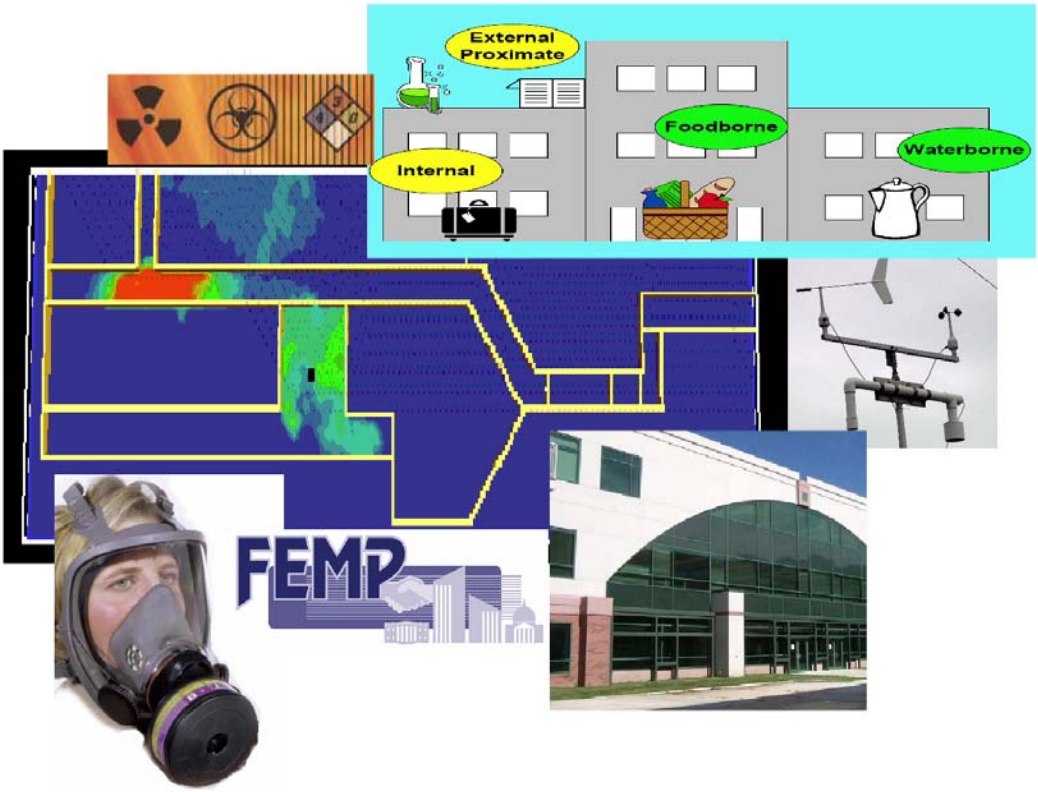
ORNL/TM-2004/260

OAK RIDGE
NATIONAL LABORATORY
MANAGED BY UT-BATTELLE
FOR THE DEPARTMENT OF ENERGY

Mitigation of CBRN Incidents for HVAC Systems in Federal Facilities

February 2005



UT-BATTELLE

ORNL/TM-2004/260

Federal Energy
Management Program

Mitigation of CBRN Incidents for HVAC Systems in Federal Facilities

Michael MacDonald

February 2005

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6070
Managed by
UT-BATTELLE, LLC
For the
U.S. DEPARTMENT OF ENERGY
Under Contract DE-AC05-00OR27725

DOCUMENT AVAILABILITY

Reports produced after January 1, 1996, are generally available free via the U.S. Department of Energy (DOE) Information Bridge:

Web site: http://www.osti.gov/bridge

Reports produced before January 1, 1996, may be purchased by members of the public from the following source:

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
Telephone: 703-605-6000 (1-800-553-6847)
TDD: 703-487-4639
Fax: 703-605-6900
E-mail: info@ntis.fedworld.gov
Web site: http://www.ntis.gov/support/ordernowabout.htm

Reports are available to DOE employees, DOE contractors, Energy Technology Data Exchange (ETDE) representatives, and International Nuclear Information System (INIS) representatives from the following source:

Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831
Telephone: 865-576-8401
Fax: 865-576-5728
E-mail: reports@adonis.osti.gov
Web site: http://www.osti.gov/contact.html

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Table of Contents

Foreword v
Executive Summary vii
Abbreviations and Acronyms xi

Introduction 1
In the News 4
Critical Infrastructure 7
People Are Important 9
Understanding CBRN Threats 11
Chemical and Biological Agents *11*
Radiological Devices *14*
Nuclear Blast *16*
CBRN Incident Exposure Reduction 20
Mitigation Technologies and Actions 26
HVAC Systems and Threat Profiles *28*
Technology Mitigation / Cost Profile *30*
Energy Efficiency *31*
HVAC System Vulnerability Mitigation Guides 33
Risk Input Scales and Scoring 35
Asset Selection and Rating *35*
Vulnerability Assessments *37*
Threat Assessment *37*
Risk Scoring *38*
Combined Analysis of Risk and Additional Factors *39*
Mitigation Priority Example 40
Conclusion 43
References 45

Foreword

This document covers a wide range of topics related to the potential mitigation of the effects of chemical, biological, radiological, or nuclear (CBRN) weapons—or so-called weapons of mass destruction—on buildings and their occupants. Since the CBRN threats of interest for this report are primarily airborne, and since the survivability of a nuclear attack primarily must consider airborne threats, the need for mitigation strategies related to air-handling systems (HVAC systems) in buildings follows directly and is an important concern of this report. However, the overall issues are largely planning issues, as guidance on HVAC systems tasks has already been developed and is available.

This report gives some indication of the effects of the Internet age: every reference except two was accessed via the Internet, and all references except three have an Internet access address provided.

As a nation we are being told, relative to potential threats from extremists or natural disasters, to embrace the Boy Scout motto, "Be Prepared." This report presents one small area that federal agencies and others can use as a resource in preparing to increase security of individual organizations.

Executive Summary

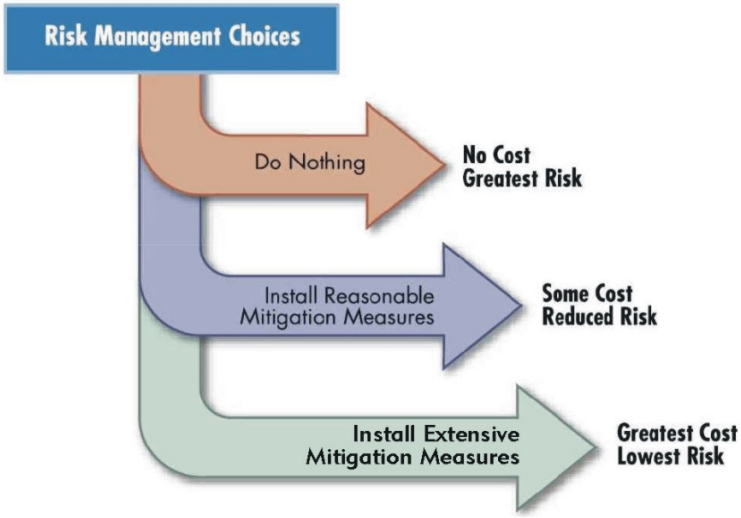
Many changes in America have resulted from the large-scale attacks of September 11, 2001, against civilian populations by extremists. A Department of Homeland Security has been created. Increased abilities to mitigate attacks by weapons of mass destruction (WMDs) have been recommended by prestigious bodies. U.S. Department of Energy (DOE) Secretary Spencer Abraham has declared that security is core to DOE's mission. Federal agencies have promulgated directives requiring increased security against WMD attacks. Federal facility managers have asked DOE's Federal Energy Management Program (FEMP) if there is any assistance that can be provided to deal with the directives, especially those related to building ventilation systems. This document provides initial guidance.

Assuming that WMDs can be scoped as comprising chemical, biological, radiological, nuclear, and (high-yield) explosive (CBRNE) agents, the subset of WMDs addressed in this document involves CBRN (chemical, biological, radiological, and nuclear) agents. Since CBRN threats, excluding the direct explosive nuclear threat, are primarily airborne, building air-handling, or HVAC, systems become an important concern. This report is intended to provide a starting point allowing federal facility managers to develop plans for CBRN incident mitigation measures that can be implemented for their buildings and HVAC systems.

Assessing CBRN threats, buildings, and their HVAC systems is a complex task. A technically sound, defensible assessment of the combination of CBRN threats to buildings and their HVAC systems is even more complex. Since buildings have people in them and require people to keep them operating correctly, the threat must be assessed in a comprehensive manner, with an emphasis on survivability and safety. This report provides background on personal preparedness, the nature of CBRN threats, and the larger context for CBRN threat mitigation.

Guidance and directives on building threats and risk assessments have mushroomed almost beyond the ability of individuals to assimilate and analyze. Emergency preparedness has become a major national undertaking, reminiscent of the Civil Defense efforts of the 1950s, but more complicated and extensive. Diverse areas of technology development have been recommended and are being pursued. Prospective research and development (R&D) for new and advanced technologies to apply to emergency preparedness and threat mitigation is being evaluated by many organizations. However, funding for extensive capital investments to enhance building security for all federal facilities is tight. Information and methods to even approximately quantify the potential threat posed by CBRN agents to federal buildings is mostly nonexistent.

In this overall context, federal facility managers are hard-pressed to meet directives for increasing facility security against potential CBRN threats. This guide briefly describes the steps needed to develop CBRN threat mitigation measures and strategies and indicates links to the many resources that can help in this overall endeavor. It provides a brief, simplified example of a federal agency that implements CBRN incident mitigation measures related to building HVAC systems and personnel. The steps illustrated in this example can be undertaken with limited resources.



The improvements that appear to be needed in order to make effective improvements in facility security are as follows:

- New technologies under development — e.g., biological agent sensors, improved chemical sensors — need to be made ready for use.
- An overall integration of multiple methods and technologies has not yet been implemented and tested. Therefore, it is expected that major integration improvements will be needed.
- Expertise on building and HVAC systems, in combination with expertise on CBRN threats, appears limited. Some guidance has been developed, but too many pieces are still missing, such as how to integrate personnel actions effectively with selected technologies.

- Facility managers are expected to need outside expertise to more effectively assess potential CBRN mitigation measures for their facilities. The procurement of outside expertise is expected to be a challenge because there is not a clear definition of the expertise needed.
- Energy efficiency is an interest of FEMP, and initial ideas for ways to integrate energy efficiency and building security have been developed, but much more work is required to understand the potential benefits and workable solutions to synergistic issues
- Better alignment and eventual standardization of methods and approaches used to assess CBRN risks for building HVAC systems will be needed. Those developed to date do not appear adequate to deal with certain unique requirements of HVAC systems — systems that are critical relative to potential CBRN threats.

Readers of this guide can use the information presented and the resources identified to work through an overall process to select and prioritize CBRN incident mitigation measures for facility HVAC systems and people. Results should be at least marginally acceptable in the short term, but many future changes in federal policy and technologies are expected to keep the overall mitigation selection process in flux for years to come.

Abbreviations and Acronyms

ARFCAM	Autonomous Rapid Facility Chemical Agent Monitor
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
AT/FP	Antiterrorism/Force Protection Program (DoD)
AXLU	Agency X local unit
BAND	Bioagent Autonomous Networked Detectors
BIAD	Bioinformatics and Assays Development Program
BMOC	building management and its operating contractor
BVAMP	Building Vulnerability Assessment & Mitigation Program
CB	chemical and biological
CBIAC	Chemical and Biological Defense Information Analysis Center
CBR	chemical, biological, and radiological
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and (high-yield) explosive
CDC	Centers for Disease Control and Prevention
CDO	Civil Defense Office (ca. 1950s)
CFR	Code of Federal Regulations
CWA	Chemical Warfare Agent
DARPA	Defense Advanced Research Projects Agency
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOS	U.S. Department of State
ECBC	Edgewood Chemical Biological Center
EPA	U.S. Environmental Protection Agency
FAA	Federal Aviation Administration
FEMA	Federal Emergency Management Agency
FEMP	Federal Energy Management Program
HSARPA	Homeland Security Advanced Research Projects Agency
HSPD	Homeland Security Presidential Directive
HVAC	heating, ventilating, and air-conditioning
JPEO-CBD	Joint Program Executive Office for Chemical and Biological Defense
JPMG	Joint Project Manager Guardian
LACIS	Lightweight Autonomous Chemical Identification System
LBNL	Lawrence Berkeley National Laboratory
LSI	lead systems integrator
NAE	National Academy of Engineering
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical

NIMS	National Incident Management System
NIOSH	National Institute for Occupational Safety and Health
NIPP	National Infrastructure Protection Plan
NRC	National Research Council
NRP	National Response Plan
ODPM	Office of the Deputy Prime Minister, United Kingdom
ORNL	Oak Ridge National Laboratory
OSHA	Occupational Safety and Health Administration
OTA	Office of Technology Assessment
PEL	permissible exposure limit
PHILIS	Portable High-Throughput Integrated Laboratory Identification System
RABIS	Rapid Automated Biological Identification System
R&D	research and development
RDD	radiological dispersal device
SAIC	Science Applications International Corporation
TIC	toxic industrial chemical
URL	Uniform Resource Locater
WMD	weapon of mass destruction

Introduction

The events of September 11, 2001, have caused many changes in America. Among these changes is an increased emphasis on security, including the creation of the Department of Homeland Security (DHS). In addition to the proliferation of changes in government at all levels, guidance and directives have mushroomed such that agencies can assimilate and analyze them only with difficulty. For the U.S. Department of Energy, Secretary Spencer Abraham has declared that security is core to the Department of Energy's (DOE's) mission.

DOE's Federal Energy Management Program (FEMP) works to reduce the cost and environmental impact of the federal government by advancing energy efficiency and water conservation, promoting the use of distributed and renewable energy, and improving utility management decisions at federal sites. FEMP helps federal energy managers identify, design, and implement new construction and facility improvement projects. As part of this work, FEMP has received several requests from agencies to assist them in dealing with security aspects of their building energy systems — most often the building heating, ventilating, and air-conditioning (HVAC) systems. This document is intended to assist federal agencies in understanding the overall HVAC security picture and also in dealing with the wide range of activities that could come under the call to make HVAC systems more secure against many types of threats. A wide range of resources is also described briefly and referenced.

For military installations, new standards and guidance documents from the Department of Defense (DoD) and from individual services and agencies have moved security of facilities to a high level. The resulting difficulties and variety of costs related to bombed facilities over the past 20 years have had a noticeable impact. As stated in paragraph 1-1 of UFC 4-010-01, July 2002, the new guidance "represents a significant commitment by DoD to seek effective ways to minimize the likelihood of mass casualties from terrorist attacks against DoD personnel in the buildings in which they work and live" (DOD 2002).

The primary threat covered by UFC 4-010 is the threat from explosives. One scheme of categorizing threats to facilities includes chemical, biological, radiological, nuclear, and (high-

yield) explosive (CBRNE) incidents. The explosive threat is primarily considered to be against people, facility structural members, and facility containment, and is not a focus of this document, since it does not pertain to HVAC systems. The radiological threat is *related* to the nuclear threat but essentially different, since a radiological threat involves radiological contamination, while a nuclear threat involves a nuclear blast.

This document was formed under the umbrella of chemical, biological, radiological, and nuclear (CBRN) security for HVAC systems in facilities. A graded approach to CBRN security or safety for facility HVAC systems is important. The term "graded approach" is used primarily for DOE facilities relative to safety, and in particular, for nuclear facility safety analyses. The importance of the graded approach lies in balancing real-world resource limitations against a potentially unrealistically high need for resources to achieve complete safety, while still achieving an appropriate high(er) level of safety. A definition of "graded approach" is provided in the Code of Federal Regulations, 10 CFR 830.3:

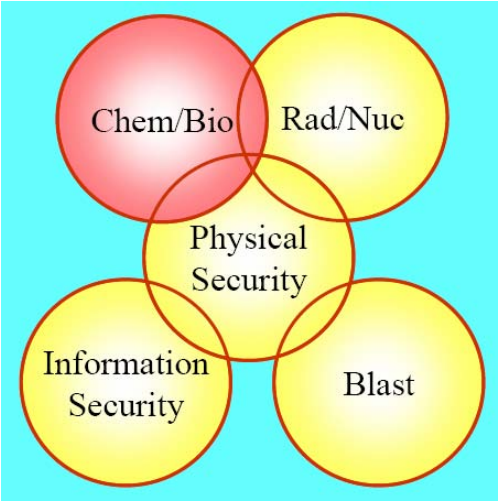
> Graded approach means the process of ensuring that the level of analysis, documentation, and actions used to comply with a requirement in this part are commensurate with:
>
> (1) The relative importance to safety, safeguards, and security;
> (2) The magnitude of any hazard involved;
> (3) The life cycle stage of a facility;
> (4) The programmatic mission of a facility;
> (5) The particular characteristics of a facility;
> (6) The relative importance of radiological and nonradiological hazards; and
> (7) Any other relevant factor.

Some adaptation and extension of this definition is needed to allow a better match to the topic of CBRN security for facility HVAC systems. Required adaptations include changing the notion of "compliance" to one of using analysis, documentation, and actions to achieve the best solutions with the resources available. Readers must understand that the tradeoffs required are large, and risk assessments performed to define the levels of threats that will be addressed may have potentially large uncertainties.

As stated in the Air Force *Installation Force Protection Guide* (U.S. Air Force n.d., 1. Introduction, D. Assumptions): "There are no universal solutions to preclude terrorist attacks, since the threat is largely unpredictable and certainly will change over time." And beyond the boundary of terrorist attacks lie potential natural disasters, major accidents or incidents, and events caused by mentally deranged individuals simply to cause high levels of disruption. The same Air Force "Assumptions" section also quotes the U.S. Department of State (DOS 1995) in

regard to embassy buildings: "No matter how many measures are implemented risk is always present."

The present document attempts to provide a starting point for federal facility managers to begin implementing CBRN security and safety procedures and measures for HVAC systems in their facilities. Potential threats must be weighed against available resources, as well as evaluated in the context of the facilities and personnel in the facilities to be protected.



Keeping in mind that the information, resources, and requirements related to CBRN protection of facilities and personnel are so extensive as to be difficult to assimilate, and that these are changing at a fast pace, this guide will be unable to cover all materials related to the diverse topics involved in a process of CBRN protection of HVAC systems. The goal is to provide enough information to allow facilities personnel to proceed as best possible.

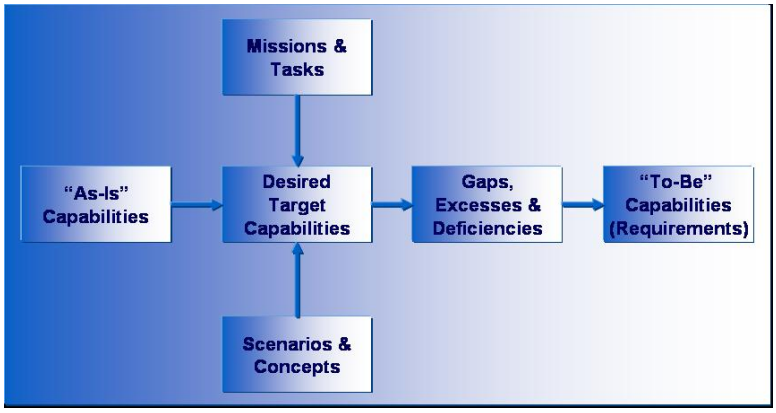
CBRN protection of HVAC systems in federal facilities must be considered in the larger context of protection of personnel, preservation of federal critical infrastructure, and overall security of federal facilities. Because of the interrelatedness of these issues, some level of background information on several topics will be presented in this report. Since FEMP is primarily concerned with energy efficiency of federal facilities, connections between efficiency and security will also be touched on briefly.

This document has been developed by DOE's Oak Ridge National Laboratory (ORNL) in support of FEMP's mission to assist federal agencies.

In the News

As this report is being prepared in the autumn of 2004, the nature of the facilities security picture is evolving continuously:

- Brussels, Belgium, May 3, 2004: Black Dawn scenario-based exercise on catastrophic terrorism held; emphasized prevention instead of consequence management, involving current and former senior officials and experts from the European Council, the European Commission, NATO, 15 member states, and various international organizations
- Emergency management in the security state is now a topic in security presentations, where our country has conceptually moved from the administrative through the entitlement to the security state, and the Homeland Security environment (the security state) is a strong factor in the future of the country
- December 17, 2003: Homeland Security Presidential Directive (HSPD) 8, "National Preparedness," is implemented with 16 major initiatives to prevent and respond to threatened or actual domestic terrorist attacks, major disasters and other emergencies. Additional national guidance is expected in March 2005.



- In addition, DHS must deal with
  - the National Strategy for Homeland Security
  - the National Incident Management System (NIMS)
  - the National Response Plan (NRP)
  - the National Infrastructure Protection Plan (NIPP, under HSPD-7)
- Areas of responsibility related to preparedness include
  - Prevention / deterrence
  - Infrastructure protection
  - Preparedness
  - Emergency assessment / diagnosis
  - Emergency management / response
  - Hazard mitigation
  - Evacuation / shelter
  - Victim care
  - Investigation / apprehension
  - Recovery / remediation

- Officers Start Wearing Vests to Shield From Bio-Attacks, Updated: Monday, Sep. 27, 2004 — 6:05 AM

  WASHINGTON (AP) - Some U.S. Capitol Police officers have begun donning new protective vests and carrying hoods designed to shield them from a biological or chemical attack.

  The Washington Post reports, a handful of officers were wearing the new vests on Friday. A hazard suit, gloves, and boots are sealed into the back of each vest, and a one-time protective hood with special filters is attached to the side.

  Officers underwent 40 hours of special training before receiving the vests.

  The vests are part of an aggressive and unusually public effort to prevent a terrorist attack before and during the upcoming presidential election. The election is in 36 days.

  The region's Joint Terrorism Task Force will meet with local and federal officials in Arlington this week to discuss potential threats.

- N.M. town to become anti-terrorism training site

  Homeland Security funding purchase of entire ghost town

  By Simon Romero, New York Times News Service

  September 26, 2004

  PLAYAS, N.M. — The Phelps Dodge mining company pictured a suburban utopia with a Southwestern flavor when it built this town for its employees from scratch in the early 1970s. It incorporated a six-lane bowling alley, a rodeo ring, a helicopter pad, a shooting range and a swimming pool into the community of 259 ranch-style homes.

  But the company shut its nearby copper smelter because of sluggish prices in the late 1990s.

  The 50 or so remaining residents of Playas say they are ready for their town to become a target for pickups laden with explosives and simulations of suicide bombs, water-supply poisoning and anthrax attacks.

  In what might be the beginning of Playas' renaissance, the Department of Homeland Security is channeling $5 million to a small New Mexico engineering school to buy the entire town. The school, in turn, aims to turn the town into one of the country's top locations for anti-terrorism training.

  "I wish they'd hurry up and start hiring people," Carol Davis, 51, a part-time emergency medical technician, said. "It's too quiet out here right now. I'd like a job driving an ambulance or something."

  The isolation of Playas is part of the allure for New Mexico Tech, which expects to complete the purchase in the next few weeks.

  "Playas is not your typical ghost town with a saloon and a couple of storefronts, which is what made it so attractive to us," said Van Romero, vice president for research and economic development at New Mexico Tech, based in the town of Socorro.

The university, which has 1,800 students, has trained more than 90,000 emergency workers to respond to terror attacks since the Oklahoma City bombing of 1995. Altogether, it is receiving $20 million in grants from the Department of Homeland Security for anti-terrorism programs.

Playas will be used mostly to train security, medical and military personnel to prevent attacks as well as respond to them. Romero said he would not ask residents to leave before the "attacks."

- News Releases
  - FOR IMMEDIATE RELEASE, May 07, 2004

SAIC Awarded U.S. Army Contract to Serve as Lead Systems Integrator for the Guardian Installation Protection Program

(MCLEAN, VA and HUNTSVILLE, AL) – SAIC announced today it has won a contract from the U.S. Army's Space and Missile Defense Command in Huntsville, Ala., to serve as the Guardian Installation Protection Program Lead Systems Integrator (LSI). The Guardian Installation Protection Program is managed by the Joint Project Manager Guardian (JPMG) for the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD). Working under the JPMG, SAIC will provide an integrated chemical, biological, radiological and nuclear protection (CBRN) capability at 200 Department of Defense (DoD) installations and facilities worldwide. This cost-plus-fixed-fee contract will be performed over a base of three years with the potential of earning up to three one-year award terms. The cumulative value of the contract is $390 million.

The Installation Protection Program is a Family of Systems that supplements other aspects of force protection against potential weapons of mass destruction. The Family of Systems will include capability for CBRN detection, identification, warning, reporting, decision support, individual and collective protection, emergency response, decontamination, medical countermeasures, medical diagnostics, and medical surveillance components and will be tailored to the needs of each installation. As LSI, SAIC will work with JPMG to design, procure, integrate, install and test the Family of Systems. After the system is fully installed, SAIC will facilitate an installation-wide weapons of mass destruction exercise. . . .

The smattering of news reports provided here is intended to give a flavor of the types of ongoing activities related to CBRN threat protection. These items are not even the tip of the iceberg, since many activities, such as those of the U.S. Department of State and many military activities, are not made known to the public, and many other activities of state and local governments are not well reported. The "Family of Systems" mentioned in the paragraph above indicates the diversity.

These news reports should leave no doubt that major changes are in progress that will affect efforts to implement CBRN threat protection and mitigation over at least the next several years. The change appears similar to the Civil Defense efforts of the 1950s, but on a larger and much more complicated scale. Responsibilities will shift and change; requirements appear likely to grow.

Critical Infrastructure

DHS has responsibilities for protection of critical infrastructure and, as mentioned in the previous section of this report, currently must oversee development of a national plan on defining and protecting critical infrastructure. In this effort, extensive interaction with other federal agencies and with private sector entities is necessary. Some overlap of responsibilities with other agencies that have critical infrastructure is inevitable, although the responsibility for agency-specific critical infrastructure may be delegated.

Several critical infrastructure sectors and a general pool of critical resources have been identified (Office of the President 2003). The sectors listed here number 12 and differ slightly, based on later reporting:

- Agriculture and food
- Water
- Public Health
- Emergency Services
- Government
- Defense Industrial Base
- Information and Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemical Industry and Hazardous Materials
- Postal and Shipping

The critical resources pool includes national monuments and icons, nuclear power plants, dams, government facilities, and key commercial assets. Many questions and decisions must still be made regarding the plan for critical infrastructure and how protection efforts will begin.

Many federal sites have some critical infrastructures on a smaller scale. Some, like the defense industrial base, include facilities owned and operated by DoD. The Postal Service is discretely identified. Federal agencies and facilities are involved in critical infrastructure in a major way, and critical infrastructure protection has been a focus area for government entities at least since the late 1990s.

In addition to government efforts, many public and private committees and organizations and private industry, university, and trade association committees and organizations are forming around topics related to protection of critical infrastructure. Since many of these

entities are new, and since the major increase in efforts on emergency preparedness and homeland security is new, well-defined charters and programs of effort do not appear to be highly visible. As homeland security efforts continue to increase, however, program definitions are likely to take better form. The changes that are occurring are expected to have impacts on all local facility planning related to CBRN protection.

Extensive research is needed relative to improving our ability to protect critical infrastructure. Urgent research opportunities identified by the NRC (2002) indicate that the following technological initiatives are needed to improve our ability to protect critical infrastructure from CBRN attacks:

- Develop effective treatments and preventatives for known pathogens for which current responses are ineffective and for potential emerging pathogens
- Develop, test, and implement an intelligent, adaptive electric-power grid
- Advance the practical utility of data fusion and data mining for intelligence analysis, and enhance information security against cyber attacks
- Develop new and better technologies (e.g., protective gear, sensors, communications) for emergency responders
- Advance engineering design technologies and fire-rating standards for blast- and fire-resistant buildings
- Develop sensor and surveillance systems (for a wide range of targets) that create useful information for emergency officials and decisions makers
- Develop new methods and standards for filtering air against both chemicals and pathogens as well as better methods and standards for decontamination

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Office of the President 2003) is available from the White House web site (see references). This strategy report is the product of many months of consultation across a broad range of stakeholders. The report identifies major protection initiatives in general terms for the critical infrastructure sectors identified above.

People Are Important

The Department of Defense *Minimum Antiterrorism Standards for Buildings* (DoD 2002) states that DoD is making a significant commitment "to minimize the likelihood of mass casualties from terrorist attacks against DoD personnel." Obviously, people and personnel are critically important. The applicable DoD program area is the Antiterrorism/Force Protection Program (AT/FP).

The Guardian Installation Protection Program mentioned in one of the previously cited news releases is a major effort to take current force protection to the next level, using available technologies, to strengthen CBRN protection. The Guardian charter states that it will "provide DoD prioritized installations with an integrated CBRN protection and response capability to reduce casualties, maintain critical operations, contain contamination and effectively restore critical operations."[1]

In the Guardian effort, the solution set for their objectives to be considered initially, before actual implementation, includes

- first responder equipment
- CBRN sensors
- medical surveillance and protection
- information management
- training
- procedures/processes
- CONOPS (concept of operations) development
- interaction with local communities; dependence/support
- augmentation of physical security design

Recognizing the importance of scarce resources, Guardian plans to have the installation design evolve over time, while focusing on improving capability and lowering sustainment costs. (Sustainment occurs after one year, when the DoD entity takes over from the installing entities.)

[1] Material on the Guardian program is taken from an "Industry Briefing," August 21, 2003, by Col. Camille Nichols, project manager. JPEO-CBD is the Joint Program Executive Office for Chemical and Biological Defense of DoD (http://www.jpeocbd.osd.mil). More recent briefing materials and additional information are also available on the JPEO-CBD web site.

The Guardian effort appears important for examining what can currently be achieved in protecting people and facilities from the effects of CBRN incidents.

Recognizing that people are critically important and are at the top of the protection list, a brief digression is covered here on the topic of preparedness of people. In the event of a CBRN attack, recognizing that risk cannot be reduced to zero, people should understand how to deal with the full range of resulting hazards.

DHS has created the Ready.Gov web site (http://www.ready.gov/) to offer resources for preparedness of individuals, businesses, and children ("coming soon"). As of this writing, the Ready America area for individuals has a banner reading, "Terrorism forces us to make a choice. Don't be afraid … Be Ready." This web site offers information on CBRN events and what individuals can do. The site also covers explosions and many types of natural disasters. Informing employees or other people who spend extensive time in facilities where CBRN response plans are being developed about the Ready.Gov web site appears appropriate, while also cautioning or informing them about differences between the Ready.Gov recommendations and local procedures that have been or are being developed.

RAND has developed a report on individual preparedness that is designed to supplement the Ready.Gov web site information on individual preparedness. The short version of the RAND report (Davis et al. 2003) is probably the most useful and the easiest to access online. This guide is another resource that organizations interested in increasing their CBRN responsiveness could consider sharing with employees and other people using their facilities on a regular basis.

These information resources are more sobering than uplifting. The nature of the Guardian charter presented above should be carefully considered, as it mentions "reduction of casualties," containment of contamination, and maintaining and restoring critical (not necessarily all) operations.

Understanding CBRN Threats

Extensive information is available on chemical and biological threats; less is available on radiological and nuclear threats. The detonation of a nuclear device would produce extensive blast and fire damage, intense direct radiation effects, and possibly widespread contamination from radioactive fallout. The hazards from radioactive fallout would be similar, but potentially much more severe, than those resulting from the release of a radiological agent. In this discussion of protective preparedness actions, the blast and thermal effects of a nuclear incident will be assumed to be at some distance from a facility.

CBRN incidents include both deliberate events and accidents. For example, a chemical incident inside or outside a building might result from an accidental or a deliberate chemical release or from a fire. The nature of the hazard resulting from a CBRN incident depends on the type of incident, the hazardous material released, the location of the release, and possibly the meteorological conditions at the time. If an incident occurs, a rapid assessment of the severity of the hazard would be required. In the sections that follow, the various types of CBRN threats—chemical and biological, radiological, and nuclear blasts—are discussed separately.

Chemical and Biological Agents

The potential threat of chemical and biological (CB) agents to buildings is usually exaggerated, although a concerted, skillful attack could be devastating. Although CB agents can be very dangerous, many conditions affect their lethality, and mitigation can be attained by many means. The RAND guide (Davis et al. 2003) covers specific recommended individual responses, with overarching goals, during potential CBRN events. For example, for a chemical incident, the overarching goal is to find clean air to breathe, and several means of mitigation and survival are discussed for different situations. Examination of individual preparedness measures also gives some insight into possible facility or building preparedness.

Terrorists continue to prefer explosives (see, for example, FEMA 2003d); explosives are more dramatic and easier to obtain than chemicals. Chemicals are easier to obtain than biological agents, but the potential lethality of biological agents can be much higher. Chemical agents include Sarin, cyanides, chlorine, mustard gas, phosgene, VX, and many others. The Centers for Disease Control and Prevention (CDC) maintain a web site that has extensive information on chemical and biological agents (http://www.bt.cdc.gov/). This source is a reasonable place to start

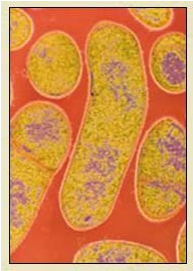
to begin understanding specific biotoxic threats. For definitions of specific chemicals, a standard web search using a search engine may be more useful.

Preparedness can be an important factor in addressing CB attacks. In World War I, German troops using chlorine killed approximately 5,000 Allied soldiers at Ypres, Belgium, in 1915. The attack had warning signs, but without a precedent and an awareness of the threat, the signs were not recognized. Warning signs included the movement of over 5,000 cylinders of chlorine into German trenches about 200 yards away, a strange hissing sound upon release, and a yellow-green cloud of chlorine coming toward them. Wind was an obvious factor in this delivery method.

This first attack, on unprepared soldiers, resulted in one death for every 70 pounds of agent released. However, overall during the war, there was one death for every two tons of agent released — a not very effective weapon. Preparedness increased, but the difficulty of delivering the chemical agents in a lethal manner also led to death reductions. Having to deliver 70 pounds of material to achieve one death is problematic. The need for two tons of agent per person killed appears likely to discourage any terrorist, since explosives are much more lethal per pound.

When chemical and biological agents are released outside, dispersal occurs far too quickly in many cases, and erratic winds can even push the agents back onto those releasing them. So levels of skillfulness and planning are required to accomplish deadly objectives when using outside release of such agents. Indoor release has the potential to be more effective, but there must be a means of dispersal, and the agent typically has to be smuggled into or onto the building first.

Among biological agents, anthrax is known to be one of the most deadly if inhaled; and tularemia bacteria, Ebola virus, encephalitis viruses and others can also be deadly. If working with deadly chemicals is both dangerous and challenging, working with highly toxic biological agents is an order of magnitude worse. From a terrorist's perspective, procedures for working with anthrax must prevent him from becoming infected unintentionally or spreading spores that could lead investigators back to the source. Someone has to be strongly committed and have extensive experience with biological production cleanroom and sterile culturing procedures. Production labs would probably have to be moved at intervals, as slight contamination evidence would accumulate if spore material were transported. Again, explosives are easier.



Experience with biological terrorism is fairly limited. In the United States the anthrax incidents along the East Coast in 2001 led to five deaths. The last case previous to 2001 was in 1979. This incident, in Sverdlosk, Russia, led to 68 deaths out of 79 exposures from an anthrax release estimated at about one gram of material. This incident, which was apparently an accidental release of anthrax spores from a Soviet biological weapons facility, indicated how deadly bioterrorism weapons might be to users before the weapon is ever deployed.

The Armed Forces have to be very concerned about potential use of chemical and biological weapons, and some of their resources are worth highlighting. The Chemical and Biological Defense Information Analysis Center (CBIAC) provides information on CB threats and also analyzes possible threats and threat reduction technologies. The web site for this organization is: http://www.cbiac.apgea.army.mil/

The CBIAC has many literature products that can be purchased, and some information can be accessed directly. The quarterly CBIAC newsletter has pertinent information relative to CB issues (http://www.cbiac.apgea.army.mil/awareness/newsletter/intro.html). The web site has a page covering medical aspects of biological agents that allows downloads of PowerPoint presentations on different biotoxic agents that were prepared for the Army Office of the Surgeon General (http://www.cbiac.apgea.army.mil/products/cr-03-08.html). The presentations can also be ordered on a CD for $10. Each presentation is 3–5 MB in size and 30–40 pages long. The topics covered are

- Anthrax
- Bubonic plague
- Crimean-Congo hemorrhagic fever
- Dengue
- Ebola
- Influenza
- Japanese encephalitis
- Lassa
- Marburg
- Pneumonic plague
- Rift Valley fever
- Staphylococcal enterotoxin B (SEB)
- Smallpox
- St. Louis encephalitis
- Tularemia

Other web sites also provide CB information. The National Research Council report *Making the Nation Safer* (NRC 2002) is available as a PDF document on the National Academies Press web site. A compact description of the characteristics of chemical and biological agents can be found

at the web site of the Nuclear, Biological, and Chemical (NBC) Industry Group (http://www.nbcindustrygroup.com/handbook/pdf/AGENT_CHARACTERISTICS.pdf).

In addition to DoD's CBIAC, the Army operates the Edgewood Chemical Biological Center (ECBC). ECBC often uses the same resources as CBIAC. ECBC and the U.S. Army Corps of Engineers have developed TI 853-01 (USACE 2001) on protecting buildings from airborne hazards, but it apparently has only been released in draft form. TI 853-01 and other similar resources will be discussed in later sections of this report.

Radiological Devices

The radiological threat is related to the nuclear threat, since the type of material used to devise a weapon is the same, and many health effects are related. The radiological threat is covered in some detail in different fact sheets, including *Radiological Attack, Dirty Bombs and Other Devices* (NAE 2004), by the National Academies and DHS. The excerpts below, taken primarily from fact sheets, describe the nature of possible attacks, based mostly on conjecture.

From the National Academy of Engineering (NAE) fact sheet (NAE 2004):

> A **radiological attack** is the spreading of radioactive material with the intent to do harm. Radioactive materials are used every day in laboratories, medical centers, food irradiation plants, and for industrial uses. If stolen or otherwise acquired, many of these materials could be used in a "radiological dispersal device" (RDD). . . .
>
> The term **dirty bomb** and RDD are often used interchangeably in technical literature. However, RDDs could also include other means of dispersal such as placing a container of radioactive material in a public place, or using an airplane to disperse powdered or aerosolized forms of radioactive material. . . .

It is very difficult to design an RDD that would deliver radiation doses high enough to cause immediate health effects or fatalities in a large number of people. Therefore, experts generally agree that an RDD would most likely be used to:

- contaminate facilities or places where people live and work, disrupting lives and livelihoods.
- cause anxiety in those who think they are being, or have been, exposed.

From *Making the Nation Safer* (NRC 2002):

> The ease of recovery from [a radiological] attack would depend to a great extent on how the attack was handled by first responders, political leaders, and the news media, all of which would help to shape public opinion and reactions."

From a February 2003 press kit (DHS 2003) available in the Press Room area of the DHS web site:

> Radiological dispersion devices (RDDs) are a combination of conventional explosives and radioactive material designed to scatter dangerous and sub-lethal amounts of radioactive material over a general area. Terrorist use of RDDs is considered far more likely than use of a nuclear device because they require very little technical knowledge to build and deploy compared to that of a nuclear device. RDDs also appeal to terrorists because certain radiological materials are used widely in medicine, agriculture, industry and research, and are much more readily available compared to weapons grade uranium or plutonium.

The possible use of RDDs appears to have more of an impact psychologically than in terms of physical harm. The DHS fact sheet goes on to explain how to be prepared and what to do if an explosion occurs. However, radiation monitoring equipment would be needed to determine whether an explosion has led to a radiological release, so the correct response would be very difficult to discern for almost all people in the short term. If first responders have radiation detection equipment, determination and notification of radiological contamination could begin.

As with CB agents, the CDC maintains fairly extensive information on radiation emergencies and radiation agents (http://www.bt.cdc.gov/radiation/index.asp). The CDC site also has information

on the effects of radiation exposure and potential treatment methods, as well as advice on suggested responses in case of a radioactive release. The RAND guide (Davis et al. 2003) also provides suggested guidance for individuals in case of a radiological incident.

Nuclear Blast

Devastation from a nuclear blast would extend far beyond the immediate blast location, fire region, and area receiving fallout, as people would be expected to react by leaving the area affected. The resulting economic slowdown could be dramatic. Cleanup could be slow and difficult, so the economic impacts could be long-lasting also. Much of the more useful information on nuclear blast effects is 30–50 years old. The Office of Technology Assessment published a study in 1979 (OTA 1979) that is most pertinent, although there have been more recent materials published in journals and magazines.

The following is the second paragraph of the OTA study's Executive Summary:

> Nuclear war is not a comfortable subject. Throughout all the variations, possibilities, and uncertainties that this study describes, one theme is constant—a nuclear war would be a catastrophe. A militarily plausible nuclear attack, even "limited," could be expected to kill people and to inflict economic damage on a scale unprecedented in American experience; a large-scale nuclear exchange would be a calamity unprecedented in human history. The mind recoils from the effort to foresee the details of such a calamity, and from the careful explanation of the unavoidable uncertainties as to whether people would die from blast damage, from fallout radiation, or from starvation during the following winter. But the fact remains that nuclear war is possible, and the possibility of nuclear war has formed part of the foundation of international politics, and of U.S. policy, ever since nuclear weapons were used in 1945.

Recovery following a nuclear blast would be dubious close to the center of the blast, so preparedness becomes a non-issue there. But large areas would not be affected directly, and the effort required for recovery would decrease as distance from the blast center increased. This report will assume preparedness applies only to facilities outside the major blast zone.

Some perspective from the 1950 National Security Resources Board, Civil Defense Office, booklet *Survival Under Atomic Attack* (CDO 1950) is also appropriate to consider, keeping in mind that longer-term effects from radiation exposure were not well understood at that time: "You can live through an atom bomb raid and you won't have to have a Geiger counter, protective clothing, or special training in order to do it."

Blast effects depend on many factors, including the type of weapon, the explosive power of the weapon, whether it is detonated in the air or on the ground, and wind. The information in the Civil Defense booklet quoted above was based on nuclear devices from the 1950s (low kiloton range), while the OTA report discusses weapons of 1–5 megatons. An important consideration relative to blast effect is that it increases much less than linearly with device power. A smaller device in the low kiloton range can do heavy damage to buildings within about a 2-mile radius. Doubling its power will extend the range of damage to only about 2.5 miles. In the same way, for a device 100 times as powerful, major damage would reach out only a little more than 10 miles, not 100 times as far. From a practical standpoint, many strategically placed smaller devices can do much more damage than one large device of the same explosive capacity.

Table 1 gives some idea of the blast effects of a 1-megaton blast at 6,000 feet. However, many smaller devices cause more damage. The U.S. nuclear weapons arsenal typically consists of final delivered devices much smaller than 1 megaton, although with multiple warheads, one missile might have a greater destructive capacity. The Russian warhead arsenals are similar although sometimes larger, in the 0.6-megaton range per device. China apparently has some older 3- and 5-megaton warhead missiles.

The National Research Council (NRC) report *Making the Nation Safer* (NRC 2002), in evaluating potential threats from terrorists, identifies the state-owned nuclear weapons of Pakistan and India as medium risk due to potential political instabilities, and those of Russia as medium risk due to large numbers of weapons and poor inventory controls. All other nuclear powers are identified as low risk relative to state-owned arsenals. This NRC effort, however, did not consider North Korea or Iran, both of which have made headlines since then, so the nuclear threat continues to evolve.

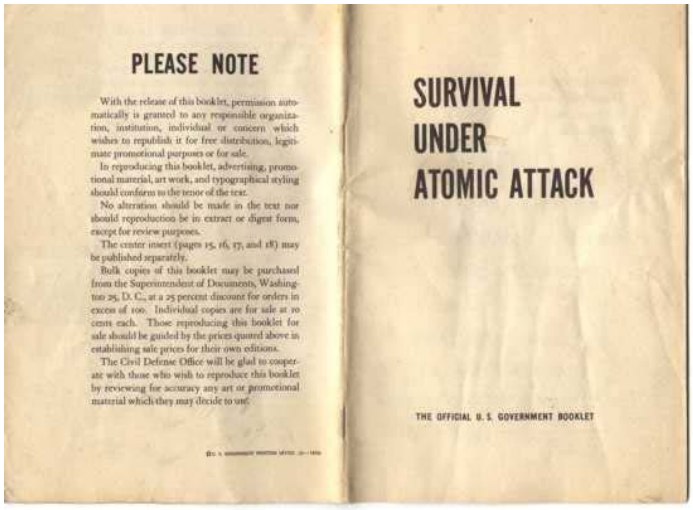
Table 1. Effects of blast from a nuclear explosion

Peak over-pressure	Effects	Distance to which effects are felt [1]
20 psi [2]	Multi-story reinforced concrete buildings demolished; winds, 500 miles per hour.	1.8 mi
10 psi	Most factories and commercial buildings collapsed; small wood and brick residences destroyed; winds, 300 miles per hour.	2.7 mi
5 psi	Unreinforced brick and wood houses destroyed; heavier construction, severely damaged; winds, 160 miles per hour.	4 mi
2 psi	Moderate damage to houses (wall frames cracked, severe damage to roofs, interior walls knocked down); people injured by flying glass and debris; winds, about 60 miles per hour.	7–8 mi

[1] One-megaton burst at 6000 feet.
[2] Pounds per square inch.

Source: Leo Sartori, "The Effects of Nuclear Weapons," *Physics Today,* March 1983, pp. 32–41, as reproduced in McMurrey 2002.

The Civil Defense booklet (CDO 1950) is fairly pointed in describing the consequences of different types of nuclear blasts. Explosion in the air leads to more destruction from the blast and heat, but residual fallout is minor except under certain circumstances. The initial radioactive release is dangerous but only lasts a little longer than a minute. For an airburst explosion, almost all radioactive particles are swept up into the air and then dispersed over a large area. Ground bursts and explosions under water are a different story, leading to extensive radioactive contamination in some areas. High danger is present for the first hour and may linger for 3–4 hours or more. Rain carries radioactive fallout to the ground, so it creates increased fallout hazard.


PLEASE NOTE

With the release of this booklet, permission automatically is granted to any responsible organization, institution, individual or concern which wishes to republish it for free distribution, legitimate promotional purposes or for sale.

In reproducing this booklet, advertising, promotional material, art work, and typographical styling should conform to the tenor of the text.

No alteration should be made in the text nor should reproduction be in extract or digest form, except for review purposes.

The center insert (pages 15, 16, 17, and 18) may be published separately.

Bulk copies of this booklet may be purchased from the Superintendent of Documents, Washington 25, D. C., at a 25 percent discount for orders in excess of 100. Individual copies are for sale at 10 cents each. Those reproducing this booklet for sale should be guided by the prices quoted above in establishing sale prices for their own editions.

The Civil Defense Office will be glad to cooperate with those who wish to reproduce this booklet by reviewing for accuracy any art or promotional material which they may decide to use.

SURVIVAL UNDER ATOMIC ATTACK

THE OFFICIAL U. S. GOVERNMENT BOOKLET

Presentations on radioactive fallout typically assume a nuclear detonation at ground level, so that fallout patterns can be predicted. But an airburst would make fallout much more dispersed and major contamination much less likely, so that the blast, heat, flying objects, and initial radioactive waves are the primary concern, lasting a little longer than a minute. However, terrorists may only

be able to carry out a ground burst incident, causing fallout to be a major issue. In the OTA study, for a 1-megaton ground burst in Detroit, if there is a 15-mph NW prevailing wind, fallout issues would extend in a fairly narrow band stretching to Pittsburgh (~200 miles). For a 15-mph SW wind, fallout concerns would extend for about 200 miles into Ontario and Quebec.

With this quick look at potential CBRN threats, pre-planning and risk assessment for reduction of exposure to CBRN incidents can be more easily understood.

CBRN Incident Exposure Reduction

Any effort to reduce the exposure of HVAC systems in facilities to CBRN threats must be part of a larger effort to prepare for possible incidents, reduce the possibilities of such incidents occurring, and minimize the possible consequences of such incidents. The "graded approach" to increasing HVAC security against CBRN incidents implies that the security of the HVAC system is a subset of overall facility security. The primary threat-reduction techniques involve reducing access to a building if necessary, and reducing access to HVAC systems and intakes as practical and possible.

U.S. DEPARTMENT OF HOMELAND SECURITY
Emergency Preparedness & Response Directorate
Mitigation Division
FEMA

Federal facilities are already required to comply with fire and safety laws and regulations, and some must also comply with requirements related to preventing chemical releases or other incidents. Natural-disaster planning is also handled on a contingency basis. Some facilities may be under requirements to develop emergency action plans (OSHA, 29 CFR 1910.38). At ORNL, as at other DOE laboratories, management conducts drills regularly to exercise these requirements. Some levels of preparedness should already exist at many federal facilities based on these requirements.

OSHA Occupational Safety and Health Administration
www.osha.gov

To a certain degree, what is required for CBRN preparedness is to extend the existing procedures and methods to cover additional situations and circumstances. In response to Homeland Security developments, additional procedures can be expected.

A large array of resources now available cover the topic of reducing risk and vulnerabilities of facilities to CBRN incidents. One such resource is from the United Kingdom's Office of the Deputy Prime Minister, *Precautions to Minimise Effects of a CBRN Event on Buildings and Infrastructure* (ODPM 2004). Although this document has a Crown copyright, it is apparently available to individuals and organizations for internal use. The document is useful because it addresses a continuum of prevention levels that covers pre-planning for risk and vulnerability assessment, through preventive measures, and on to decontamination procedures, if required. The limitations of this document include

oversimplification of some threats and an implied assumption that analysis with difficult-to-obtain numbers will provide the answers needed.

This document and others highlight the need for risk assessment and planning to reduce a facility's vulnerability to CBRN incidents. In order to pursue a graded approach to exposure reduction, some type of risk analysis is required. The Federal Emergency Management Agency (FEMA) has many resources available, having extended its focus beyond natural disasters to include protection of critical infrastructure. As a result, current information from FEMA is directly relevant for reducing the exposure of HVAC systems to CBRN incidents. In particular, FEMA has developed important information on risk assessment in a document on mitigating manmade hazards (FEMA 2003c) and has a series of risk management reports linked to its web site (http://www.fema.gov/fima/rmsp.shtm). One of these reports, addressed to the insurance, regulatory, and financial sectors (FEMA 2003a), offers some useful perspectives.

Risk assessment is an extensive topic, applicable to many different situations. One can assume that federal facilities have already evaluated industrial accident scenarios and done some planning for dealing with such incidents, but the many uncertainties in potential CBRN incidents make risk analysis especially difficult. Incidents such as terrorist attacks occur infrequently enough in the United States that there are few relevant records for analyzing any potential hazard. While many natural hazards are identifiable and even, in some cases, predictable, manmade hazards are, to a large extent, unpredictable. In addition, since resources on the reduction of CBRN vulnerabilities in HVAC systems are likely to be limited, some prioritization is necessary to evaluate where these efforts and expenditures will be applied.

Quantifying the value of risk reduction for manmade hazards is a questionable exercise, since putting a value on preventing an extremely unlikely scenario is neither simple nor believable in most cases. Measures for preventing industrial accidents and terrorism are difficult to model and quantify. Those interested in more academic treatments of the risk quantification and conceptualization issues can consult Kunreuther et al. (2004) and Chapman and Leng (2004). FEMA once suggested that in the absence of a viable quantitative method, we should "adopt a more subjective, qualitative approach focusing on criticality, vulnerability, and threat in making decisions and setting priorities" (FEMA 2003b, p. 17). Some simple quantification may be needed though.

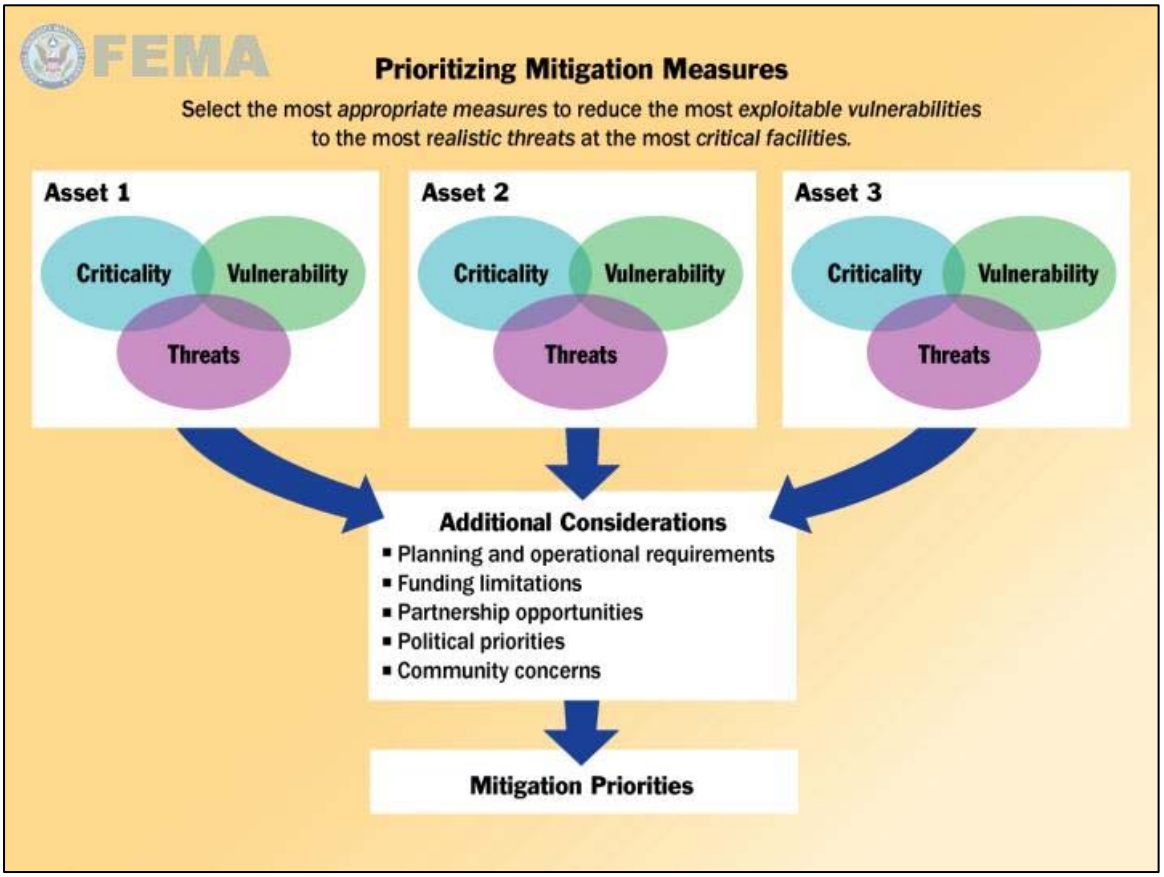


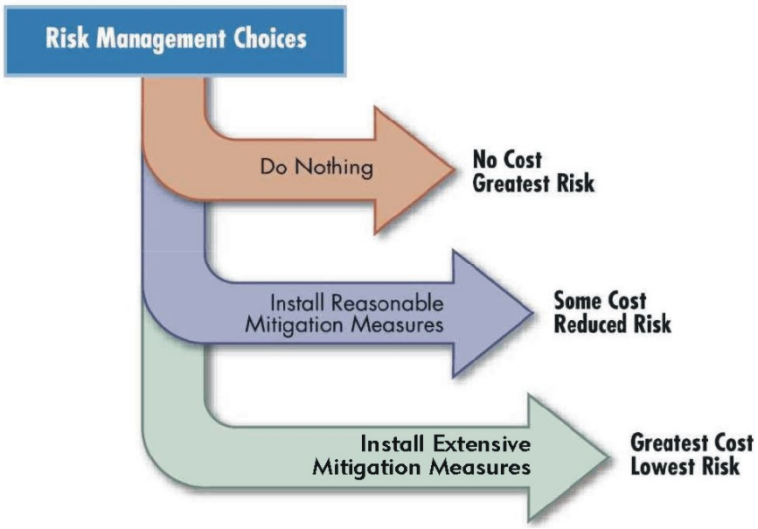
Fig. 1. Simple method for prioritizing mitigation measures.

The simple method diagrammed in Fig. 1 can be applied at different levels of an organization, with appropriate adjustments in concepts. For federal facilities, some levels of possible application are nationwide, region-wide, agency-wide, statewide, and facility-wide. For this document, an additional level of distinction involves examining assets within a specific facility based on the system-by-system coverage of the assets by the HVAC systems (i.e., determining which HVAC systems could affect which organizational assets in each facility).

FEMA has extended this general idea in attempting to quantify the risk assessment for facilities (FEMA 2003e). This quantification extension is useful in many ways, and will be used in this document The method uses the concept of "asset value" to replace the "criticality" factor in the figure above. Rating schemes are used to assign numeric values to asset value, vulnerability, and threat level. These three values are then multiplied to arrive at a score, and different scoring levels are assigned — green, yellow, or red (low, medium, or high) — to the total risk categories. Readers wishing to explore this quantification method in depth should consult the FEMA

reference manual (FEMA 2003e). The information provided is most useful at an agency-wide level of planning.

Considering these three elements of criticality, vulnerability, and threats, many CBRN threat issues were covered previously in this report. Table 2 presents one profile set of threat characteristics that can serve as a reminder of the threats covered previously, as well as providing additional details. The table includes an initial entry on the explosive threat for comparison.



Asset criticality or value must be determined by each organization based on internal factors or considerations. The vulnerabilities of HVAC systems must then be considered together with asset criticality to develop mitigation priorities. Funding limitations are expected to be a major factor affecting mitigation project possibilities. Readers can consult FEMA (2003b, 2003c, 2003e, and Appendix B of 2003a) to examine additional information on an overall process for mitigating CBRN threats against buildings.

Chapman and Leng (2004) provide more extensive information on quantification, simulation, and life cycle cost analyses related to large-scale hazards and risk management for buildings for those who need more information on those issues. FEMA is also developing a threat assessment tool.

FEMA notes that "in conducting the vulnerability assessment, it is important to ensure that the focus is not only on hazard reduction but also on preparedness, response, and recovery considerations. . . . it is critical to consider the secondary hazards that could arise from well-intended efforts to reduce vulnerabilities" (FEMA 2003c, p. 2-9).

Table 2. Threat profiles

Hazard	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Conventional Bomb/ Improvised Explosive Device	Detonation of explosive device on or near target; delivery via person, vehicle, or projectile.	Instantaneous; additional "secondary devices" may be used, lengthening the time duration of the hazard until the attack site is determined to be clear.	Extent of damage is determined by type and quantity of explosive. Effects generally static other than cascading consequences, incremental structural failure, etc.	Overpressure at a given standoff is inversely proportional to the cube of the distance from the blast; thus, each additional increment of standoff provides progressively more protection. Terrain, forestation, structures, etc. can provide shielding by absorbing and/or deflecting energy and debris. Exacerbating conditions include ease of access to target; lack of barriers/shielding; poor construction; and ease of concealment of device.
Chemical Agent	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/ containers; or munitions.	Chemical agents may pose viable threats for hours to weeks depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.	Air temperature can affect evaporation of aerosols. Ground temperature affects evaporation of liquids. Humidity can enlarge aerosol particles, reducing inhalation hazard. Precipitation can dilute and disperse agents but can spread contamination. Wind can disperse vapors but also cause target area to be dynamic. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place can protect people and property from harmful effects.
Biological Agent	Liquid or solid contaminants can be dispersed using sprayers/aerosol generators or by point or line sources such as munitions, covert deposits and moving sprayers.	Biological agents may pose viable threats for hours to years depending on the agent and the conditions in which it exists.	Depending on the agent used and the effectiveness with which it is deployed, contamination can be spread via wind and water. Infection can be spread via human or animal vectors.	Altitude of release above ground can affect dispersion; sunlight is destructive to many bacteria and viruses; light to moderate wind will disperse agents but higher winds can break up aerosol clouds; the micro-meteorological effects of buildings and terrain can influence aerosolization and travel of agents.
Nuclear Bomb	Detonation of nuclear device underground, at the surface, in the air or at high altitude.	Light/heat flash and blast/shock wave last for seconds; nuclear radiation and fallout hazards can persist for years. Electromagnetic pulse from a high-altitude detonation lasts for seconds and affects only unprotected electronic systems.	Initial light, heat and blast effects of a subsurface, ground or air burst are static and are determined by the device's characteristics and employment; fallout of radioactive contaminants may be dynamic, depending on meteorological conditions.	Harmful effects of radiation can be reduced by minimizing the time of exposure. Light, heat and blast energy decrease logarithmically as a function of distance from seat of blast. Terrain, forestation, structures, etc. can provide shielding by absorbing and/or deflecting radiation and radioactive contaminants.
Radiological Agent	Radioactive contaminants can be dispersed using sprayers/aerosol generators, or by point or line sources such as munitions, covert deposits and moving sprayers.	Contaminants may remain hazardous for seconds to years depending on material used.	Initial effects will be localized to site of attack; depending on meteorological conditions, subsequent behavior of radioactive contaminants may be dynamic.	Duration of exposure, distance from source of radiation, and the amount of shielding between source and target determine exposure to radiation.

Source: FEMA 2003c.

FEMA also advises that

> when addressing antiterrorism and other manmade hazard mitigation actions, you should recognize that many of these are sensitive and that information about them should be restricted to a very limited number of people. You must carefully consider whether each part of the process will be open to the public [or all employees] or whether for security reasons you will have only the planning team and perhaps a limited number of outside stakeholders (such as key public officials not on the planning team) discuss the best actions for [specific] facilities. (FEMA 2003c, p. 1-7)

An example of part of the FEMA threat assessment tool under development which examines overall risk scoring for basic commercial building systems and infrastructures is shown in Fig. 2 (FEMA Risk Management Project 452, "Methodology for Preparing Threat Assessments," to be published).

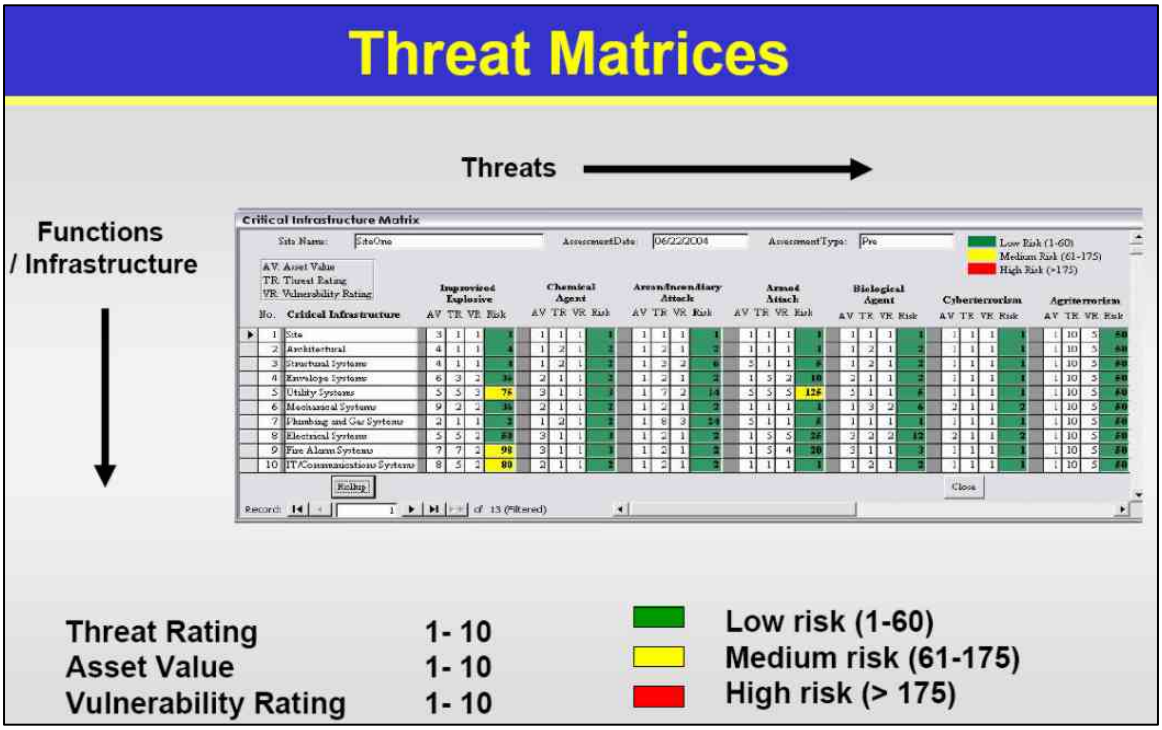


Fig. 2. Example of FEMA threat assessment tool under development.

Mitigation Technologies and Actions

What do the abbreviations RABIS, BAND, ARFCAM, RACIS, and PHILIS have in common? No, they are not new diseases. They are all highly advanced new technologies being developed by the Department of Homeland Security's (DHS's) Homeland Security Advanced Research Projects Agency (HSARPA) for the Bioinformatics and Assays Development (BIAD) Program. Advanced technologies will be examined first in this section to indicate the direction needed to improve U.S. abilities to mitigate CBRN incidents.

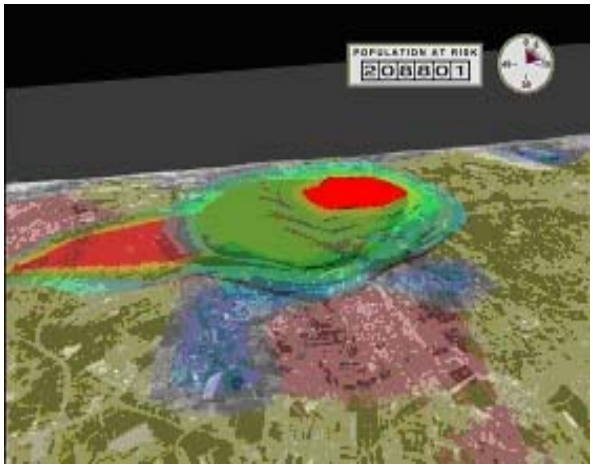
Why do we need advanced technologies for CBRN incident mitigation? Currently there is no truly real-time sensor capability for detecting the presence of deadly biological agents. Chemical sensing is available but needs improvement. Radiological sensors are available. The cost for most sensor capabilities needs to be reduced. We need more rapid processing of sensor signals. Many other improvements are needed.

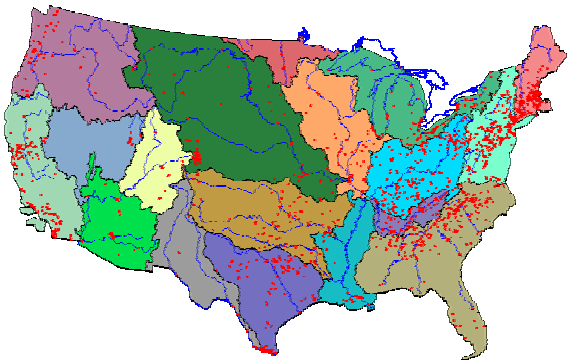
Briefly, the notional capabilities envisioned for the items listed above include the following:

- RABIS — Rapid Automated Biological Identification System
  - Real-time monitoring for buildings and selected outdoor locations and events
  - Enabler of "detect to protect" response to attacks
- BAND — Bioagent Autonomous Networked Detectors
  - Upgrade and expansion of previous system (BioWatch)
  - Reduced costs and expanded coverage
  - Support for other bioaerosol surveillance missions
  - Enabler of "detect to treat" response to attacks
- ARFCAM — Autonomous Rapid Facility Chemical Agent Monitor
  - "Detect-to-warn" system
  - Continuous facility monitoring
  - Monitoring of chemical warfare agents (CWAs) and high-priority toxic industrial chemicals (TICs)
  - Fully autonomous monitor capable of detecting dangerous levels of chemicals with a response time that provides sufficient warning to enable effective protection by limiting exposure

- LACIS — Lightweight Autonomous Chemical Identification System
    - Fully autonomous and hand portable system with ability to detect allowable limits within 2 minutes
    - Capability to identify CWAs and high-priority TICs analytes
    - Local control unit simultaneously providing operational state and system status for a minimum of ten detectors
- PHILIS — Portable High-Throughput Integrated Laboratory Identification System
    - Rapidly deployable field laboratory in a box capable of analyzing thousands of samples per day
    - Capability to identify and help characterize chemically contaminated areas
    - Lower detection limit meeting or lower than Environmental Protection Agency (EPA) permissible exposure limits (PELs) for the presence of CWA and TIC contamination

In addition to HSARPA technology development, other efforts are ongoing. For example, several partners are working with researchers at ORNL to design and develop a "system of systems," called SensorNet, to provide nationwide detection and assessment of CBRNE threats. The goal, as sensors become available for different threat agents, is real-time detection, identification, and assessment of CBRNE hazards. In addition to providing a data highway for detection systems, the overall "system" is also intended to include modeling capabilities and incident response protocols and direction to help mitigate CBRNE incidents. SensorNet has been deployed in Tennessee in some locations and at Fort Bragg in North Carolina, and has also been tested in other locations. The eventual coverage is intended to be nationwide. SensorNet is being considered as a key piece of the Guardian Installation Protection Program (see p. 6).





The Special Projects Office of the Defense Advanced Research Projects Agency (DARPA) is pursuing projects in many of these same areas, in a program area called Defense against

Chemical, Biological, and Radiological Weapons. Many national laboratories are also working on these technology areas. Project and program listings given here are not meant to be all-inclusive.

Moving from future-looking technologies to the present, many technologies are now available to help with mitigation of CBRN events. For instance, chemical agent detectors are being used in the Washington, D.C., subway system; and efforts to expand the detectors to Boston subways have begun.

Many CBRNE mitigation technologies are provided by organizations that belong to the NBC (Nuclear, Biological, and Chemical) Industry Group (http://www.nbcindustrygroup.com). Members of this group support nuclear, chemical, and biological warfare defense activities. In addition to military defense against chemical and biological warfare, interests of the group encompass domestic preparedness against chemical and biological terrorism and support for the Chemical Weapons Convention and other treaties. A handbook compiled by the group (http://www.nbcindustrygroup.com/handbook/index08.htm) identifies currently available products and services. The topics in the NBC Industry Handbook include

- Agent characteristics
- Contamination avoidance
- Individual protection
- Collective protection
- Decontamination
- Communications
- Medical systems
- Demilitarization
- Research & development
- NBC services

The most extensive listings are under "NBC services." As noted on pp. 13–14 above, the description of agent characteristics is a compact set of characteristics for several chemical and biological agents, grouped according to invasive method.

It should be noted that the NBC Industry Group is not all-encompassing of key organizations and technologies, so one must look beyond what is offered on the NBC web site.

HVAC Systems and Threat Profiles

In order to plan reasonably to define CBRN threat mitigation priorities and strategies, one must consider both HVAC system characteristics and CBRN threat characteristics.

With HVAC systems one is concerned with airborne agents or contamination, so other vectors of delivery can be dropped from consideration. For threats from outside a building, HVAC systems should be shut off to reduce introduction of outside air into a building. All fan devices (e.g., exhaust fans) should be shut off. All doors and windows should be shut tightly, and elevators should not be used because they draw air flows into buildings.

The HVAC response for biological or radiological agents released indoors is much the same as for an outdoor release: turn off all HVAC fans to prevent further dispersal, limit spread of contamination, and isolate the building.

In the case of an indoor release of a CBR agent, one important first response is to evacuate the building, upwind. Other important responses become much more complicated. For a chemical release indoors, mitigation by dissipation is usually considered most effective, so leaving everything running is considered preferable in most cases. A fairly extensive report — *Protecting Buildings from a Biological or Chemical Attack: Actions to Take before or during a Release*, prepared by DOE's Lawrence Berkeley National Laboratory (LBNL) (Price 2003) — discusses actions to take during an incident as well as actions to mitigate such incidents. The report (available at http://securebuildings.lbl.gov/) is particularly useful for gaining an understanding of the response issues related to chemical or biological incidents. Given that responses to radiological or nuclear incidents would be similar to responses for a biological incident, the advice for biological incidents can also be extended to these other types.

Just as the graded approach to HVAC system protection must consider the overall efforts to mitigate CBRN incident effects, the critical issues here are that

- mitigation actions are probably more important than mitigation technologies, and
- HVAC actions and technologies are bound up in other actions and technologies in many mitigation responses.

So in the graded approach, mitigation priorities will include response actions — before, during, and after a CBRN incident — in synergistic combination with the priorities for HVAC system or technology measures.

Technology Mitigation / Cost Profile

Just as the nature of CBRN threats must be understood in attempting to establish priorities in mitigation measures, the nature of the "grades" of technological fixes must also be understood. The LBNL report highlights the importance of knowing whether to evacuate or not, depending on the type of incident. Evacuation and sheltering-in-place are part of the typical first line of response to CBRN attacks. However, some buildings, such as the main buildings of U.S. embassies on foreign soil, may need significantly enhanced protection like multiple levels of filtration and continuous positive pressurization of critical building assets, as evacuation may be dangerous.

Figure 3 shows, in approximate terms, the change in costs as the level of technological protection of HVAC systems against CBRN incidents increases. Note that the cost scale is logarithmic — costs increase by a factor of 1,000 for each step on the scale. Thus, a wide range in costs can be found, but the general trends can be understood from this graph: as the level of protection goes up, costs go from hundreds to millions of dollars. In most cases, some mix of technologies is likely to be appropriate. Again, funding limitations are likely to severely limit what can be done.

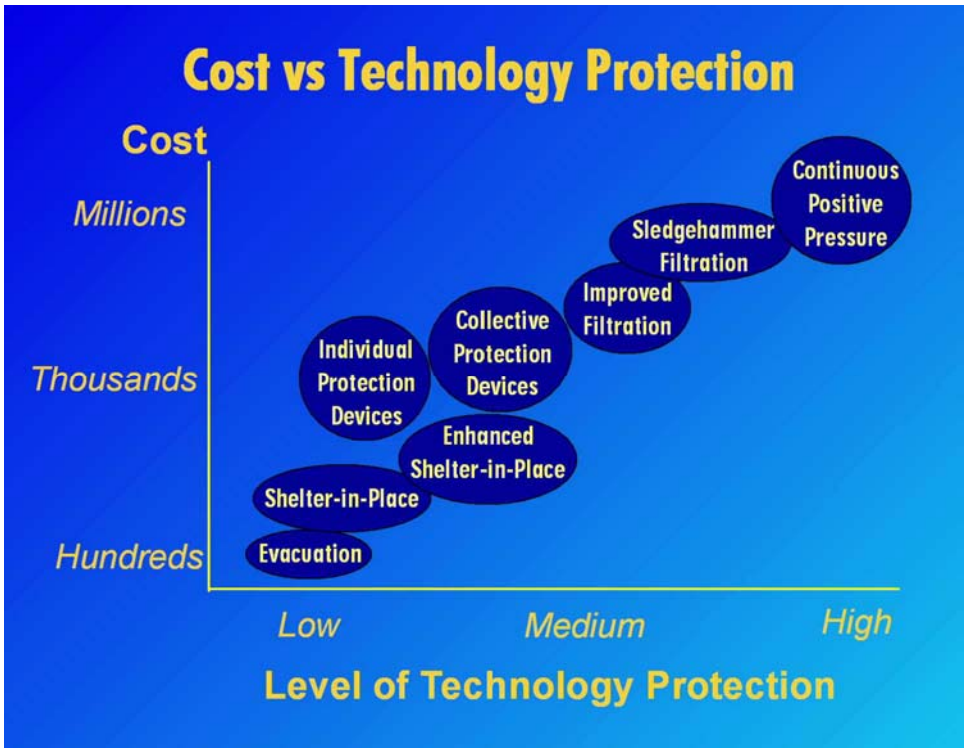


Fig. 3. Acceleration of costs as technological protection increases.

The items shown in Fig. 3 do not cover all the categories of technologies that could be considered, but the general trend of technologies is indicated. At the low end, procedures for

evacuation and sheltering-in-place should be developed and implemented. Methods for control of HVAC systems for different types of CBRN events should be developed. If high-end technologies such as continuous positive pressure equipment are installed, people should be informed of the limits of any such equipment and what parts of buildings can be considered safer in case an external CBRN incident occurs.

The high-end technologies generally attempt to isolate a building from potential external CBRN threats by filtering out CBRN agents that might come through the HVAC systems to make these systems secure, possibly killing biological agents that are very small, and pressurizing the building with the secure HVAC systems to keep CBRN agents from entering through any other means. This approach typically requires that the building envelope be sealed well.

If facilities are to receive modifications to HVAC systems and development of incident procedures, building occupants need to understand what those systems and procedures are and how the protective systems are to be deployed. Occupants may also need training on the proper deployment of protection equipment and systems and on the modifications to building HVAC systems and related hardware.

The range of activities, actions, and technologies that could be considered to prepare people and HVAC systems for increased security against CBRN incidents is large. An Internet search using the terms *homeland* + *security* + *products* will give readers some idea of the range.

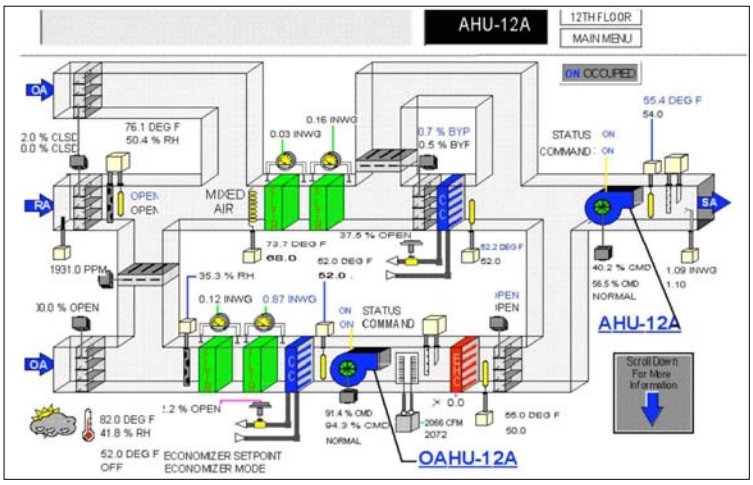
Energy Efficiency

Finally, since FEMP is primarily concerned with the energy efficiency of federal facilities, readers should note that many higher-end mitigation technologies have the potential to significantly increase energy use and costs. Federal agencies, and energy managers in particular, have a special

interest in the relationships between building security and energy usage. Hadley (2002) presents many of the basic issues related to building security and energy efficiency and also presents ways energy improvements can help enhance security. FEMP has also developed a white paper covering some of the positive links between ensuring security and improving energy efficiency, as well as areas where tradeoffs may be required (Harris 2002). This paper provides information on the possibilities for synergistic benefits, as well as on tradeoffs.

HVAC System Vulnerability Mitigation Guides

As indicated previously, the number of publications on building security and security guidelines has grown significantly in the last two years and continues to grow quickly. Several guides are mentioned here that address HVAC mitigation technologies, strategies, and actions.



In addition to the LBNL report on protecting buildings (Price 2003), LBNL has also developed user tools to help facility managers work through the vulnerability assessment process. The Building Vulnerability Assessment & Mitigation Program (BVAMP) helps develop building-specific advice regarding vulnerabilities in order to

- help improve emergency preparedness,
- develop building HVAC system control protocols for use during incidents or other emergencies,
- plan for shelter-in-place responses, and
- evaluate access restrictions that may be needed for building systems and information.

The tool itself comes as a compiled Java file that runs on the Java Virtual Machine, with all modules compiled together in a Java archive (jar) file (LBNL 2004). The zip file containing the jar file also has versions of the building questions and building walkthrough process that can be read with a word processor, for those who want a preview before starting the process.

As mentioned previously, the Edgewood Chemical Biological Center (ECBC) and the Army Corps of Engineers have released a guide (technical instructions) in draft form that can be accessed via the Internet entitled *Protecting Buildings and Their Occupants from Airborne Hazards* (USACE 2001). This guide provides information in both form and substance not typically found in other guides and should be studied, along with the

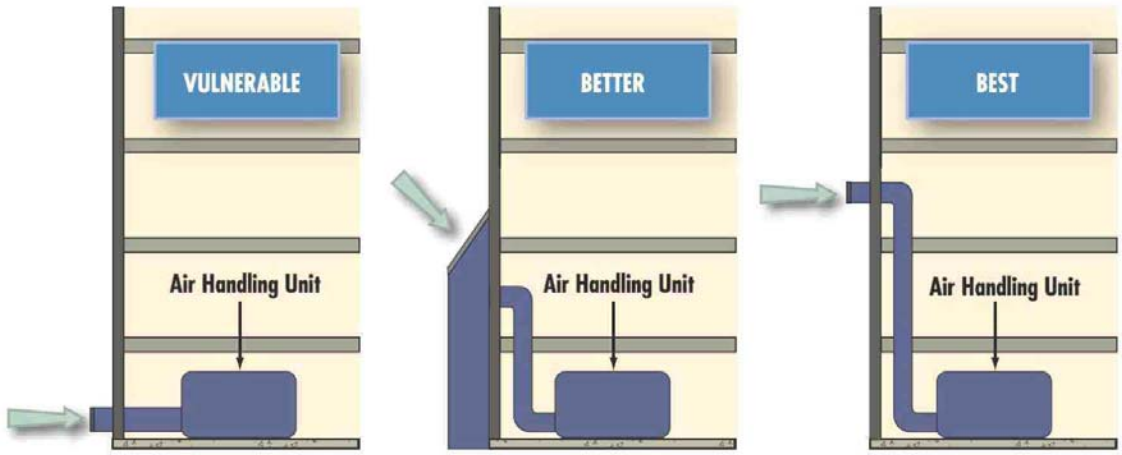
advice from the United Kingdom (ODPM 2004), LBNL, and www.ready.gov, to scope out potential vulnerability mitigation options. The ECBC guide covers

- pertinent facts about airborne hazards,
- how to determine a building's protective capability,
- architectural and mechanical design features for protection,
- security measures to prevent an internal release,
- protective actions for perceptible hazards,
- developing a protective-action plan, and
- applying air filtration systems to buildings.

Some of the measures are more practical for new construction or major modifications.

Other guidance related to these topics can be found in the following sources:

- *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks* (NIOSH 2002)
- *Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attacks* (NIOSH 2003)
- *Risk Management Guidance for Health, Safety, and Environmental Security under Extraordinary Incidents* (ASHRAE 2003)
- *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings* (FEMA 2003e)



Risk Input Scales and Scoring

Vulnerability and risk assessment methodologies are extensive and varied. Surveys of these methods are continually conducted. Current results of such a survey and analysis by the DHS are not publicly available. Although vulnerability and risk assessment methods can be either simple or more involved and complicated than the methods presented here, the approach used here illustrates one basic means of assessing risk for building HVAC systems. This method uses a risk equation to calculate overall, relative scores. Other methods, such as simple checklists, comparison ratings, and specialized risk matrices, can also be used.

The basic method presented here for prioritizing CBRN incident mitigation measures involves the following steps:

- Selection of assets, whether buildings, people, departments, production lines, or other, to rank the value of each asset relative to that of other assets (criticality ranking)
- Mapping of assets to specific HVAC systems for any HVAC-specific vulnerability assessments
- Analysis of additional factors driving or limiting options for mitigation measures
- Assessment of the vulnerabilities of each asset and its related HVAC system to CBRN incidents
- Ranking of CBRN threat potential (threat assessment)
- Performing a vulnerability risk assessment that considers asset criticality, threat potential, and vulnerabilities
- Setting/staging mitigation priorities: actions, technologies, strategies, etc.

Each element in this process is fairly complex and challenging in and of itself. Asset selection and rating is necessary in order to have a reasonable initial framework for analyzing ways to mitigate potential CBRN incident impacts on HVAC systems. Scoring can be numerical or comparative (pair-wise priority), although only numerical scoring will be presented here.

Asset Selection and Rating

Defining an asset categorization or classification scheme is the first challenge. Different schemes may be needed for different types of facilities and occupancies. The cornerstone of any security strategy is an understanding of an organization's assets. Some understanding of asset value is also

necessary to effectively prioritize how critical each asset is to the mission of an organization. Contacts with organizational real property managers are probably necessary to some degree to select and categorize assets. Asset management is a large field that is not possible to cover in this short document, and classification and rating the criticality (value) of assets is part of asset management.

In its *Security Risk Management Guide* (FAA 2002), the Federal Aviation Administration defines an asset as "as any person, place, thing, or commodity, for which there is a safeguarding requirement." The notion of a "thing" could be extended to many possible categories, including departments, process lines, laboratories, and test cells. Similarly, groups of people or places or commodities could also be chosen as assets. The FAA guide notes that identification of assets to be safeguarded is a requirement in the security risk management process.

Classification of assets should also be coordinated with the mapping of HVAC systems to assets served. Once assets to be rated for criticality are defined, levels of criticality need to be selected. These levels can usually be handled most easily by correlating descriptions of the levels with numerical values, with higher values meaning those assets more critical to the organization. Figure 4 shows an example of an asset value scale from FEMA's reference manual (2003e). Some practice with such scales is probably useful before conducting a full-scale analysis so as to develop an understanding of the interactions between vulnerability and threat scales and to develop the most reasonable category descriptions describing rating categories. Only assets with the highest values may need to be considered initially. Building occupants (employees and visiting workers at a minimum) should probably be considered in overall groups as assets also, with a value of 10 out of 10, regardless of whether smaller groups of the same people are classified as assets, since many lower-cost actions with important benefits can be accomplished with people.

Asset Value	
Very High	10
High	8-9
Medium High	7
Medium	5-6
Medium Low	4
Low	2-3
Very Low	1

Fig. 4. Example of an asset value scale. *Source:* FEMA 2003e.

Vulnerability Assessments

The discussion here assumes that, as asset classifications have been developed, mapping of assets to HVAC systems has been integrated into the asset classification scheme — that HVAC systems are intrinsically part of the asset categories. As indicated previously, the vulnerability assessment procedures (BVAMP) developed by LBNL (2004) are probably the most useful and can be used together with the guidance documents from NIOSH and others to develop vulnerability assessment procedures specific to the assets being evaluated. Users may wish to map types of vulnerabilities or vulnerability patterns to a simple scale as shown in Fig. 5 — or one might use quick, reactive scoring to test results. For numerical evaluation, some type of rating score will be needed for each asset. Some development work may be necessary to make the vulnerability scales match the types of assets and HVAC systems being evaluated.

Scale	Vulnerability
0	Little or None
1	Medium Low
2	Medium
3	Medium High
4	High
5	Very High

Asset	Rating
Asset 1	
Asset 2	
Asset 3	
Asset - - -	

Fig. 5. Examples of a vulnerability scale and an asset rating form.

Threat Assessment

This report has covered the potential CBRN threats in detail because the nature of the threats is complex. CBRN agents are often referred to as weapons of mass destruction (WMDs), although effective (deadly) use is inhibited by many factors. Some parties tend to promote fears related to these threats, while others downplay the potential for extensive deadly results. Economic disruption (although an area well outside the scope of this report) may be a more troublesome consequence of limited CBRN attacks, and possibly more destructive, as response with extensive deadly force might be morally out of scale, while less lethal responses may not have been prepared effectively and also might be seen as inappropriate for other reasons.

CBRN threat assessment ratings and approaches are likely to change depending on proximate events. A rating given in the absence of any immediate elevated threat condition is, by nature, nebulous, since the likelihood of any CBRN incident is low for most federal facilities. In many cases, the level of threat from a

Asset	Threat Level
Asset 1	2
Asset 2	2
Asset ---	2

CBRN incident will be similar, if not the same, for all assets at a given federal facility. Absent any immediate factors suggesting elevated threat level, the probability of any given CBRN incident might be considered low. Possibly, different numerical threat levels could be assigned to different types of CBRN threats. However, care should be taken that threat level, given its greater uncertainty, does not unduly influence any final scoring of overall risk. Ignoring threat could hinder wider-scale integration.

A more immediate indication of elevated threat conditions would be expected to lead to a reevaluation of the threat level and modification to an overall risk analysis. A two-stage threat assessment might be needed. One possible second-level assessment factor set shown by FEMA (2003e, p. 1-24) and credited to the Kentucky Office of Homeland Security is shown in Fig. 6.

Threat Level	Threat Analysis Factors				
	Existence	Capability	History	Intentions	Targeting
Severe (Red)	●	●	●	●	●
High (Orange)	●	●	●	●	❑
Elevated (Yellow)	●	●	●	❑	
Guarded (Blue)	●	●	❑		
Low (Green)	●	❑			

● Factor must be present ❑ Factor may or may not be present

Fig. 6. Chart for scoring threat level. *Source:* FEMA 2003e, p. 1-24.

One possible two-level method for scoring threat level would assign numerical scores to low (green) through severe (red) threat conditions — e.g., 0 for green through 4 for red. These immediate-threat-condition scores could be added to previous asset-threat-level scores to arrive at a new, two-level score. Other secondary, proximate-cause scoring methods might also be developed.

Explosive threat might also be included in any analysis, to provide an overall comparison vector (set of risk scores) for all assets being analyzed. Although CBRN threat levels may be low, the explosive threat level could be very high.

Risk Scoring

Risk scoring involves generation of the overall scoring of the factors presented above. Some comparison of initial results with intuitive expectations and workable scoring ranges might be

helpful in tuning the scales used for the threat, asset criticality, and vulnerability scores. Typically the category scores would be multiplied:

$$\text{Risk} = \text{Asset criticality score} \times \text{Vulnerability score} \times \text{Threat level score}$$

The calculated risk values can then be used to assign risk categories. The scales may need tuning to arrive at results that have the most meaning to users. Final scores then provide input to the combined analysis of risk and external factors such as resources for making changes.

Combined Analysis of Risk and Additional Factors

Once users are satisfied with the level of information provided by risk calculations, a final field assessment and analysis of risk and additional factors are conducted. Then prioritization and staging of CBRN incident mitigation options for HVAC systems can begin. Additional factors for the final analysis include such things as

- funding limitations,
- political priorities,
- planning and funding horizons and cycles,
- operational and system configuration factors,
- graded-approach common-sense factors such as facility age and condition that were not properly considered in the scoring, and
- synergistic funding and procedure, capital, or project alignment options.

This analysis should set the stage for implementing and staging mitigation options. Integration into larger organizational planning efforts would require consistency in approach.

Mitigation Priority Example

To provide a sense of how all the information and methods can work together, an example is provided below. This example is not definitive and not meant to be fully consistent with current security readiness or procedures at federal facilities. Rather, it is meant to show a practical application that integrates several concepts previously discussed.

The fictitious agency considered here, Agency X, is a tenant occupying two floors of an office building somewhere in middle America. After the Oklahoma City incident, security against explosive threat was improved, which included securing the building perimeter. Access to the building now requires screening upon entry, with a known destination inside; but once inside, people could find ways to move around on most floors, including the two floors belonging to Agency X.

A security screening directive has been issued by Agency X to all locations, including the part of the agency (local unit) on the two floors in this office building. This directive requires the local unit to examine security risks, including CBRN risks, and the directive has a topical area checklist to cover in the security screening. The Agency X local unit (AXLU) works through the checklist and finds that potential risks related to the HVAC systems in the building must be examined. AXLU contacts building management and its operating contractor (BMOC) to explain what it is now required to do and to ask if any help can be provided.

Finding a guide on the Internet titled *Mitigation of CBRN Incidents for HVAC Systems in Federal Facilities*, AXLU considers how to examine possible security risks for the HVAC systems in its building, and it uses this guidance to respond to questions posed by BMOC. AXLU develops an initial asset criticality list and asks BMOC to map the HVAC systems to the asset list and also to provide comments on the asset list.

AXLU examines the ODPM (2004) material and the LBNL (2004) BVAMP questions and walk-through items. A determination is made that significant building systems expertise is needed to reasonably evaluate HVAC systems in the context of an overall program of CBRN incident mitigation, and a delay of almost a year occurs while a means of procuring the required expertise

is developed and the expertise is procured. The outside experts can be retained only for a short time due to funding limitations.

With the needed expertise on board, AXLU conducts a walk-through assessment of its systems, building areas, and the roof to develop reasonably final results for its overall analysis. Threat factors are ignored, and only three assets are used: people overall and all agency property on each of the two floors of the building. An analysis of risk findings and additional factors is conducted. AXLU determines that only limited funds are available for any mitigation measures, and BMOC is also fairly constrained in what it can do. AXLU and BMOC decide to pursue the following mitigation actions:

- Since people have high importance, AXLU determines that some minimal training is required for all personnel to inform them of CBRN threats and actions being taken
- BMOC determines that all agencies in the building would benefit from similar training and agrees to help develop the training session in cooperation with other agencies in the building. Other agencies are asked to participate in the training development, and three other agencies agree to provide a representative to participate. The initial training material is developed and presented to the personnel of Agency X and any others interested. Three sessions are required to accommodate everyone for this initial training.
- Based on the materials reviewed, AXLU determines that a computer resource–sharing agreement is needed with Agency Y in the next state, so that in the event of inability to use computer resources, either agency would be ready and could use the other's computer resources during a short transitional period of detoxification, cleanup, or other disruptive corrective actions.

- AXLU and BMOC determine that the main HVAC systems are reasonably secure, being in locked mechanical rooms on the same floors occupied by AXLU. An outdoor air supply fan on the roof, which provides air to the main HVAC systems, is less secure. BMOC agrees to install extra security cameras on the outdoor air fan and roof and include those camera views in regular security scans.
- The building does not have sensors to measure wind speed and direction. BMOC agrees to purchase and install these sensors and connect them to the building energy

management system (this EMS is the only system that could handle the sensors). Installation of local readouts of these sensors on the two floors occupied by AXLU is paid for by AXLU.

- There is no quick means of shutting either the HVAC or outdoor air fans off in an emergency. AXLU and BMOC agree to co-fund changes to building controls to develop a quick means of turning these fans off and on. In addition, an indicator of outdoor air fan status is added to several locations in the building, including the AXLU space. AXLU also pays to have BMOC install reliable, multi-attribute status indicators of the HVAC fans on its two floors.
- AXLU purchases 12 CBR agent protective face masks for specific personnel, 7 on one floor and 5 on the other; and these 12 people receive instruction on use of the masks. (BMOC decides to buy a few also.) Practice drills on use of the masks are conducted each year, and these personnel are wardens with specific responsibilities during any emergencies.
- AXLU funds are used to install dampers that shut off outdoor air to the HVAC systems on the floors occupied by AXLU. Three of the personnel with face masks on each AXLU floor are instructed in how to shut off outdoor air to the units using these dampers, as well as how to shut off and turn on the HVAC units in an emergency. Shutoff and turn-on procedures are practiced once a year. A concealed, sealed security compartment on each AXLU floor has the key to the mechanical room for a real emergency.
- AXLU and BMOC develop new emergency management procedures, including threat identification procedures, evacuation and shelter-in-place procedures based on wind speed and direction, and communication protocols for different types of incidents.

This list could easily be much longer for many situations. All the items described here had to be completed with very limited resources, so documentation was not extensive, and further improvements were needed. The training sessions continued to be offered about once a year, were picked up and enhanced by FEMA for wider use, and were expanded to include specific types of personal protective equipment available for attendees to try out. After waiting seven years for funding requests to work their way through the system, AXLU installed an enhanced filtration system that did not have an excessive pressure drop on the outdoor air system.

Conclusion

Homeland security efforts, including development of improved methodologies and technologies, continued in 2004 and will continue for the foreseeable future. The country has seen multiple attempted or completed large-scale attacks against civilian populations by extremists. Emergency preparedness throughout the United States has expanded in scope. Critical infrastructure has been identified as needing protection. Weapons of mass destruction (WMDs) have been identified as the most serious threat. Increased abilities to mitigate WMD attacks have been recommended by prestigious bodies. Information and guidance on how to protect facilities against WMD attacks have proliferated in the past two years. Federal agencies have promulgated directives requiring increased security against WMD attacks. Federal facility managers have asked FEMP whether there is any assistance that can be provided to deal with the directives, especially related to building ventilation systems.

This short guide summarizes information related to mitigation of a subset of WMD incidents for federal facilities, although the information can be applied much more broadly than federally. Because WMDs can be scoped as comprising CBRNE agents, the WMDs addressed in this document are actually a subset involving only CBRN agents.

Using the information in this guide, together with some of the reference resources available on the Internet, federal facility managers should be able to plan an initial assessment of possible CBRN mitigation strategies for HVAC systems. The ability to conduct a final field assessment and analysis that allow CBRN incident mitigation priorities to be established for facility assets and the HVAC systems that serve them is expected to be problematic because the required expertise does not appear to be readily available. The development of capable CBRN incident analysts and experts will require training and accrued experience over time.

Following the initial setting of CBRN incident mitigation priorities, annual refinements to the assessment process and mitigation priorities should be expected. Given an apparent lack of unified assessment processes at this time among and within federal agencies, some gradual alignment and eventual standardization of these procedures should be pursued (e.g., the FEMA threat assessment tool [FEMA risk management project 452], which is a step in this direction; see p. 25 above). Methods for HVAC system assessments are available at this time but may require extensions to be more effective. Some pilot assessment and mitigation measure implementation projects appear to be needed.

The importance of people as an asset category has been stressed and should be given high emphasis throughout the process. The probable greater importance of mitigation actions and procedures compared to hardware technologies for HVAC system and CBRN incident mitigation solutions has also been emphasized. This emphasis may change as new technologies are developed and deployed. This relative importance is expected to hold true for most federal facilities.

Current OSHA requirements related to emergency preparedness may be inadequate to deal with possible CBRN incidents, so increased training and exercises related to the full range of responses needed for different CBRN incidents also appear to be needed at federal facilities. Increased levels of response to CBRN incident mitigation probably also include significant new technologies, many of which are only concepts at this time.

Energy efficiency should not be abandoned in the quest for security. FEMP has developed some initial ideas about synergistic system opportunities that apply to buildings, HVAC systems, and increased CBRN incident mitigation security. Significant additional work appears needed to better develop these ideas, reasonable methods of application, and some scaling of potential benefits from different approaches.

References

ASHRAE. 2003. *Risk Management Guidance for Health, Safety, and Environmental Security under Extraordinary Incidents*. Presidential Report of the American Society of Heating, Refrigerating and Air-Conditioning Engineers, Atlanta. http://xp20.ashrae.org/about/extraordinary.pdf (accessed Oct. 4, 2004).

CDO. 1950. *Survival under Atomic Attack*. NSRB Doc. 130, U.S. GPO O-1950. National Security Resources Board of the Civil Defense Office, Washington, D.C. http://www.schouwer-online.de/technik/zivilschutz_atomicattack.htm (accessed Oct. 20, 2004).

Chapman, C., and C. J. Leng. 2004. *Cost-Effective Responses to Terrorist Risks in Constructed Facilities*. NISTIR 7073. National Institute of Standards and Technology, Building and Fire Research Laboratory. http://www.bfrl.nist.gov/oae/publications/nistirs/7073.pdf (accessed Nov. 10, 2004).

Davis, L. E., et al. 2003. *Individual Preparedness and Response to Chemical, Radiological, Nuclear, and Biological Terrorist Attacks: A Quick Guide.* RAND Corp., Santa Monica, Calif. http://www.rand.org/publications/MR/MR1731.1/MR1731.1.pdf (accessed Oct. 5, 2004).

DHS. 2003. Radiological Dispersion Devices Fact Sheet. Feb. 10. http://www.dhs.gov/dhspublic/display?content=4232 (accessed Oct. 19, 2004).

DOD. 2002. *DoD Minimum Antiterrorism Standards for Buildings.* UFC 4-010-01. U.S. Department of Defense, Washington, D.C., July. https://pdmcx.pecp1.nwo.usace.army.mil/library/ufc/4-010/index.php (accessed Jan. 21, 2005).

DOS. 1995. *Structural Engineering Guidelines for New Embassy Office Buildings* (Limited Official Use Only). U.S. Department of State, Bureau of Diplomatic Security, August.

FAA. 2002. *Security Risk Management Guide*. Federal Aviation Administration Acquisition System Toolset. Federal Aviation Administration, Washington, D.C. http://fast.faa.gov/Riskmgmt/Secriskmgmt/secrisktoc.htm (accessed Nov. 3, 2004).

FEMA. 2003a. *Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings*. FEMA 429. http://www.fema.gov/fima/rmsp429.shtm (accessed Nov. 10, 2004).

FEMA. 2003b. *Integrating Manmade Hazards into Mitigation Planning.* Resource material developed for an Emergency Management Institute workshop, June 12, 2003. Federal Emergency Management Agency, Washington, D.C. http://www.fema.gov/doc/fima/antiterrorism/resourcematerials.doc (accessed Oct. 22, 2004).

FEMA. 2003c. *Integrating Manmade Hazards into Mitigation Planning.* FEMA 386-7, Version 2. Federal Emergency Management Agency, Washington, D.C. http://www.fema.gov/fima/planning_toc6.shtm (accessed Oct. 25, 2004).

FEMA. 2003d. *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*. FEMA 427. Federal Emergency Management Agency, Washington, D.C. http://www.fema.gov/pdf/fima/427/fema427.pdf (accessed Oct. 4, 2004).

FEMA. 2003e. *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings*. FEMA 426. Federal Emergency Management Agency, Washington, D.C. http://www.fema.gov/pdf/fima/426/fema426.pdf (accessed Oct. 4, 2004).

Hadley, S. W. 2002. *Building Assurance: September 11 and National Security Implications for the Built Environment.* ORNL/M02-113973. Oak Ridge National Laboratory, Oak Ridge, TN, April 2.

Harris, J., W. Tschudi, and B. Dyer. 2002. *Securing Buildings and Saving Energy: Opportunities in the Federal Sector.* DOE Federal Energy Management Program white paper. http://www.eere.energy.gov/femp/pdfs/security_sustain_whitepaper_ final_12aug.pdf (accessed Oct. 6, 2004).

Kunreuther, H. et al. 2004. *Risk Analysis for Extreme Events: Economic Incentives for Reducing Future Losses*. NIST GCR 04-871. National Institute of Standards and Technology, Building and Fire Research Laboratory, Gaithersburg, Md. http://www.bfrl.nist.gov/oae/publications/gcrs/04871.pdf (accessed Nov. 10, 2004).

LBNL. 2004. Building Vulnerability Assessment & Mitigation Program (BVAMP). http://securebuildings.lbl.gov/BVAMP.html (accessed Oct. 1, 2004). Web site with linked documents.

McMurrey, David A. 2002. Immediate Effects of a Nuclear Attack. http://www.io.com/~hcexres/tcm1603/acchtml/caus_ex.html (accessed Oct. 8, 2004). Page on the web site *Online Technical Writing* (http://www.io.com/~hcexres/tcm1603/acchtml/acctoc.html).

NAE. 2004. *Radiological Attack, Dirty Bombs and Other Devices*. National Academy of Engineering. http://www.nae.edu/NAE/pubundcom.nsf/weblinks/CGOZ-46NVG/$file/radiological%20attack.pdf (accessed Oct. 7, 2004). Possibly a draft document under comment.

NIOSH. 2002. *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks.* NIOSH Publication 2002-139. National Institute for Occupational Safety and Health, Washington, D.C. http://www.cdc.gov/niosh/bldvent/2002-139.html (accessed Oct. 1, 2004).

NIOSH. 2003. *Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attacks*. NIOSH Publication 2003-136. National Institute for Occupational Safety and Health, Washington, D.C. http://www.cdc.gov/niosh/docs/2003-136/2003-136.html (accessed Oct. 1, 2004).

NRC. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* National Research Council, Washington, D.C. http://www.nap.edu/html/stct/index.html.

ODPM. 2004. *Precautions to Minimise Effects of a CBRN Event on Buildings and Infrastructure.* Office of the Deputy Prime Minister Publications, Wetherby, United Kingdom. http://www.odpm.gov.uk/stellent/groups/odpm_fire/documents/page/odpm_fire_029042-10.hcsp (accessed Oct. 4, 2004).

Office of the President. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Office of the White House, Washington, D.C. http://www.whitehouse.gov/pcipb/physical.html (accessed Oct. 8, 2004).

OTA. 1979. *The Effects of Nuclear War*. Office of Technology Assessment. http://www.wws.princeton.edu/cgi-bin/byteserv.prl/~ota/disk3/1979/7906/ (accessed Oct. 6, 2004).

Price, P. N., et al. 2003. *Protecting Buildings from a Biological or Chemical Attack: Actions to Take before or during a Release*. LBNL/PUB-51959. Lawrence Berkeley National Laboratory, Berkeley, Calif. http://securebuildings.lbl.gov/images/BldgAdvice.pdf (accessed Oct. 1, 2004).

USACE. 2001. *Protecting Buildings and Their Occupants from Airborne Hazards*. TI 853-01. U.S. Army Corps of Engineers. http://buildingprotection.sbccom.army.mil/downloads/reports/airborne_hazards_report.pdf (accessed from Edgewood Chemical Biological Center of the Army, Oct. 1, 2004).

U.S. Air Force. N.d. (ca. 1997 based on references). *Installation Force Protection Guide*. U.S. Air Force, n.p. http://www.wbdg.org/media/pdf/installation_force.pdf (accessed Oct. 2004).