Affairs
Washington, DC 20420

Richard McCrone
Engineering
Department of Veterans Affairs
Washington, DC 20420

Keith Frost
Police and Security Service
Department of Veterans Affairs
Washington, DC 20420

Mark Ackerman
Veterans Benefits Administration
Department of Veterans Affairs
Washington, DC 20420

Leo Phelan, AIA
Director, Space Management and
Emergency Preparedness
Veterans Benefits Administration
Department of Veterans Affairs
Washington, DC 20420

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
INTRODUCTION	3
RECOMMENDATION 1: VULNERABILITY AND FACILITY ASSESSMENTS	9
RECOMMENDATION 2: CRITICAL FACILITIES	15
RECOMMENDATION 3: SHORT-TERM PROTECTION STRATEGIES	17
RECOMMENDATION 4: SECURITY CRITERIA	19
RECOMMENDATION 5: FACILITY ASSESSMENT TEAMS	21
RECOMMENDATION 6: PROTECTION REQUIREMENTS	23
RECOMMENDATION 7: CONSTRUCTION DOCUMENTS	25
RECOMMENDATION 8: CONSTRUCTION ACTIVITIES	27
RECOMMENDATION 9: OPERATIONS AND MAINTENANCE	29
APPENDICES	31
I. VULNERABILITY ASSESSMENT PROCEDURES	32
II. FACILITY ASSESSMENT CHECKLIST	33
III. FACILITY ASSESSMENT REPORT OUTLINE	60
IV. GLOSSARY	62
V. BIBLIOGRAPHY	63
VI. TASK GROUP AND PROJECT TEAM BIOGRAPHIES	64

EXECUTIVE SUMMARY

In May 2002, at the request of the Department of Veterans Affairs (VA), the National Institute of Building Sciences (NIBS) assembled a Task Group of volunteer experts and a project team representing the healthcare, facility, security, and cemetery sectors to advise VA on what major emergency and disaster threats should be guarded against and how best to evaluate its facilities' vulnerabilities against these threats.

NIBS was established and authorized by the U.S. Congress through Public Law 93-383 to serve as an authoritative national source to make findings and to advise both the public and private sectors of the United States with respect to matters of building science.

It has long been the policy of the United States to assure the continuity and viability of critical infrastructure. Executive Order 12656, issued 18 November 1988, requires that "The head of each Federal department and agency shall ensure the continuity of essential functions in any national security emergency by providing for: a succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities."

The Task Group for the Physical Security Assessment for the Department of Veterans Affairs Facilities met on 31 May, 26 June, and 31 July 2002.

Current assessments of VA show that the primary threats faced by the Department continue to be routine criminal activity and violence in the workplace; however the proximity of some VA facilities to high vulnerability targets and their role in the public health system elevate the risk of VA facilities to collateral damage.

The following recommendations serve as a collective deliberation of the Task Group to provide an implementation plan for VA to systematically assess the vulnerability of its facilities and provide mitigation solutions in order to remain an effective part of national emergency services.

The Task Group believes that the implementation of these recommendations will:

- ◆ Permit the Department of Veterans Affairs to define the vulnerability of its critical infrastructure and implement cost-effective remedial and mitigation solutions in a structured and timely manner;

- ◆ Permit the Department of Veterans Affairs to identify and redress the most significant critical infrastructure vulnerabilities first; and
- ◆ Provide the Department of Veterans Affairs with the necessary framework to ensure the continuity of operations (COOP) of critical infrastructure.

The Task Group for the Physical Security Assessment for the Department of Veterans Affairs Facilities recommends that the Department of Veterans Affairs¹:

1. Perform a full vulnerability assessment of VA facilities by conducting on-site facility assessments of critical facilities utilizing the process presented in the appendices.
2. Identify those facilities that must remain operational during periods of emergency and national crisis and specific protection strategies for these facilities.
3. Investigate major protection strategies to new and existing VA facilities to improve their short-term protection during emergencies and national crises.
4. Review and continue to review state-of-the-art federal and private sector building security criteria and document patterns and trends identified during the facility assessments in order to develop, maintain, and amend policies, guidance, and design criteria for the protection of VA facilities.
5. Form and train physical security facility assessment teams composed of members with high levels of expertise in architecture, civil/structural engineering, mechanical/electrical engineering, security operations/systems engineering, chemical-biological-radiological specialties, and cost estimation to conduct VA facility assessments.
6. Provide a safe environment and minimize the possibility of mass casualties in all VA facilities by adopting the levels of protection requirements in accordance with the Department of Defense *Minimum Antiterrorism Standards for Buildings*.
7. Develop policies and guidance for the preparation and security of construction documents including design drawings, specifications, system and equipment drawings, as-built drawings, and facility assessments to improve the protection of VA facilities and the safeguarding of the documentation.
8. Develop policies and guidance for the physical security of the new and retrofit construction activities of VA facilities and portions of VA facilities that take into consideration the potential threat of emergencies and national crisis.
9. Develop facility operation and maintenance policies and guidance to provide for procedures and practices that ensure the continued safe operation of the physical plant and security systems of VA facilities during emergencies and national crisis.

¹ The recommendations do not address information systems, research laboratories, or security operational procedures which were specifically excluded from the scope of this Task Group.

INTRODUCTION

The U.S. Department of Veterans Affairs (VA) is composed of headquarters and three administrations, the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA) and the National Cemetery Administration (NCA).

One of VA's missions is to provide backup medical resources to the military health system and local communities following large scale emergencies and disasters. It has responsibility for six emergency response functions:

- ◆ Ensuring the continuity of VA medical facility operations.
- ◆ Backing up DoD's medical resources following an outbreak of war or other emergencies involving military personnel.
- ◆ Jointly administering the National Disaster Medical System.
- ◆ Carrying out Federal Response Plan efforts to assist state and local governments in coping with disasters.
- ◆ Carrying out Federal Radiological Emergency Response Plan efforts to respond to nuclear hazards.
- ◆ Supporting efforts to ensure the continuity of government during national emergencies.²

In May 2002, at the request of VA, the National Institute of Building Sciences (NIBS) assembled a Task Group of experts representing the healthcare, facility, security, and cemetery sectors to advise VA on what major emergency and disaster threats should be guarded against and how best to evaluate its facilities' vulnerabilities against these threats.

NIBS was established and authorized by the U.S. Congress through Public Law 93-383 to serve as an authoritative national source to make findings and to advise both the public and private sectors of the United States with respect to matters of building science.

It has long been the policy of the United States to assure the continuity and viability of critical infrastructure. Executive Order 12656, issued 18 November 1988, requires

² Cynthia A. Bascetta, Director, Health Care-Veterans' Health and Benefits Issues, General Accounting Office, before the Committee on Veterans' Affairs, House of Representatives. October 15, 2001.

that “The head of each Federal department and agency shall ensure the continuity of essential functions in any national security emergency by providing for: a succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities.”

A Department of Justice study called *Vulnerability Assessment of Federal Facilities* conducted after a presidential directive issued one day after the 19 April 1995 Oklahoma City bombing, produced minimum standards for security at federal facilities. It divided Federal sites into five security levels ranging from Level 1 (minimum security needs) to Level 5 (maximum). The study identified recommendations for upgrading federal building security, including 52 security standards addressing such items as parking, lighting, physical barriers, and closed circuit television monitoring.

On 19 October 1995, the President issued Executive Order 12977 to improve government-wide coordination of security initiatives. The order created a federal Interagency Security Committee (ISC) to develop and evaluate security standards for Federal facilities. The ISC, of which VA is a member, is responsible for establishing policies for the security and protection of Federal facilities and is overseeing the implementation of security measures in Federal facilities.

Presidential Decision Directive (PDD) 63³ issued 22 May 1998 states, “No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63, that is, 22 May 2003, the United States shall have achieved and shall maintain the ability to protect our nation’s critical infrastructures from intentional acts that would significantly diminish the abilities of:

- ◆ the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- ◆ state and local governments to maintain order and to deliver minimum essential public services; and
- ◆ the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.”

PDD 63 goes on to state, “For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment followed by

³ National Security Presidential Directive (NSPD) 1 issued 13 February 2001 reaffirmed PDD 63.

VULNERABILITY ASSESSMENT DRIVERS

- ◆ **Legislation**
- ◆ **Executive Directives**
- ◆ **New Nature of Threats**
- ◆ **Criticality of Facilities**
- ◆ **Continuity of Operations**
- ◆ **Vulnerability of Facilities**

INFRASTRUCTURE ASSESSMENT OBJECTIVES

- ◆ **Life Safety**
- ◆ **Asset Protection**
- ◆ **Continuity of Operations**

periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector. Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities, and funding.”

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

In addressing this potential vulnerability and the means of eliminating it, PDD 63 asks those involved to be mindful of several principles and concerns including the following:

- ◆ Frequent assessments shall be made of our critical infrastructures’ existing reliability, vulnerability, and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.
- ◆ The Federal government shall, through its research, development, and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.

The General Accounting Office has stated that both the GAO and Inspectors General have issued reports highlighting concerns about PDD 63 implementation and that efforts to perform substantive, comprehensive analyses of infrastructure sector vulnerabilities and development of related remedial plans have been limited.⁴ A March 2001 report by the President’s Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in federal agencies’ implementation of PDD 63 requirements to (1) establish plans for protecting their own critical infrastructure that were to be implemented within 2 years and (2) develop procedures and conduct vulnerability assessments. Specifically,

- ◆ many agency critical infrastructure protection plans were incomplete and some agencies had not developed such plans,
- ◆ most agencies had not completely identified their mission-essential infrastructure assets, and
- ◆ few agencies had completed vulnerability assessments of their minimum essential infrastructure assets or developed remediation plans.

PDD 67 issued 21 October 1998 directs agencies to provide for continuity of operations (COOP) and continuity of government (COG) operations. The purpose of

⁴ Robert F. Dacey, Director, Information Security Issues, General Accounting Office, before the Committee on Energy and Commerce, House of Representatives. July 9, 2002

COOP and COG is to ensure survival of a constitutional form of government and the continuity of essential Federal functions.

Federal Preparedness Circular (FPC) 65 issued 26 July 1999 provides guidance to federal departments for use in developing viable and executable contingency plans for COOP. COOP planning is an effort to assure that the capability exists to continue essential agency functions across a wide range of potential emergencies. The objectives of a COOP plan include:

- ◆ Ensuring the continuous performance of an agency's essential functions/ operations during an emergency;
- ◆ Protecting essential facilities, equipment, records, and other assets;
- ◆ Reducing or mitigating disruptions to operations;
- ◆ Reducing loss of life, minimizing damage and losses; and,
- ◆ Achieving a timely and orderly recovery from an emergency and resumption of full service to customers.

Executive Order 13010, issued in 1996, emphasized eight critical infrastructures whose services are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures are:

- ◆ Electrical Power
- ◆ Gas and Oil Production, Storage, and Delivery
- ◆ Telecommunications
- ◆ Banking and Finance
- ◆ Water Supply Systems
- ◆ Transportation
- ◆ Government Operations
- ◆ Emergency Services

Public Law 107-188, enacted 12 June 2002, requires actions to enhance the readiness of Department of Veterans Affairs medical centers to enable them to fulfill their obligations as part of the Federal response to public health emergencies. Under Section 154 the Law specifically requires VA to carry out an evaluation of the security needs at VA medical centers and research facilities.

The 11 September 2001 terrorist attacks demonstrated the country's vulnerability to even a wider range of threats and reasserted heightened public concern for the safety of built facilities and the continued operation of emergency services.

Healthcare facilities and emergency services are an integral part of the nation's critical infrastructure. The planned role of VA hospitals in providing healthcare assistance to other federal agencies, including the Department of Defense, and to their local communities during a large scale emergency require that these facilities remain operational. Certain consolidated or unique VBA benefits and administrative centers providing national operations would result in major economic impacts and wide scale service disruptions if closed should also remain operational. In addition several NCA cemeteries providing continuous operation and national support should remain operational.

Threats to these critical infrastructures fall into two categories: physical threats to tangible property and threats of electronic or computer-based attacks on the information systems that control these critical infrastructures. The deliberations of the Task Group and the recommendations documented in this report involve only physical threats.

Current assessments of VA show that the primary physical threats faced by the Department continue to be routine criminal activity and violence in the workplace; however the proximity of some VA facilities to high vulnerability targets and their role in the public health system elevate their risk from both internal and external threats.

The Task Group for the Physical Security Assessment for the Department of Veterans Affairs Facilities met on 31 May, 26 June, and 31 July 2002. The following recommendations serve as a collective deliberation of the Task Group to provide a plan for VA to assess systematically the vulnerability of its facilities and provide mitigation solutions in order to remain an effective part of the national emergency service during a national or local emergency.

VULNERABILITY ASSESSMENT OF CRITICAL INFRASTRUCTURE DIRECTIVES

- ◆ **EXECUTIVE ORDER 13010: CRITICAL INFRASTRUCTURE PROTECTION (1996)**
- ◆ **PRESIDENTIAL DECISION DIRECTIVE 63: CRITICAL INFRASTRUCTURE PROTECTION (1998)**
- ◆ **PRESIDENTIAL DECISION DIRECTIVE 67: ENSURING CONTINUITY OF GOVERNMENT OPERATIONS (1998)**
- ◆ **NATIONAL SECURITY PRESIDENTIAL DIRECTIVE 1 (2001)**
- ◆ **PUBLIC LAW 107-188: PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2002 (2002)**

RECOMMENDATION**1:** **Vulnerability and Facility Assessments****PERFORM A FULL VULNERABILITY ASSESSMENT OF VA FACILITIES BY CONDUCTING ON-SITE FACILITY ASSESSMENTS OF CRITICAL FACILITIES UTILIZING THE PROCESS PRESENTED IN THE APPENDICES.**

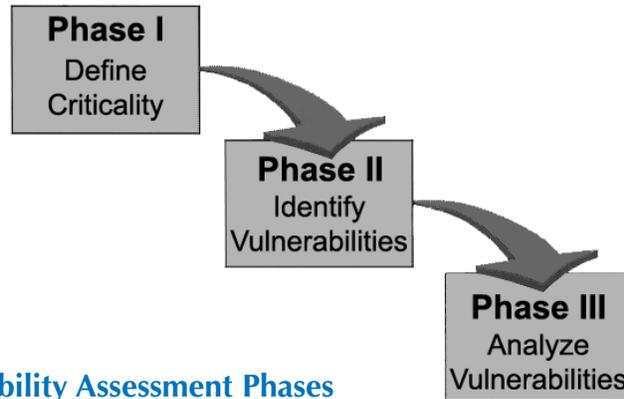
A vulnerability assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may be exploited and suggests alternatives to eliminate or mitigate those weaknesses. The assessments are conducted by teams of experts skilled in such areas as engineering, intelligence, security, information systems, finance, and other disciplines.⁵

An assessment of the 163 hospital facilities, hundreds of related buildings, more than 800 outpatient clinics, 57 benefit offices, 130 cemeteries, and other administrative facilities is needed to determine the threat to and the vulnerability of VA facilities within the total emergency service system of the country.

The Task Group identified a three-phase process to assess the vulnerability of VA facilities:

- Phase I.** Define the criticality of VA facilities, referred to as the Minimum Critical Infrastructure (MCI)
- Phase II.** Identify vulnerabilities of VA's critical facilities
- Phase III.** Assess and analyze vulnerable VA facilities and identify remedial actions

⁵ Raymond J. Decker, Director, Defense Capabilities and Management, before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives. October 12, 2001.



The Vulnerability Assessment Phases

In **Phase I** VA facilities are evaluated with respect to their criticality to the Department's overall missions. The factors applied to make the determination include the value of the facility to VA as a whole, the value to the region, the value to the local community, and/or the value to other critical federal and private facilities; other factors are identified including the proximity of specific VA facilities to perceived strategic targets and proximity to metropolitan areas, especially those areas that might be targets of possible attack or urban disruption.

In order to implement Phase I, the Task Group recommended the following factors for ranking VHA facilities for their criticality:

- ◆ *Criticality of Function* describes the importance of the facility's function in terms of the overall VA mission.
- ◆ *Location of Facility* considers the possibility of adjacent threats from nearby non-VA targets and the community in general.
- ◆ *Habitation of Facility* describes the ambulatory capabilities of the facility's occupants.
- ◆ *Involvement in Community Disaster Operations* considers the facility's involvement in related community facility/disaster recovery activities.
- ◆ *Continuity of Operations* describes the allowable time for returning the facility to operational capability.
- ◆ *Critical External Commitments* identifies critical elements or facility roles of a special or national nature.

These factors are quantified and the result of the analysis is a ranking of VA facilities in terms of their criticality.

In **Phase II** additional physical information on VA facilities compiled from building condition, security, and other existing VA databases are used to further rank the critical VA facilities based on their potential vulnerabilities.

The following data is used to define the overall vulnerability of critical facilities in order to produce a ranked list for on-site physical assessments:

- ◆ Facility population
- ◆ Number of floors
- ◆ Number of acres
- ◆ Distance to fire station
- ◆ Power supply
- ◆ Mechanical equipment access
- ◆ Closed Circuit TVs
- ◆ Intrusion detection system
- ◆ Barriers
- ◆ External lighting
- ◆ Armed officers
- ◆ Adjacent threats
- ◆ Parking

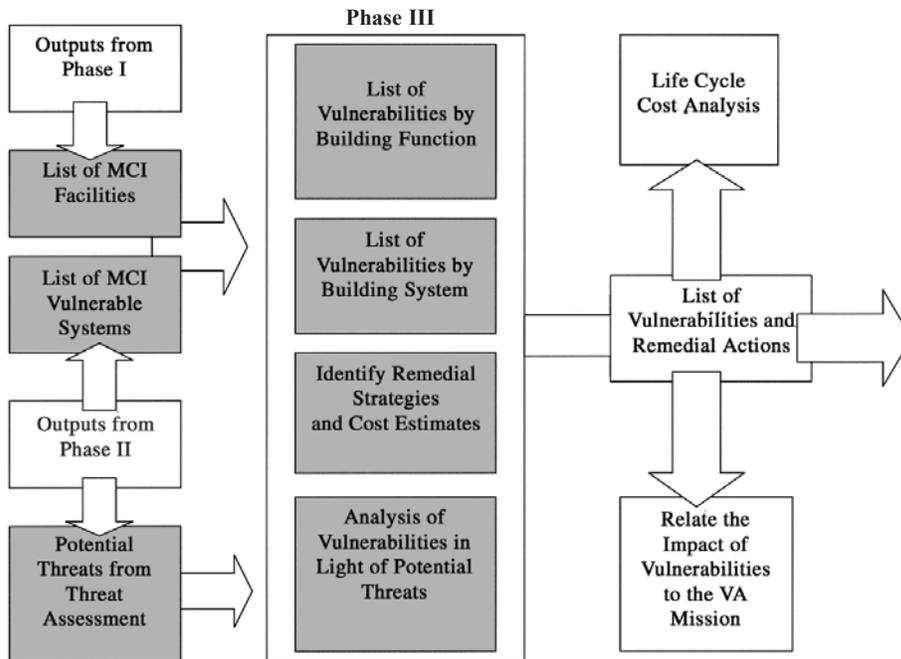
Assumptions are made on the probability of harmful activity against a given asset. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability, intention, and lethality of a situation. The threats that have been identified for VA facilities by the Task Group include accidents, contamination, criminal activity, cyber attack, patient assault, public mass hysteria, natural disasters, power outage, systems failures, terrorist acts, collateral damage, and war.

Information on the core functions of each facility and building system (site, utility, structural, envelope, interior, transportation, mechanical, electrical, fire protection, life safety, and security) are made as to the likelihood or probability of the event, the severity of impact or consequences of the event, and the extent of mitigation or redundancy found in the existing facility.

The analysis of these risk factors (probability, impact, and mitigation) results in assigning each individual facility and its core functions a numerical vulnerability ranking that takes into account both high-risk core functions and building systems for specific threats. The critical facilities are ranked for the implementation of facility assessments.

In **Phase III** high risk VA facilities and their respective at-risk building systems would receive physical security facility assessments. A facility assessment is a systematic process to consider the likelihood that a threat will harm an asset and to identify actions to reduce the vulnerability and mitigate the consequences on an attack.

The objective of the physical security assessments is to identify shortcomings in physical security of the specific facility in order to identify and estimate the cost of mitigation of these shortcomings to reduce the opportunity to disrupt or destroy the ability of the facility to perform the VA mission. The Task Group recommended the



The Vulnerability Assessment Process

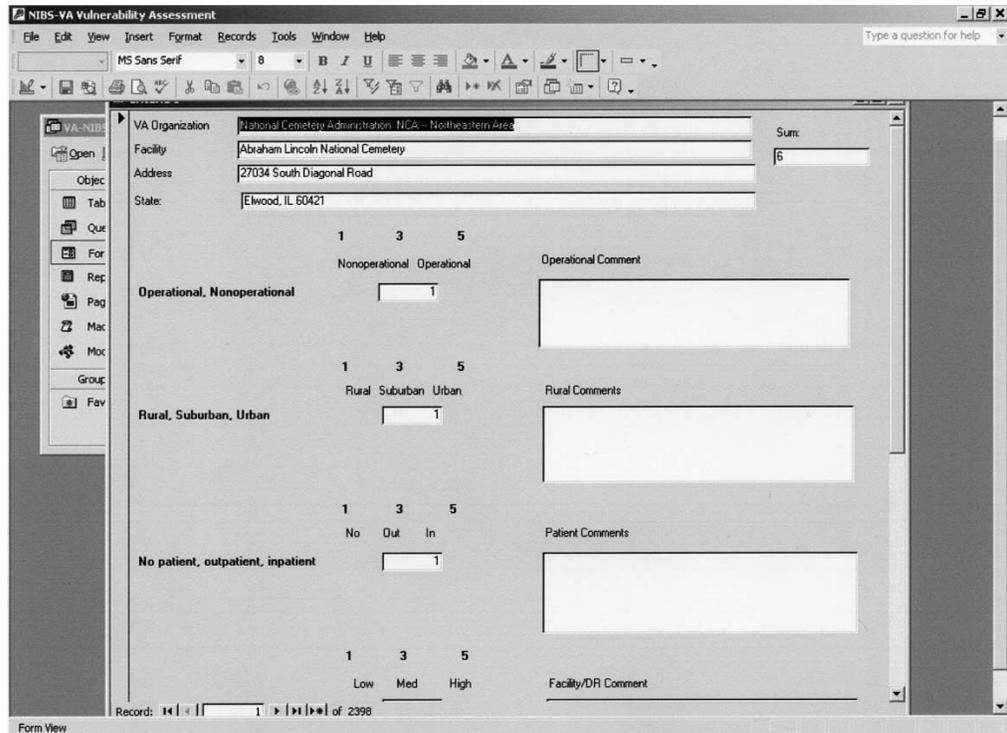
procedures and guidance for the physical security assessments located in the appendices of this report.

The assessment team assigned to a particular VA facility would develop a specific checklist prior to the assessment visit. The checklist would be prepared based on the following elements:

- ◆ Type of facility;
- ◆ Vulnerable functions and building systems as determined by the Phase II analysis; and
- ◆ Specific threat environment as determined by the Phase II analysis.

A master checklist for the following facility infrastructure components is included in the appendices to be used for guidance by the assessment team in preparing the specific facility assessment checklist:

- ◆ Site;
- ◆ Architectural;
- ◆ Structural Systems;
- ◆ Building Envelope;
- ◆ Utility/Mechanical/Plumbing/Electrical Systems; and
- ◆ Security Systems and Security Master Plan.



Phase I Define Criticality

The assessment team would evaluate at-risk facility core functions and building systems, determining and recommending remedial solutions for vulnerable elements in order to provide continued operation of the facility. Cost estimate and time schedules would be documented for the remedial mitigation recommendations. The following life cycle costs would be determined for each recommendation:

- ◆ First costs
- ◆ Replacement costs
- ◆ Operational costs
- ◆ Maintenance costs
- ◆ New staffing requirements

A life cycle cost analysis would be performed on the identified remedial actions in order to prioritize a list of cost effective recommendations for the assessed facility.

The Task Group recommended that the process first be tested on a small number of facilities to fully document assessment cost and schedule requirements in order to develop a complete implementation plan for Phase III.

Microsoft Excel - NIBS-VA Vulnerability Assessment MTC 6-7-02

	A	B	C	D	E	F	G	H
1								
2	Risk Factors definitions							
3		Low	Med	High				
4	Likelihood/probability of event	1	3	5	Low Risk	3-5		
5		Min		Severe	Medium Risk	7-10		
6	Impact/consequence of event	1	3	5	High Risk	11-15		
7								
8	Mitigations/Redundencies	Multiple		Minimal				
9		1	3	5				
10								
11	Facility	Baltimore VA Hospital						
12								
13			MCI	Accidents	Contamination	Criminal Activity	Cyber Attack	Patient Assault
14	Critical Infrastructure		(Spills, floods)	(Food, drug, water)	(Arson, Rape, Robbery)	(IA, Hacking)	(Staff, Dr., Infrastructure)	(Civ
262								
263	Security Systems		3		3		3	9
264								
265	Patient Monitoring/Abduction		3		3		3	9
266		Likelihood	1		1		1	5
267		Impact	1		1		1	3
268		Mitigation	1		1		1	1
269	Biometric Access Control		3		3		3	9
270		Likelihood	1		1		1	5
271		Impact	1		1		1	3
272		Mitigation	1		1		1	1
273	Card Key Control		3		3		3	9
274		Likelihood	1		1		1	5
275		Impact	1		1		1	3
276		Mitigation	1		1		1	1
277	Metal Detection		3		3		3	9
278		Likelihood	1		1		1	5
279		Impact	1		1		1	3

Phase II Identify Vulnerabilities (Building Systems)

Microsoft Excel - NIBS-VA Vulnerability Assessment MTC 6-7-02

	A	B	M	N	O	P
1						
2	Risk Factors definitions					
3		Low	Med	High		
4	Likelihood/probability of event	1	3	5		
5		Min		Severe		
6	Impact/consequence of event	1	3	5		
7						
8	Mitigations/Redundencies	Multiple		Minimal		
9		1	3	5		
10						
11	Facility	Baltimore VA Hospital				
12						
13	Core Process/Function		Terrorist Act	Collocated Damage	War	
42	Day Care		(Chem, Bio, Radiological, Explosive)	(IRS, DOJ, Port, etc)	(Direct, EMP)	
43		Likelihood	3	3	3	6
44		Impact	5	3	3	2
45		Mitigation	3	5	5	2
46	Clinical Laboratory		11	11	11	6
47		Likelihood	3	3	3	2
48		Impact	5	3	3	2
49		Mitigation	3	5	5	2
50	Research Laboratory		11	11	11	6
51		Likelihood	3	3	3	2
52		Impact	5	3	3	2
53		Mitigation	3	5	5	2
54	Cemetary		5	5	5	8
55		Likelihood	1	1	1	1
56		Impact	2	2	2	5
57		Mitigation	2	2	2	2
58	In-patient care		11	11	11	6
59		Likelihood	3	3	3	1
60		Impact	5	3	3	3

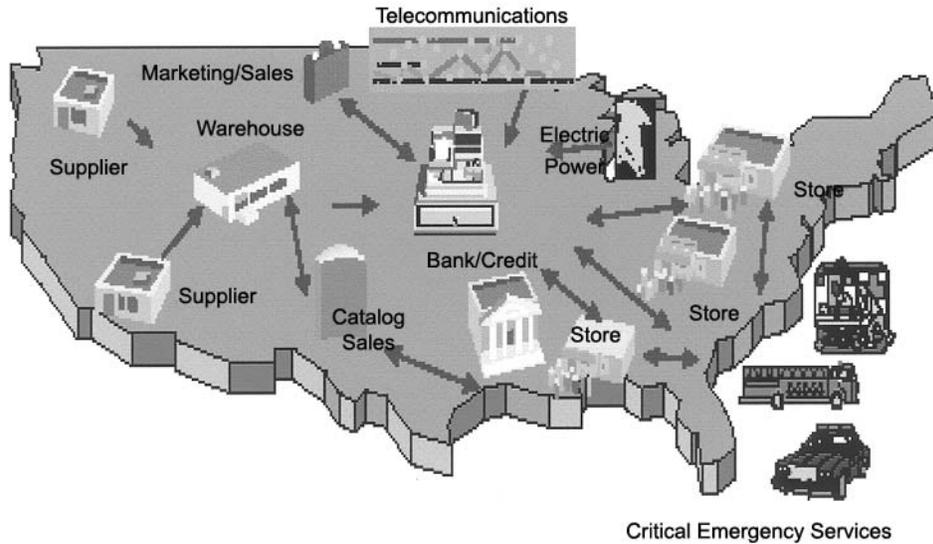
Phase II Identify Vulnerabilities (Core Functions)

RECOMMENDATION**2:** **Critical Facilities****IDENTIFY THOSE FACILITIES THAT MUST REMAIN OPERATIONAL DURING PERIODS OF EMERGENCY AND NATIONAL CRISIS AND SPECIFIC PROTECTION STRATEGIES FOR THESE FACILITIES.**

Executive Order 13010, issued in 1996, emphasized eight critical infrastructures whose services are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures are:

- ◆ Electrical Power
- ◆ Gas and Oil Production, Storage, and Delivery
- ◆ Telecommunications
- ◆ Banking and Finance
- ◆ Water Supply Systems
- ◆ Transportation
- ◆ Government Operations
- ◆ Emergency Services

Emergency services are the critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies.



The Nation's Critical Infrastructure

The Task Group identified critical VA facilities as those facilities that must remain mission operational during periods of emergencies or national crisis and should function at significantly higher levels of protection than those provided by current federal or industry requirements. Examples of those facilities include:

- ◆ Acute Healthcare Facilities
- ◆ Emergency Command Centers
- ◆ Consolidated or unique VA Benefits Centers providing continuity of services
- ◆ Unique VA Administrative Centers providing continuity of operations
- ◆ National Cemeteries providing continuity of operations functions and national support

RECOMMENDATION**3:** **Short-Term Protection Strategies****INVESTIGATE MAJOR PROTECTION STRATEGIES TO NEW AND EXISTING VA FACILITIES TO IMPROVE THEIR SHORT-TERM PROTECTION DURING EMERGENCIES AND NATIONAL CRISES.**

There are several major strategies that should be investigated for application to new and existing VA facilities where applicable and cost justified. These protection strategies when appropriately applied to new designs may reduce or eliminate future costs and should be investigated for integration into existing buildings when mission and cost justified.

- ◆ *Review Points of Vulnerability* to ensure limited access, physical control, and surveillance of electrical, water and other utility distribution, boiler plant, hazardous materials and other vulnerable systems.
- ◆ *Maximize Standoff Distance* to allow for the accommodation of exterior protection strategies and mitigate adjacencies to non-VA properties that are potential targets of large-scale threats.
- ◆ *Prevent Building Collapse* by providing structural system continuity and redundancy among structural system components.
- ◆ *Minimize Hazardous Flying Debris from Blast* by providing for enhanced window and exterior wall components designed as an integrated system.
- ◆ *Provide Effective Building Layout* to minimize vulnerabilities and increase the use of protection strategies.



Point of Vulnerability

- ◆ *Provide Decentralized, Modular, and Redundant Building Systems* in order to maximize the potential for continuity of operations of critical building systems during and/or immediately following an emergency.
- ◆ *Limit Potential Airborne Contamination* through the effective design of HVAC systems.



Potential Airborne Contamination

RECOMMENDATION**4:** **Security Criteria**

REVIEW AND CONTINUE TO REVIEW STATE-OF-THE-ART FEDERAL AND PRIVATE SECTOR BUILDING SECURITY CRITERIA AND DOCUMENT PATTERNS AND TRENDS IDENTIFIED DURING THE FACILITY ASSESSMENTS IN ORDER TO DEVELOP, MAINTAIN, AND AMEND POLICIES, GUIDANCE, AND DESIGN CRITERIA FOR THE PROTECTION OF VA FACILITIES.

The Task Group recommends that VA continually review security criteria developed by other federal agencies, specifically DoD and GSA. Although not specifically healthcare related, there are a number of recent security criteria developed by federal agencies, including:

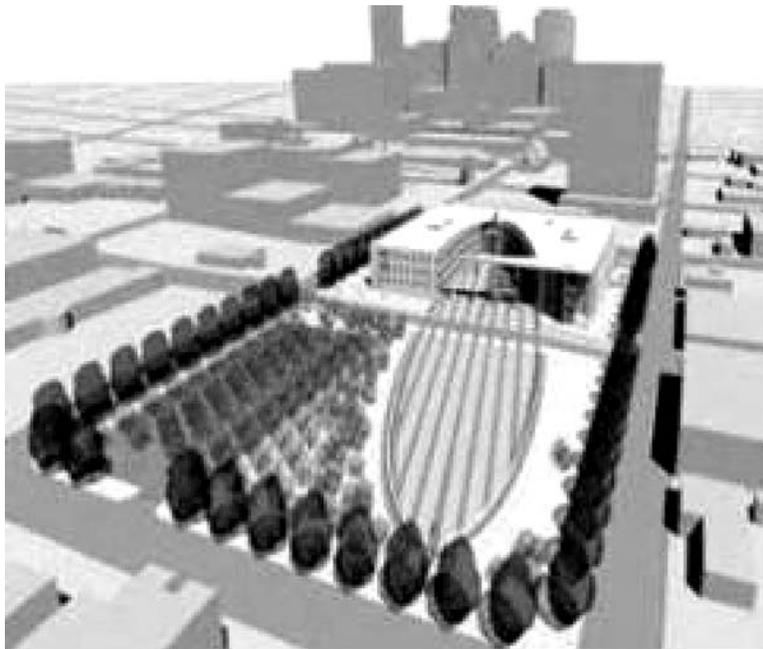
- ◆ General Services Administration *Facilities Standards for the Public Building Service (November 2000)*
- ◆ Interagency Security Committee (ISC) *Security Design Criteria (28 May 2001)*
- ◆ U.S. Army Corps of Engineers *Protecting Buildings and Their Occupants From Airborne Hazards (October 2001)*
- ◆ Department of Health and Human Services *Guidance for Protecting Building Environments from Airborne Chemical, Biological or Radiological Attacks (May 2002)*

- ◆ Department of Defense *Minimum Antiterrorism Standards for Buildings* (08 May 8 2002)
- ◆ National Capital Planning Commission's *National Capital Urban Design and Security Plan* (July 2002)

There are currently no existing federal security criteria that specifically meet the complex requirements of healthcare environments. Several related private sector associations have been developing security related criteria including:

- ◆ American Society of Hospital Engineers (ASHE)
- ◆ American Society for Industrial Security (ASIS)
- ◆ International Association for Healthcare Safety & Security (IAHSS).

Trends and patterns emanating from the on-site security assessments will most likely lead to the creation of new criteria. There is a need to continually monitor and update developed criteria.



New Oklahoma City Federal Building designed using state-of-the-art security criteria.

RECOMMENDATION**5:** **Facility Assessment Teams**

FORM AND TRAIN PHYSICAL SECURITY FACILITY ASSESSMENT TEAMS COMPOSED OF MEMBERS WITH HIGH LEVELS OF EXPERTISE IN ARCHITECTURE, CIVIL/STRUCTURAL ENGINEERING, MECHANICAL/ELECTRICAL ENGINEERING, SECURITY OPERATIONS/SYSTEMS ENGINEERING, CHEMICAL-BIOLOGICAL-RADIOLOGICAL SPECIALTIES, AND COST ESTIMATION TO CONDUCT VA FACILITY ASSESSMENTS.

The Task Group recommended that the teams that are used to conduct the facility assessments should be composed of members with security expertise in the following areas:

- ◆ Architecture/Site Design
- ◆ Civil/Structural Engineering
- ◆ Mechanical/Electrical Engineering
- ◆ Security Operations/Systems Engineering
- ◆ Chemical-Biological-Radiological Specialties
- ◆ Cost Estimating

While the Task Group agreed on the need for an Information Technologist, it decided there was no need to include one on the assessment team



Security Assessment Team

because VA has a concurrent project to explore the protection of its information systems and data bases.

The Task Group recommended that the assessment teams utilize qualified experts to ensure that the evaluations are uniform and unbiased, particularly recognizing the need for a skilled evaluation of the cost effective prioritization of facility protection strategies to be implemented. The assessment teams would be augmented with appropriate VA facility staff to provide a range of specialized support, especially in healthcare facility operation and management. All assessments should be reviewed at headquarters prior to implementing remediation activities to ensure that system-wide priorities are considered.

The Task Group felt there is a need for a detailed agenda and training program for the assessment team site visits. Prior to the site assessment, the team should send a specific agenda and pre-assessment forms so on-site staff can have the necessary local VA staff available and have the necessary documentation prepared to assist in the assessment. Uniform training requirements provide for more consistent assessments among teams and over time, and offer the opportunity to calibrate assessments to reach conclusions on an agency-wide basis.

RECOMMENDATION

6: Protection Requirements

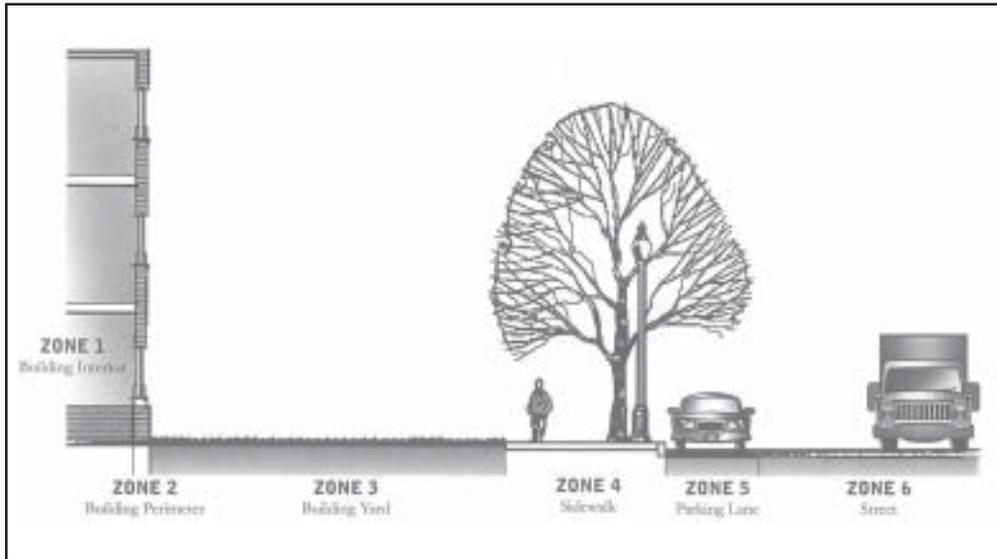
PROVIDE A SAFE ENVIRONMENT AND MINIMIZE THE POSSIBILITY OF MASS CASUALTIES IN ALL VA FACILITIES BY ADOPTING THE LEVELS OF PROTECTION REQUIREMENTS IN ACCORDANCE WITH THE DEPARTMENT OF DEFENSE *MINIMUM ANTITERRORISM STANDARDS FOR BUILDINGS.*

Comprehensive protection against the range of possible threats to all VA facilities may be cost prohibitive, but an appropriate level of protection can be provided for all VA personnel and patients at a reasonable cost.

The intent for all VA facilities is to provide a safe environment and minimize the possibility of mass casualties in buildings or portions of buildings owned, leased, or otherwise occupied by VA. Incorporating these protection measures into VA facilities is least expensive at the time those buildings are either being designed and constructed or are undergoing major renovation, repair, or modification. The costs associated with this level of protection are assumed to be less than the physical and incalculable costs associated with incurring mass casualties.

The Task Group recommended that all occupied VA facilities be brought into conformance with the levels of protection guidance presented in the Department of Defense *Minimum Antiterrorism Standards for Buildings* (08 May 2002).

VA facilities designated as critical must be designed to higher levels of protection as documented in Recommendation 3 of this report.



Building Security Zones

RECOMMENDATION**7:** **Construction Documents**

DEVELOP POLICIES AND GUIDANCE FOR THE PREPARATION AND SECURITY OF CONSTRUCTION DOCUMENTS INCLUDING DESIGN DRAWINGS, SPECIFICATIONS, SYSTEM AND EQUIPMENT DRAWINGS, AS-BUILT DRAWINGS, AND FACILITY ASSESSMENTS TO IMPROVE THE PROTECTION OF VA FACILITIES AND THE SAFEGUARDING OF THE DOCUMENTATION.

The Task Group recognized the need to develop policies and guidance documents for the preparation of drawings, specifications, and system/equipment selection in order to provide protective strategies to VA facilities. VA design guides, design manuals, equipment guide lists, design details, and guide specifications should be revised to incorporate security enhancements. New security vulnerabilities dictate VA require actual as-built construction drawings from their general contractors at occupancy of the facility and VA continue to update the drawings during the life of the facility.

As-built construction drawings that reflect the actual construction of the facility are an integral part of future security assessments and continued operation of the facility in case of a large-scale emergency. These drawings must be actively maintained to reflect current conditions of the facility. Current and accurate system diagrams and labeling protocols should be provided to ensure rapid response actions in case of an emergency.

Policies for the security of facility documentation including drawings, specifications, equipment plans, operating and maintenance plans and manuals, and field assessments should be secured so that only VA staff and contractors with a need to know the information be allowed to access it, records should be kept of those who receive the information, and the information should be safeguarded during and after use.



Production of construction documents

RECOMMENDATION**8:** **Construction Activities**

DEVELOP POLICIES AND GUIDANCE FOR THE PHYSICAL SECURITY OF THE NEW AND RETROFIT CONSTRUCTION ACTIVITIES OF VA FACILITIES AND PORTIONS OF VA FACILITIES THAT TAKE INTO CONSIDERATION THE POTENTIAL THREAT EMERGENCIES AND NATIONAL CRISIS.

The Task Group observed that there is currently no specific security guidance for VA building construction and renovation activities. The need to secure and make safe portions of critical facilities under renovation is a major requirement for total facility protection. In addition there is a need to develop and implement policies and procedures to ensure safe and secure construction activities and sites during large-scale emergencies.

It is critical to provide enough detail in contract specifications to ensure that contractors understand VA's requirements on security issues, allow for the increased costs to cover strict security precautions, and employ effective risk management strategies.

A new or renovation construction project often requires that workers have access to high-risk or sensitive areas of a facility. Notification, access, and supervision procedures should be developed and implemented.

The Task Group recommended that VA undertake the implementation of a construction security program to include the development of on-site construction security policies, procedures, and construction specifications.



Construction activities



Renovation activities

RECOMMENDATION**9: Operations and Maintenance****DEVELOP FACILITY OPERATION AND MAINTENANCE POLICIES AND GUIDANCE TO PROVIDE FOR PROCEDURES AND PRACTICES THAT ENSURE THE CONTINUED SAFE OPERATION OF THE PHYSICAL PLANT AND SECURITY SYSTEMS OF VA FACILITIES DURING EMERGENCIES AND NATIONAL CRISIS.**

The Task Group observed that there is currently no specific security guidance for building operations and maintenance (O&M). A number of examples were identified in which O&M procedures or lack thereof were impacted during security alerts. While the Task Group noted that this recommendation is not a forum for developing O&M procedures, O&M procedures should be recognized and identified in the conduct of the activity.

Procedures and preventive maintenance schedules should be implemented for maintaining physical plant and security systems. This is critical to ensure that protection and mitigation systems operate as intended in case of an emergency. Periodic training of operation and maintenance staff in system operation and maintenance should be conducted. The training should include procedures to be followed in the event of a large-scale emergency. Training should also cover health and safety aspects for maintenance personnel.

Policies, plans, and procedures for building operation and maintenance provide an opportunity for cost saving strategies for the implementation and maintenance of security protection in VA facilities.



Building operations and maintenance



Building equipment maintenance

APPENDICES

I. VULNERABILITY ASSESSMENT PROCESS

II. FACILITY ASSESSMENT CHECKLIST

III. FACILITY ASSESSMENT REPORT OUTLINE

IV. GLOSSARY

V. SELECTED BIBLIOGRAPHY

VI. TASK GROUP and PROJECT TEAM BIOGRAPHIES

APPENDIX I: VULNERABILITY ASSESSMENT PROCESS

The vulnerability assessment process is contained on the accompanying diskette.

APPENDIX II: FACILITY ASSESSMENT CHECKLIST

The facility assessment checklist does not specifically address building code, life safety, or HAZMAT requirements for the facility which are currently conducted through other existing VA evaluation procedures.

PHYSICAL SECURITY FACILITY ASSESSMENT CHECKLIST	
1.	Site
2.	Architectural
3.	Structural Systems
4.	Building Envelope
5.	Utility Systems
6.	Mechanical Systems
7.	Plumbing and Medical Gas Systems
8.	Electrical Systems
9.	Fire Alarm Systems
10.	Communications and Information Technology Systems
11.	Equipment Operations and Maintenance
12.	Security Systems
13.	Security Master Plan

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
1 Site			
1.1	What major structures surround the facility?		
1.2	What are the site access points to the facility?		
1.3	What are the existing types of anti-ram devices for the facility?		
1.4	What is the anti-ram buffer zone standoff distance from a building to unscreened vehicles or parking?	<i>Anti-ram protection may be provided by adequately designed: bollards, street furniture, sculpture, landscaping, walls and fences.</i>	
1.5	Are perimeter barriers capable of stopping vehicles?	<i>If the recommended distance is not available consider structural hardening, perimeter barriers and parking restrictions; relocation of vulnerable functions within or away from the building; operational procedures, acceptance of higher risk.</i>	
1.6	Does site circulation prevent high-speed approaches by vehicles?		
1.7	Are there offsetting vehicle entrances from the direction of a vehicle's approach to force a reduction of speed?		
1.8	Is there space for inspection at the curb line or outside the protected perimeter? What is the minimum distance from the inspection location to the building?	<i>Design features for the vehicular inspection point include: vehicle arrest devices that prevent vehicles from leaving the vehicular inspection area and prevent tailgating. If screening space cannot be provided, other design features such as: hardening and alternative space for inspection.</i>	
1.9	In dense, urban areas, does curb lane parking place uncontrolled parked vehicles unacceptably close to a facility in public rights-of-way?	<i>Where distance from the building to the nearest curb provides insufficient setback, restrict parking in the curb lane. For typical city streets this may require negotiating to close the curb lane.</i>	
1.10	Is there a minimum setback distance between the building and parked vehicles?	<i>Adjacent public parking should be directed to more distant or better-protected areas, segregated from employee parking and away from the facility.</i>	
1.11	Does adjacent surface parking maintain a minimum standoff distance?	<i>Parking within _____ feet of the building shall be restricted to authorized vehicles.</i>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
1.12	Do stand-alone, above ground parking facilities provide adequate visibility across as well as into and out of the parking facility?	<p><i>Pedestrian paths should be planned to concentrate activity to the extent possible.</i></p> <p><i>Limiting vehicular entry/exits to a minimum number of locations is beneficial.</i></p> <p><i>Stair tower and elevator lobby design shall be as open as code permits.</i></p> <p><i>Stair and/or elevator waiting area should be as open to the exterior and/or the parking areas as possible.</i></p> <p><i>Potential hiding places below stairs should be closed off; nooks and crannies should be avoided.</i></p> <p><i>Elevator lobbies should be well-lighted and visible to both patrons in the parking areas and the public out on the street.</i></p>	
1.13	Are garage or service area entrances for government controlled or employee permitted vehicles that are not otherwise protected by site perimeter barriers protected by devices capable of arresting a vehicle of the designated threat size at the designated speed?		
1.14	Does site landscaping provide hiding places?	<p><i>It is desirable to hold planting away from the facility to permit observation of intruders.</i></p>	
1.15	Is the site lighting adequate from a security perspective in roadway access and parking areas?	<p><i>Security protection can be successfully addressed through adequate lighting. The type and design of lighting including illumination levels is critical. IESNA guidelines can be used.</i></p>	
1.16	Is a perimeter fence or other types of barrier controls in place?		
1.17	Do signs provide control of vehicles and people?		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
2 Architectural			
2.1	Does the site planning and architectural design incorporate strategies from a crime prevention through environmental design (CPTED) perspective?	<i>The focus of CPTED is on creating defensible space by employing natural access controls, natural surveillance and territorial reinforcement to prevent crime and influence positive behavior, while enhancing the intended uses of space. Examples of CPTED attributes include spatial definition of space to control vehicle and pedestrian circulation patterns, placement of windows to reinforce surveillance, defining public space from private/restricted space through design of lobbies, corridors, door placement, pathway and roadway placements, walls, barriers, signage, lighting, landscaping, separation and access control of employee/visitor parking areas, etc.</i>	
2.2	Is it a mixed-tenant facility?	<i>High-risk tenants should not be housed with low-risk tenants. High-risk tenants should be separated from publicly accessible areas. Mixed uses may be accommodated through such means as separating entryways, controlling access, and hardening shared partitions, as well as through special security operational counter-measures.</i>	
2.3	Are public toilets, service spaces or access to vertical circulation systems located in any non-secure areas, including the queuing area before screening at the public entrance?		
2.4	Are areas of refuge identified, with special consideration given to egress?		
2.5	Are loading docks and receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances including electrical, telephone/data, fire detection/ alarm systems, fire suppression water mains, cooling and heating mains, etc.?	<i>Loading docks should be located so that vehicles will not be driven into or parked under the building. If loading docks are in close proximity to critical equipment, the service shall be hardened for blast.</i>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
2.6	<p>Are mailrooms located away from facility main entrances, areas containing critical services, utilities, distribution systems, and important assets?</p> <p>Does the mailroom have adequate space for explosive disposal containers?</p> <p>Is the mailroom located near the loading dock?</p>	<p><i>The mailroom should be located at the perimeter of the building with an outside wall or window designed for pressure relief.</i></p>	
2.7	<p>Is space available for equipment to examine incoming packages and for special containers?</p>	<p><i>Off-site screening stations may be cost effective, particularly if several buildings may share one mailroom.</i></p>	
2.8	<p>Are critical building components located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, interior parking?</p>	<p><i>Critical building components include: Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; Normal fuel storage; Main switchgear; Telephone distribution and main switchgear; Fire pumps; Building control centers; UPS systems controlling critical functions; Main refrigeration systems if critical to building operation; Elevator machinery and controls; Shafts for stairs, elevators, and utilities; Critical distribution feeders for emergency power. Evacuation and rescue require emergency systems to remain operational during a disaster and they should be located away from attack locations. Primary and back-up systems should not be co-located.</i></p>	
2.9	<p>Do doors and walls along the line of security screening meet requirements of UL752 "Standard for Safety: Bullet-Resisting Equipment"?</p>		
2.10	<p>Do entrances avoid significant queuing?</p>	<p><i>If queuing will occur within the building footprint, the area should be enclosed in blast-resistant construction. If queuing is expected outside the building, a rain cover should be provided.</i></p>	
2.11	<p>Do public and employee entrances include space for possible future installation of access control and screening equipment?</p>	<p><i>These include walk-through metal detectors and x-ray devices, ID check, electronic access card, and turnstiles.</i></p>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
2.12	Are there trash receptacles and mailboxes in close proximity to the facility that can be used to hide explosive devices?	<i>The size of the trash receptacles and mailbox openings should be restricted to prohibit insertion of packages.</i>	
2.13	Is roof access limited to authorized personnel by means of locking mechanisms?		
2.14	Are stairwells required for emergency egress located as remotely as possible from high-risk areas where blast events might occur?	<i>Stairs should not discharge into lobbies, parking, or loading areas.</i>	
2.15	Are enclosures for emergency egress hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees?		
2.16	Is access control provided through main entrance points for employees and visitors (e.g. by lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control system(s))?		
2.17	Is access to private and public space or restricted area space clearly defined through the design of the space, signage, use of electronic security devices, etc.?		
2.18	Is access to elevators distinguished as to those that are designated only for employees, patients and visitors?		
2.19	Are high value or critical assets located as far into the interior of the building as possible?		
2.20	Is high visitor activity away from assets?		
2.21	Are critical assets located in spaces that are occupied 24 hours per day? Are assets located in areas where they are visible to more than one person?		
2.22	Is interior glazing near high-threat areas minimized?		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
2.23	Do interior barriers differentiate level of security within a facility?		
2.24	Do foyers have reinforced concrete walls and offset interior and exterior doors from each other?		
2.25	Does the circulation routes have unobstructed views of people approaching controlled access points?		
2.26	Are pedestrian paths planned to concentrate activity to aid in detection?		
2.27	Are ceiling and lighting systems designed to remain in place during emergencies?		
3 Structural Systems			
3.1	What type of construction? What type of concrete & reinforcing steel? What type of steel? What type of foundation?	<p><i>The type of construction provides an indication of the robustness to abnormal loading and load reversals. Reinforced concrete moment resisting frame provides greater ductility and redundancy than a flat-slab or flat-plate construction. The ductility of steel frame with metal deck depends on the connection details and pre-tensioned or post-tensioned construction provides little capacity for abnormal loading patterns and load reversals. The resistance of load-bearing wall structures varies to a great extent, depending on whether the walls are reinforced or unreinforced. A rapid screening process developed by FEMA for assessing structural hazard identifies the following types of construction with a structural score ranging from 1.0 to 8.5. The higher the score indicates a greater capacity to sustain load reversals.</i></p> <p>Wood buildings of all types - 4.5 to 8.5 Steel moment resisting frames - 3.5 to 4.5 Braced steel frames - 2.5 to 3.0 Light metal buildings - 5.5 to 6.5 Steel frames with cast-in-place concrete shear walls - 3.5 to 4.5</p>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
		Concrete moment resisting frames - 2.0 to 4.0 Concrete shear wall buildings - 3.0 to 4.0 Concrete frame with unreinforced masonry infill walls - 1.5 to 3.0 Steel frame with unreinforced masonry infill walls - 1.5 to 3.0 Tilt-up buildings - 2.0 to 3.5 Precast concrete frame buildings - 1.5 to 2.5 Reinforced masonry -3.0 to 4.0 Unreinforced masonry - 1.0 to 2.	
3.2	Do the reinforced concrete structures contain symmetric steel reinforcement (positive and negative faces) in all floor slabs, roof slabs, walls, beams and girders that may be subjected to rebound, uplift and suction pressures? Do the lap splices fully develop the capacity of the reinforcement? Are lap splices and other discontinuities staggered? Do the connections possess ductile details? Does special shear reinforcement, including ties and stirrups, available to allow large post-elastic behavior?		
3.3	Are the steel frame connections moment connections? Are the column spacing minimized so that reasonably sized members will resist the design loads and increase the redundancy of the system? What are the floor-to-floor heights?		
3.4	Are critical elements vulnerable to failure?	<p><i>The priority for upgrades should be based on the relative importance of structural or non-structural elements that are essential to mitigating the extent of collapse and minimize injury and damage.</i></p> <p><i>Primary Structural Elements provide the essential parts of the building's resistance to cata-</i></p>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
		<p><i>strophic blast loads and progressive collapse. These include columns, girders, roof beams, and the main lateral resistance system;</i></p> <p><i>Secondary Structural Elements consist of all other load bearing members, such as floor beams, slabs, etc.;</i></p> <p><i>Primary Non-Structural Elements consist of elements (including their attachments) which are essential for life safety systems or elements which can cause substantial injury if failure occurs, including ceilings or heavy suspended mechanical units; and</i></p> <p><i>Secondary Non-Structural Elements consist of all elements not covered in primary non-structural elements, such as partitions, furniture, and light fixtures.</i></p>	
3.5	<p>Will the structure suffer an unacceptable level of damage resulting from the postulated threat?</p>	<p><i>The extent of damage to the structure and exterior wall systems from the bomb threat may be related to a protection level:</i></p> <p><i>Low and Medium/Low Level Protection - Major damage. The facility or protected space will sustain a high level of damage without progressive collapse. Casualties will occur and assets will be damaged. Building components, including structural members, will require replacement, or the building may be completely unrepairable, requiring demolition and replacement.</i></p> <p><i>Medium Level Protection - Moderate damage, repairable. The facility or protected space will sustain a significant degree of damage, but the structure should be reusable. Some casualties may occur and assets may be damaged. Building elements other than major structural members may require replacement.</i></p> <p><i>Higher Level Protection - Minor damage, repairable. The facility or protected space may globally sustain minor damage with some</i></p>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
		<p><i>local significant damage possible. Occupants may incur some injury, and assets may receive minor damage.</i></p>	
3.6	<p>Is the structure vulnerable to progressive collapse?</p> <p>Is the facility capable of sustaining the removal of a column for one floor above grade at the building perimeter without progressive collapse?</p> <p>In the event of an internal explosion in an uncontrolled public ground floor area (such as lobbies, loading docks and mailrooms) does the design prevent progressive collapse due to the loss of one primary column or does the design preclude such a loss?</p> <p>Do architectural or structural features provide a minimum 6-inch standoff to the internal columns?</p> <p>Are the columns in the unscreened internal spaces designed for an unbraced length equal to two floors, or three floors where there are two levels of parking?</p>	<p><i>Design to mitigate progressive collapse is an independent analysis to determine a system's ability to resist structural collapse upon the loss of a major structural element or the system's ability to resist the loss of a major structural element. Design to mitigate progressive collapse may be based on the methods outlined in ASCE 7-98. Designers may apply static and/or dynamic methods of analysis to meet this requirement and ultimate load capacities may be assumed in the analyses. Existing buildings should not be retrofitted to prevent progressive collapse unless they are undergoing a structural renovation, such as a seismic upgrade. Existing facilities may be retrofitted to withstand the design level threat or to accept the loss of a column for one floor above grade at the building perimeter without progressive collapse.</i></p>	
3.7	<p>Are there adequate redundant load paths in the structure?</p>	<p><i>Special consideration should be given to materials which have inherent ductility and which are better able to respond to load reversals such as cast in place reinforced concrete and steel construction.</i></p> <p><i>Careful detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads. Primary vertical load carrying members shall be protected where parking is inside a facility and the building superstructure is supported by the parking structure.</i></p>	
3.8	<p>Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?</p>	<p><i>The floor of the loading dock does not need to be designed for blast resistance if the area below is not occupied and contains no critical utilities.</i></p>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
3.9	<p>Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?</p>	<p><i>Where mailrooms and unscreened retail spaces are located in occupied areas or adjacent to critical utilities, walls, ceilings, and floors, they should be blast and fragment resistant.</i></p> <p><i>Methods to facilitate the venting of explosive forces and gases from the interior spaces to the outside of the structure may include blow-out panels and window system designs that provide protection from blast pressure applied to the outside but that readily fail and vent if exposed to blast pressure on the inside.</i></p>	
3.10	<p>Are there transfer girders that are supported by columns within unscreened public spaces or at the exterior of the building?</p>		
<p>4 Building Envelope</p>			
4.1	<p>To what level are the exterior Walls designed to provide less than a high hazard response?</p> <p>Are the walls capable of withstanding the dynamic reactions from the windows?</p>	<p><i>The performance of the façade varies to a great extent on the materials. Different construction includes brick or stone with block back-up, steel stud walls, precast panels, curtainwall with glass, stone or metal panel elements. The performance of the glass will similarly depend on the materials. Glazing may be single pane or double pane, monolithic or laminated, annealed, heat strengthened or fully tempered. Shear walls that are essential to the lateral and vertical load bearing system, and that also function as exterior walls, shall be considered primary structures and shall resist the actual blast loads predicted from the threats specified. Where exterior walls are not designed for the full design loads, special consideration shall be given to construction types that reduce the potential for injury. As a minimum goal, the window systems should be designed so that at least __ % of the total glazed areas of the facility meet the specified performance conditions when subjected to the defined threats.</i></p>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
4.2	<p>Is there less than 40 % fenestration openings per structural bay?</p> <p>Are the window systems design (glazing, frames, anchorage to supporting walls, etc.) on the exterior facade balanced to mitigate the hazardous effects of flying glazing following an explosive event?</p> <p>Do the glazing systems with a 1/2-inch bite contain an application of structural silicone?</p> <p>Is the glazing Laminated or is it protected with an anti-shatter film?</p> <p>If an anti-shatter film is used, is it a minimum of a 7-mil thick film, or specially manufactured 4-mil thick film?</p>		
4.3	<p>Do the walls, anchorage, and window framing fully develop the capacity of the glazing material selected?</p> <p>Will the anchorage remain attached to the walls of the facility during an explosive event without failure?</p> <p>Is the façade connected to back-up block or to the structural frame?</p> <p>Are non-bearing masonry walls reinforced?</p>	<p><i>Government produced and sponsored computer programs coupled with test data and recognized dynamic structural analysis techniques may be used to determine whether the glazing either survives the specified threats or the post damage performance of the glazing protects the occupants. A breakage probability no higher than 750 breaks per 1000 may be used when calculating loads to frames and anchorage.</i></p>	
4.4	<p>Does the facility contain ballistic glazing?</p> <p>Does the ballistic glazing meet the requirements of UL 752 Bullet-Resistant Glazing?</p> <p>Does the facility contain security-glazing?</p> <p>Does the security-glazing meet the requirements of ASTM F1233 or UL 972, Burglary Resistant Glazing Material?</p> <p>Do the Window Assemblies containing Forced Entry resistant glazing (excluding the glazing) meet the requirements of ASTM F 588?</p>	<p><i>Glass-clad polycarbonate or laminated polycarbonate are two types of acceptable glazing material.</i></p>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
4.5	<p>Do non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection required for the exterior wall?</p> <p>Are non-window openings, such as mechanical vents and exposed plenums, designed to the level of protection required for the exterior wall?</p>	<p><i>In-filling of blast over-pressures must be considered through non-window openings such that structural members and all mechanical system mountings and attachments should resist these interior fill pressures.</i></p>	
4.6	<p>Is interior glazing shatter resistant?</p>	<p><i>Interior glazing should be minimized where a threat exists and should be avoided in enclosures of critical functions next to high-risk areas.</i></p>	
5 Utility Systems			
5.1	<p>What is the source of domestic water?</p>	<p><i>Critical water supply may be vulnerable. Sources include municipal, wells, storage tank.</i></p>	
5.2	<p>Are there multiple entry points for the water supply?</p>	<p><i>If the facility has only one source of water entering at one location, the entry points should be secure.</i></p>	
5.3	<p>Is the incoming water supply in a secure location?</p>	<p><i>Access to water supply should not be open to non-authorized personnel.</i></p>	
5.4	<p>Does the facility have storage capacity for domestic water? How much?</p>	<p><i>Operational facilities will require reliance on adequate domestic water supply.</i></p>	
5.5	<p>What is the source of water for the fire suppression system?</p>	<p><i>Describe location and number of service entry points. Is the service reliant on the local utility company?</i></p>	
5.6	<p>Are sewer systems protected? Are they accessible?</p>	<p><i>Sanitary and storm water sewers should be protected from unauthorized access and possible contamination.</i></p>	
5.7	<p>What fuel supplies do the facility rely on for critical operation?</p>	<p><i>Typically natural gas, propane, or fuel oil are required for continued operation</i></p>	
5.8	<p>How much fuel is stored on the facility? How is it stored?</p>	<p><i>Fuel storage protection is essential for continued operation.</i></p>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
5.9	Where is the fuel supply obtained? How is it delivered?	<i>The supply of fuel is dependent on the reliability of the supplier.</i>	
5.10	Are there alternate sources of fuel? Can alternate fuels be used?	<i>Critical functions may be served by alternate methods if normal fuel supply is interrupted.</i>	
5.11	What is the normal source of electrical service for the facility?	<i>Utilities are the general source unless co-generation or a private energy provider is available.</i>	
5.12	Is there a redundant electrical service source? Can the facilities be feed from more than one utility substation?	<i>The utility may have only one source of power from a single substation. There may be only single feeders from the main substation.</i>	
5.13	How many service entry points does the facility have for electricity?	<i>Electrical supply at one location creates a vulnerable situation unless alternate source are available.</i>	
5.14	What provisions for emergency power exist?	<i>Describe the emergency power system and its location. Can the utility provide backup power if the normal electrical service is interrupted?</i>	
5.15	Is the incoming electric service to the building secure?	<i>Typically, the service entrance is a locked room, inaccessible to the public.</i>	
5.16	Does the fire alarm system require communication with external sources?	<i>Typically, the local fire department responds to an alarm. Describe how the alarm signal is sent to the responding agency: telephone, radio, etc.</i>	
5.17	By what means does the main telephone and data communications interface the facility?	<i>Typically communication ducts or other conducts are available.</i>	
5.18	Are there multiple or redundant location for the communication service?	<i>Secure locations of communications wiring entry to the facility are required.</i>	
6 Mechanical Systems			
6.1	Where are the air intakes and exhaust louvers for the building?	<i>Describe location and relation to public access. Indicate if intakes are low, high or midpoint of building structure.</i>	
6.2	Are there multiple air intake locations?	<i>Single air intakes may feed several air handling units. Indicate if the air intakes are localized or separated.</i>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
6.3	What are the types of air filtration?	<i>Describe the efficiency and number of filter modules for each of the main air handling systems.</i>	
6.4	Is there space for larger filter assemblies on critical air handling systems?	<i>Air handling units serving critical functions during continued operation may be retrofitted to provide enhanced protection during emergencies.</i>	
6.5	How are the air handling systems zoned?	<i>Describe the areas and functions served by each of the primary air handling systems.</i>	
6.6	Are there large central air handling units or are there multiple units serving separate zones?	<i>Independent units can continue to operate if damage occurs to limited areas of the facility.</i>	
6.7	Are there any redundancies in the air handling system?	<i>Describe if critical areas can be served from other units if a major system is disabled.</i>	
6.8	Is the air supply to critical areas compartmentalized?	<i>Describe if air flow can occur from critical to non-critical areas either through building openings, ductwork, or air handling system.</i>	
6.9	Are supply and exhaust air systems for laboratories secure?		
6.10	What is the method of temperature and humidity control? Is it localized or centralized?	<i>Central systems can range from monitoring only to full control. Local control may be available to override central operation.</i>	
6.11	Where are the control centers and cabinets located? Are they in secure areas? How is the control wiring routed?	<i>Access to any component of the building automation and control system could compromise the functioning of the system.</i>	
6.12	Are there provisions for air monitors or sensors for chemical or biological agents?	<i>Duct mounted sensors are found in limited cases generally in laboratory areas.</i>	
7 Plumbing and Medical Gas Systems			
7.1	What is the method of water distribution?	<i>Central shaft locations for piping are more vulnerable than multiple riser locations.</i>	
7.2	What is the method of medical gas distribution?		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
7.3	Is there redundancy to the main piping distribution?	<i>Looping of piping and use of section valves provide redundancy in the event sections of the system are damaged.</i>	
7.4	What is the method of heating domestic water? What fuel is used?	<i>Single source of hot water with one fuel source is more vulnerable than multiple sources and multiple fuel types.</i>	
7.5	Where are the oxygen and nitrous oxide tanks located? How are they piped to the distribution system?	<i>Describe the locations relative to the facility including any blast protection? Indicate if the distribution piping is above or belowground.</i>	
7.6	Are there reserve supplies of oxygen and nitrous oxide?	<i>Localized gas cylinders could be available in the event of damage to the central tank system.</i>	
8 Electrical Systems			
8.1	How are the electrical rooms secured?	<i>Describe if all primary electrical equipment is located in a secured area.</i>	
8.2	Are critical electrical systems co-located with other building systems?	<i>Indicate those areas where major electrical equipment is co-located with other systems or is located in areas outside secured electrical areas.</i>	
8.3	Are electrical distribution panels secured or in secure locations?	<i>Describe the means of access and location of critical electrical distribution panels serving branch circuits.</i>	
8.4	Does emergency backup power exist for all areas within the facility? How is the emergency power distributed?	<i>Is the emergency power system independent from the normal electrical service, particularly in critical care areas?</i>	
8.5	How is the primary electrical system wiring distributed? Is there redundancy of distribution to critical areas?	<i>Central utility shafts may be subject to damage. Describe if the distribution is co-located with other major utilities and if there are alternate suppliers.</i>	
8.6	What is the extent of the external facility lighting in utility and service areas?	<i>Indicate the amount of exterior lighting particularly in critical areas such as utility and service areas.</i>	
8.7	Are there any transformers or switchgears located outside the building or accessible from the building exterior?	<i>Describe how these devices are secured and if they are vulnerable to public access.</i>	

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
9 Fire Alarm Systems			
9.1	Is the facility fire alarm system centralized or localized?	<i>Describe the main components of the system including methods and extent of annunciation both locally and centrally.</i>	
9.2	Where are the fire alarm panels located?	<i>Indicate the location and accessibility of the panels particularly with regard to access by unauthorized personnel.</i>	
9.3	Is the fire alarm system stand-alone or integrated with other functions such as security and environmental systems?	<i>Describe what interface the fire alarm system has with other building management systems.</i>	
10 Communications and IT Systems			
10.1	Where are communication systems wiring closets located? Are they in secure areas?	<i>Describe if communications closets are independent or if they are co-located with other utilities.</i>	
10.2	How is communications system wiring distributed?	<i>Indicate if wiring systems are in chases or if distribution is in occupied areas.</i>	
10.3	Are there redundant communications systems available?	<i>Critical areas should be supplied with multiple or redundant means of communications.</i>	
10.4	Do the IT systems meet requirements of confidentiality, integrity, and availability?		
10.5	Where is the disaster recovery/ mirroring site?		
10.6	Where is the back-up tape/file storage site and what is the type of safe environment? (safe, vault, underground) Is there redundant refrigeration in the site?		
10.7	Where is the main distribution facility? Where are the secondary and/or intermediate distribution facilities?		
10.8	Where are the routers and firewalls located?		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
10.9	What type, power rating, and location of the UPS? (battery, on-line, filtered)		
10.10	What type and where are the WAN connections?		
10.11	What type and where are the wireless systems (RF, HF, VHG, MW) located?		
10.12	What type of LAN (Cat 5, fiber, Ethernet, Token Ring) is used?		
10.13	What type and where are data centers located?		
11 Equipment Operations and Maintenance			
11.1	Have critical air systems been rebalanced? If so, when and how often?	<i>Rebalancing may only occur during renovation.</i>	
11.2	Is air pressurization monitored regularly?	<i>Some areas required positive or negative pressure to function properly. Pressurization is critical in a hazardous environment or emergency situation.</i>	
11.3	Are there composite drawings indicating location and capacities of major systems? Do updated O&M manuals exist?	<i>Describe if there are composite layout drawings of electrical, mechanical and fire protection systems and the status of latest updates.</i>	
11.4	Does the facility have a policy or procedure for periodic recommissioning of major M/E/P systems?	<i>Recommissioning involves testing and balancing of systems to ascertain their capability to perform as described.</i>	
11.5	Is there an adequate operations and maintenance program including training of facilities management staff?	<i>Describe level of maintenance and operation and the extent of training provided at the facility.</i>	
11.6	What maintenance and service agreements exist for MEP systems?		
12 Security Systems			
	Perimeter Security		
12.1	Are black/white or color CCTV cameras used? Are they analog or digital by design?		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
	<p>What are the number of fixed, wireless and pan-tilt-zoom cameras used?</p> <p>Who are the manufacturers of the CCTV cameras?</p> <p>What is the age of the CCTV cameras in use?</p>	<p><i>Security technology is frequently considered to compliment or supplement security personnel forces and to provide a wider area of coverage. Typically these physical security elements provide the first line of defense in deterring, detecting and responding to threats and vulnerabilities. They must be viewed as an integral component of the overall security program. Their design, engineering, installation, operation and management must be able to meet daily security challenges from a cost effective and efficiency perspective.</i></p>	
12.2	<p>Are the cameras programmed to respond automatically to perimeter building alarm events?</p> <p>Do they have built-in video motion capabilities?</p>	<p><i>Example, if a perimeter door is opened, the closest camera responds and begins surveillance of the area.</i></p>	
12.3	<p>Are panic/duress alarm sensors used, where are they located and are they hardwired or portable?</p>		
12.4	<p>Are intercom call-boxes used in parking areas or along the building perimeter?</p>		
12.5	<p>Are the perimeter cameras supported by an uninterrupted power supply source; battery or building emergency power?</p>		
12.6	<p>What is the quality of video images both during the day and hours of darkness?</p> <p>Are infrared camera illuminators used?</p>		
12.7	<p>What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?</p>		
12.8	<p>What type of camera housings are used and are they environmental in design to protect against exposure to heat and cold weather elements?</p>		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
12.9	Who monitors the CCTV system?		
12.10	What type of exterior IDS sensors are used: electromagnetic, fiber optic, active infrared, bistatic microwave, seismic, photoelectric, ground, fence, glass break (vibration/shock), single, double and roll-up door magnetic contacts or switches.		
12.11	Is a global positioning satellite system (GPS) used to monitor vehicles and asset movements?		
Interior Security			
12.12	<p>Are black/white or color CCTV cameras used?</p> <p>Are they monitored and recorded 24 hours/7 days a week? By whom?</p> <p>Are they analog or digital by design?</p> <p>What are the number of fixed, wireless and pan-tilt-zoom cameras used?</p> <p>Who are the manufacturers of the CCTV cameras?</p> <p>What is the age of the CCTV cameras in use?</p>		
12.13	<p>Are the cameras programmed to respond automatically to interior building alarm events?</p> <p>Do they have built-in video motion capabilities?</p>	<i>Example, if a perimeter door is opened, the closest camera responds and begins surveillance of the area.</i>	
12.14	What are the first costs and maintenance costs associated with the interior cameras?		
12.15	Are their panic/duress alarm sensors used, where are they located and are they hardwired or portable?		
12.16	Are intercom call-boxes or building intercom system used throughout the facility?		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
12.17	Are the interior cameras supported by an uninterrupted power supply source; battery or building emergency power?		
12.18	Is the quality in interior camera video images of good visual and recording quality?		
12.19	Are the camera lenses used of the proper specifications, especially distance viewing and clarity?		
12.20	What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?		
12.21	What type of camera housings are used and are they designed to protect against exposure or tampering?		
12.22	Are magnetometers (metal detectors) and x-ray equipment used and at what locations within the facility?		
12.23	Does a security photo identification badge processing system in place? Does it work in conjunction with the access control system or is it a standalone system?		
12.24	What type of interior IDS sensors are used: electromagnetic, fiber optic, active infrared-motion detector, photoelectric, glass break (vibration/shock), single, double and roll-up door magnetic contacts or switches?		
12.25	Is there a security system in place to protect against infant/patient abductions?		
12.26	Is there a security asset tracking system in place that monitors the movement, control and accountability of assets within and removal from a facility (e.g. electronic tags, bar codes, wire, infrared/black light markings, etched or chemical embedded id number, etc.)?		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
12.27	Is there a holdup-cash register security controls in place that activates upon removal of cash and works in conjunction with other CCTV and related IDS systems?		
12.28	<p>What type of security access control systems is used?</p> <p>Are these same devices used for physical security also used (integrated) with providing access control to security computer networks (e.g. in place of or combination with user id's and system passwords)?</p>		
12.29	What types of access control transmission media is used to transmit access control system signals (same as defined for CCTV cameras)?		
12.30	What is the backup power supply source for the access control systems; battery backup or some form of other uninterrupted power sources?		
12.31	<p>What access control system equipment is used?</p> <p>How old are the systems and what are the related first and maintenance service costs?</p>		
12.32	Are mechanical, electrical, medical gas, power supply, radiological material storage, voice/data telecommunication system nodes, security system panels, elevator and critical system panels, and other sensitive rooms continuously locked, under electronic security CCTV camera and intrusion alarm systems surveillance?		
12.33	What security safeguards are in place to control the movement, custody, accountability and tracking of facility assets?		
12.34	<p>Are their vaults or safes used and are they protected against unauthorized or forced entry?</p> <p>Where are they located?</p>		

PHYSICAL SECURITY ASSESSMENT

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
12.35	<p>What security controls are in place to handle the processing of mail and protect against potential biological, explosive or other threatening exposures?</p>		
12.36	<p>What type of security key management system is in place? How are keys made, issued and accounted for?</p> <p>Who is responsible for key management and the authorized release of them?</p>		
12.37	<p>What types of locking hardware are used throughout the facility?</p> <p>Are manual and electromagnetic cipher, keypad, pushbutton, panic bar, door strikes and related hardware and software used?</p>		
12.38	<p>Are any potentially hazardous chemicals, combustible or toxic materials stored on-site in non-secure and non-monitored areas?</p>		
12.39	<p>Is there a designated security control room and console in place to monitor security, fire alarm and possibly other building systems?</p>		
12.40	<p>Is the security console and control room adequate in size, provide room for expansion, have adequate environment controls (e.g. a/c, lighting, heating, air circulation, backup power, etc.) and is ergonomically designed?</p>		
12.41	<p>Is the location of the security room located in a secure area with limited, controlled and restricted access controls in place?</p>		
12.42	<p>What are the means by which facility and security personnel can communicate with one another: portable radio, pager, cell phone, personal data assistants (PDA's), etc)?</p> <p>What problems have been experienced with these and other electronic security systems?</p>		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
12.43	Is there a computerized security incident reporting system used to prepare reports and track security incident trends and patterns?		
12.44	Does the present security force have access to use a computerized guard tour system?	<i>This system allows for the systematic performance of guard patrols with validation indicators built in. The system notes stations/locations checked or missed, dates and times of such patrols and who conducted them on what shifts. Management reports can be produced for record keeping and manpower analysis purposes.</i>	
Security System Documents			
12.45	Are security system as-built drawings been generated and ready for review?	<i>Critical to the consideration and operation of security technologies its overall design and engineering processes. These historical reference documents outline system specifications and layout security device used, their application, location and connectivity. They are a critical resource tool for troubleshooting system problems, for replacing and adding other security system hardware and software products. Such documents are an integral component to new and retrofit construction projects.</i>	
12.46	Have security system design and drawing standards been developed?		
12.47	Are security equipment selection criteria defined?		
12.48	What contingency plans have been developed or are in place to deal with security control center redundancy and backup operations?		
12.49	Have security system construction specification documents been prepared and standardized?		
12.50	Are all security system documents to include as-built drawings current?		
12.51	Have qualifications been determined in using security consultants, system designers and engineers, installation vendors and contractors?		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
12.52	Are security systems decentral-ized, centralized, integrated, and operate over existing IT network or standalone method of operation?		
12.53	What security systems manuals are available?		
12.54	What maintenance or service agreements exist for security systems?		
13 Security Master Plan			
13.1	Does a written security plan exist for this facility? When was the initial security plan written and last revised? Who is responsible for preparing and reviewing the security plan?	<i>The development and imple-mentation of a security master plan provides a roadmap which outlines the strategic direction and vision, operational, managerial and technological mission, goals and objectives of the organizations security program.</i>	
13.2	Has the security plan been communicated and disseminated to key management personnel and departments?		
13.3	Has the security plan been benchmarked or compared against related organizations and operational entities?		
13.4	Has the security plan ever been tested and evaluated from a cost-benefit and operational efficiency and effectiveness perspective?		
13.5	Does it define mission, vision, short-long term security program goals and objectives?		
13.6	Are threats, vulnerabilities, risks adequately defined and security countermeasures addressed and prioritized relevant to their criticality and probability of occurrence?		
13.7	Has a security implementation schedule been established to address recommended security solutions?		
13.8	Have security operating and capital budgets been addressed, approved and established to support the plan?		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
13.9	What regulatory or industry guidelines/standards were followed in the preparation of the security plan?		
13.10	Does the security plan address existing security conditions from an administrative, operational, managerial and technical security systems perspective?		
13.11	Does the security plan address the protection of people, property, assets and information?		
13.12	Does the security plan address the following major components: access control, surveillance, response, building hardening and protection against biological, chemical, radiological and cyber-network attacks?		
13.13	Has the level of risk been identified and communicated in the security plan through the performance of a physical security assessment?		
13.14	When was the last security assessment performed? Who performed the security risk assessment?		
13.15	Were the following areas of security analysis addressed in the security master plan: Asset Analysis: Does the security plan identify and prioritize the assets to be protected in accordance to their location, control, current and replacement value? Threat Analysis: Does the security plan address potential threats; causes of potential harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services? Examples include possible criminal acts (documented and review of police/security incident reports) associated with forced entry, bombs, ballistic assault, biochemical and related terrorist tactics, attacks against utility systems infrastructure and buildings.		

ITEM	ASSESSMENT QUESTION	ASSESSMENT GUIDANCE	ASSESSMENT COMMENT
	<p>Vulnerability Analysis: Does the security plan address other areas and anything else associated with a facility and its operations that can be taken advantage of to carry out a threat? Examples include the architectural design and construction of new and existing facilities, technological support systems (e.g. heating, air conditioning, power, lighting and security systems, etc.) and operational procedures, policies and controls.</p> <p>Risk Analysis: Does the security plan address the findings from the asset, threat, and vulnerability analyses to develop, recommend and consider implementation of appropriate security countermeasures?</p>		

APPENDIX III: FACILITY ASSESSMENT REPORT OUTLINE

FOREWORD

Description of the content of the report and contractual requirements for the assessment.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Overview

Identification of the facility, assessment dates, team composition and assessment objectives.

Summary of Major Conclusions and Recommendations

Summary of general assessment of the facility on each major area of vulnerability and proposed remedial action.

BACKGROUND

Facility Description

Detailed description of the facility including:

- ◆ Major functions
- ◆ Overall physical characteristics and conditions
- ◆ Significant features, including history
- ◆ Occupant information
- ◆ Community statistics
- ◆ Geographic location annotated with regional and local adjacencies, hazardous conditions, emergency services, etc.
- ◆ Transportation system nodes and arteries related to the facility
- ◆ Description of the contiguous major city and potential threats to the facility

Assessment Overview

Facility Significance (Phase I)

Description of the criticality of the facility

Assessment Process

Description of the assessment process including:

- ◆ PreAssessment (Phase II)
 - ◆ Critical and vulnerable functions
 - ◆ Critical and vulnerable building systems
 - ◆ Significant threats
 - ◆ Available documentation

- ◆ Assessment (Phase III)
 - ◆ Team composition
 - ◆ Schedule

SECURITY ASSESSMENT OF THE FACILITY

Description of each major area of vulnerability and description and cost estimate of remedial action including future costs and increased staff costs if applicable.

- ◆ Site
- ◆ Architectural
- ◆ Structural Systems
- ◆ Building Envelope
- ◆ Utility Systems
- ◆ Mechanical Systems
- ◆ Plumbing and Medical Gas Systems
- ◆ Electrical Systems
- ◆ Fire Alarm Systems
- ◆ Communications and Information Technology Systems
- ◆ Equipment Operations and Maintenance
- ◆ Security Systems
- ◆ Security Master Plan

CONCLUSIONS AND RECOMMENDATIONS

Ranked listing of cost effective remedial action recommendations for the facility.

APPENDICES

Facility Photographs and Floor Plans
Facility Assessment Checklist Results
Cost Analysis Results

APPENDIX IV: GLOSSARY

Asset is any potential target of attack or disaster, most commonly people, equipment, or buildings.

Continuity of Operations (COOP) is an uninterrupted state that ensures essential functions are performed.

Collateral Damage is secondary damage attained not as a direct result of a threat but because of adjacency to the target.

Critical Facilities are those facilities that must remain mission operational during periods of national crisis or emergency.

Criteria are information in the form of guidance, directives, standards or other documentation on which professional judgment is made.

Emergency Services are the medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to a public health or safety incident where speed and efficiency are necessary.

Facility is a building or group of buildings in one physical location.

Facility Assessment is a systematic process to consider the likelihood that a threat will harm an asset and to identify actions to reduce the vulnerability and mitigate the consequences on an attack.

Infrastructure is the basic underlying base of facilities, equipment, or other assets needed for the functioning of a total system.

Minimum Critical Infrastructure (MCI) is the least possible base of facilities or other assets needed to provide for continued operation of critical services.

National Security Presidential Directive (NSPD) is used to promulgate Presidential decisions on national security matters.

Physical Security is concerned with material strategies designed to safeguard people, buildings, equipment, and other assets.

Presidential Design Directive (PDD) series is used to promulgate Presidential decisions on national security matters.

Standoff Distance is the distance between an asset and a threat.

Threat Assessment is a continual process of compiling and examining available information on impending danger to an asset.

Vulnerability is the susceptibility to any action by any means through which operational effectiveness is reduced.

Vulnerability Assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may be exploited and suggests alternatives to eliminate or mitigate those weaknesses.

APPENDIX V: SELECTED BIBLIOGRAPHY

- Balancing Security and Openness.* General Services Administration. 30 November 1999.
- Executive Order 12656: Assignment of Emergency Preparedness Responsibilities.* 18 November 1988.
- Executive Order 12977: Interagency Security Committee.* 19 October 1995.
- Executive Order 13010: Critical Infrastructure Protection.* 15 July 1996.
- Facilities Standards for the Public Building Service (PBS-P100) Chapter 8: Security Design.* General Services Administration. November 2000.
- Federal Preparedness Circular (FPC) 65: Federal Executive Branch Continuity of Operations (COOP).* 16 July 1999.
- Guidance for Protecting Building Environments from Airborne Chemical, Biological or Radiological Attacks.* Department of Health and Human Services. May 2002.
- ISC Security Design Criteria.* Interagency Security Committee. 28 May 2001.
- Minimum Antiterrorism Standards for Buildings (UFC 4-010-01).* Department of Defense. 8 May 2002.
- National Capital Urban Design and Security Plan.* National Capital Planning Commission. July 2002.
- Presidential Decision Directive (PDD) 63: Critical Infrastructure Protection.* 22 May 1998.
- Presidential Decision Directive (PDD) 67: Ensuring Constitutional Government and Continuity of Government Operations.* 21 October 1998.
- Protecting Buildings and Their Occupants From Airborne Hazards (TI 853-01).* U.S. Army Corps of Engineers. October 2001.
- Public Law 107-188: Public Health Security and Bioterrorism Preparedness and Response Act of 2002.* 12 June 2002.
- Risk Management Guidance for Health and Safety under Extraordinary Incidents.* American Society for Heating, Refrigerating, and Air-Conditioning Engineers. 12 January 2002.
- Vulnerability Assessment of Federal Facilities.* Department of Justice. 28 June 1995.

APPENDIX VI: TASK GROUP/PROJECT TEAM BIOGRAPHIES

Curt P. Betts, PE is a security and structural engineer with the US Army Corps of Engineers Protective Design Center. He is currently the co-chair of the DoD Security Engineering Working Group developing the DoD Minimum Antiterrorism Standards for Buildings and is past chair of the Security Architecture and Engineering Council of the American Society for Industrial Security (ASIS).

Michael Chipley, PhD is Vice President for UTD, Inc. and is responsible for engineering, scientific, and information technology programs where he is the program manager for the US Coast Guard Port Vulnerability Assessment project. He retired as a US Air Force civil engineer serving on the air staff at the Pentagon serving as Chief Engineer on the Secretary of the Air Force Executive issues team as well as serving as a Program Manager at the Air Force Office of Scientific Research.

William H. Choquette is Senior Vice President for Gilbane Building Company where he is responsible for federal agency projects. He is a past member of the Board of Directors of the Associated General Contractors of America (AGC) and serves on the Board of Directors of the National Institute of Building Sciences representing the construction sector.

Robert Cizmadia, CPP, FSO is the Director Corporate Security Services for Gage-Babcock & Associates providing global security and fire protection consulting and systems engineering services. He is a Certified Protection Professional (CPP) of the American Society for Industrial Security (ASIS) and a certified Facility Security Officer (FSO) of the Defense Security Service. He serves on the Architectural and Security Engineering Executive Council of ASIS and is a security advisor to the American Institute of Architects (AIA).

James G. Haughton, MD, MPH is Medical Director of Public Health in the Los Angeles County Department of Health Services. He has served as Executive Medical Director of the New York City Department of Health, First Deputy of the Health Services Administration of the City of New York and Chief Executive Officer of the Health and Hospitals Governing Commission of Cook County, Illinois. He is a member of the Board of Directors of the California Conference of Local Health Officers and the Health Officers Association of California. He is a member of the American Public Health Association and the Institute of Medicine of the National Academy of Sciences and served on the Commission on the Future of VA Healthcare.

Earle Kennett is Vice President of the National Institute of Building Sciences where he is responsible for a number of programs and councils. He has managed hundreds of projects for a range of federal agencies including DoD, NAVFAC, Corps of Engineers, GSA, NSF, FEMA, NASA, DOE, and VA. Before coming to NIBS he was the Administrator for Research for the American Institute of Architects where he was responsible for directing research activities for the architectural profession. He has degrees in engineering and architecture.

Stuart L. Knoop, FAIA is Principal in Oudens + Knoop Architects providing design and security related services to a range of federal agencies including the Department of State, General Services Administration, National Institutes of Health, and the Walter Reed Army Medical Center. He has served on numerous security-related Academy of Science committees and is the current chair of a National Research Council (NRC) committee reviewing the Interagency Security Committee (ISC) criteria. He is a fellow in the American Institute of Architects and member of the American Society for Industrial Security and the Building Officials and Code Administrators.

Richard H. McClintock is Director of Security at the Dartmouth Hitchcock Medical Center. He served as a commissioned officer in the US Army Military Police in numerous positions including responsibility for physical security operations in the upper mid-west region of the US and with

the US Army Reserves at the Office of the Provost Marshal, Walter Reed Army Medical Center. He is the current chair of the Healthcare Security Council of the American Society for Industrial Security (ASIS) and has served as a State Chair of the International Association for Healthcare Safety & Security (IAHSS).

Charles A. Meyer, PE, FACEC is President of Henry Adams, Inc. providing mechanical/electrical engineering services to a range of federal agencies including the Department of Veterans Affairs. He is a fellow of the American Council of Engineering Companies (ACEC) where he chaired the Federal Agency Committee. He is also a member of the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) and the Society of American Military Engineers (SAME).

Robert Ted Nuckolls, CCE is Baltimore Area Executive for a number of Baltimore cemeteries. He is past president and current member of the Board of Directors of the International Cemetery and Funeral Association (ICFA). He is president of Loudon Park Cemetery, one of the largest cemeteries in the US with over 1000 acres of property.

Michael L. Rawson, CHSP, HEM is Corporate Director of Safety, Security, and Environmental Health of Intermountain Health Care, Inc. He is a Certified Healthcare Safety Professional (CHSP) and a Certified healthcare Environmental Manger (HEM). He served as a commissioned officer in the US Army Military Police and is a graduate of the US Army Command and General Staff College. He is a member of the Safety and Security Committee of the American Society for Healthcare Engineering (ASHE) and was recently involved with supporting hospital security activities at the 2002 Winter Olympic Games.

Terri Rebmann, RN, MSN, CIC is the Infectious Disease Specialist for the Center for the Study of Bioterrorism and Emerging Infections at Saint Louis University, School of Public Health. A registered nurse with an emphasis in infectious diseases she is responsible for overseeing construction and rehabilitation projects to prevent construction-related infections in patients. She is a member of the Bioterrorism Working Group of the Association for Professionals in Infection Control and Epidemiology (APIC).

Robert Smilowitz, PhD, PE is a Principal in Weidlinger Associates and Adjunct Professor of Engineering at the Cooper Union. He analyzed the World Trade Center underground parking garage in response to the 1993 bombing and the Khobar Towers in response to the terrorist bomb attack and was a member of the American Society of Civil Engineers/Federal Emergency Management Agency Building Performance Assessment Team for the 2001 World Trade Center collapse. He has participated in numerous design and vulnerability studies of federal, military, and commercial buildings.

Charles H. Thornton, PhD, PE is Chairman of The Thornton-Tomasetti Group and is a recognized expert in the area of collapse and structural failure analysis. He has led and participated in a number of investigations including the Hartford Coliseum Roof collapse, New York State Thruway Schoharie Bridge collapse, and the Murrah Office Building and World Trade Center bombings. He was elected to the National Academy of Engineering in 1997 and awarded Engineering News-Record Award of Excellence in 2001. He is currently the Chair of the NIBS Building Seismic Safety Council.

Russell E. Weber, AIA is an architect with Leo A. Daly Company with a broad range of design experience and knowledge in healthcare, medical research, military, and airport facilities and security applications. He is presently managing an assessment of existing security systems to achieve compliance with new Transportation Security Administration requirements. He has designed and managed several VA medical centers and National Institutes of Health facilities. He is a member of the American Institute of Architects (AIA).

Pax T. Williams is Program Manager for Battelle's Threat, Vulnerability, and Protection Assessment program dealing with chemical, biological, and radiological (CBR) threats. He previously served as the Assistant Program Manager for Nuclear, Biological, and Chemical systems integration within the US Army Defense Systems. He also served as a US Army representative to the Army Materiel Command Headquarters for the prioritization, funding, and fielding of CBR defense technology and equipment.

James E. Woods, PhD, PE is executive director of the Building Diagnostics Research Institute, Inc., where he is responsible for numerous research projects for federal agencies, private companies and associations. He is a fellow of the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) and a past member of the ASHRAE Board of Directors. He is current chair of the ASHRAE Presidential AD Hoc Committee on Building Health and Safety under Extraordinary Incidents, which is responsible for the January 2002 report "Risk Management Guidance for Health and Safety under Extraordinary Events." He has also served on the Science Advisory Board for the US Environmental Protection Agency and several committees of the National Research Council.

