



FINAL REPORT NCEMBT-091027

DEVELOPMENT OF ASSESSMENT PROTOCOLS FOR SECURITY MEASURES - A SCOPING STUDY

OCTOBER 2009

William Bahnfleth
James Freihaut
Justin Bem
The Pennsylvania State University

T. Agami Reddy
Steven Snyder
Drexel University

Davor Novosel
National Center for Energy Management and Building Technologies



FINAL REPORT NCEMBT-091027

**NATIONAL CENTER FOR ENERGY MANAGEMENT
AND BUILDING TECHNOLOGIES TASK 06-11:
DEVELOPMENT OF ASSESSMENT PROTOCOLS FOR
SECURITY MEASURES - A SCOPING STUDY**

OCTOBER 2009

Prepared By:

William Bahnfleth, Principal Investigator
James Freihaut, co-PI
Justin Bem, Graduate Research Assistant
The Pennsylvania State University

T. Agami Reddy, co-PI
Steven Snyder, Research Assistant
Drexel University

Davor Novosel
National Center for Energy Management and Building Technologies

Prepared For:

U.S. Department of Energy
William Haslebacher
Project Officer / Manager

This report was prepared for the U.S. Department of Energy
Under Cooperative Agreement DE-FC26-03G013072

NOTICE

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.

THE PENNSYLVANIA STATE UNIVERSITY CONTACT

William P. Bahnfleth Ph.D., P.E.
Professor of Architectural Engineering Director, Indoor Environment Center
The Pennsylvania State University
207 Engineering Unit A
University Park PA 16802-1417
(814) 863-2076
wbahnfleth@psu.edu

NATIONAL CENTER FOR ENERGY MANAGEMENT AND BUILDING TECHNOLOGIES CONTACT

Davor Novosel
Chief Technology Officer
National Center for Energy Management and Building Technologies
601 North Fairfax Street, Suite 250
Alexandria VA 22314
703-299-5633
dnovosel@ncembt.org
www.ncembt.org

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
1. PROJECT OBJECTIVES	3
2. LITERATURE REVIEW	4
2.1 Objectives and Scope	4
2.2 Summary of Existing Knowledge.....	5
2.3 Conclusions and Research Needs	5
3. IDENTIFICATION AND EVALUATION OF EXISTING TOOLS.....	7
3.1 Objectives and Scope	7
3.2 Evaluation Methodology	7
3.2.1 Identify Tools.....	7
3.2.2 Evaluation Criteria.....	7
3.2.3 Risk Assessment Questionnaire	8
3.2.4 Identification of Representative Buildings.....	8
3.3 Tools Identified.....	8
3.4 Buildings Selected.....	11
3.5 Evaluation Results.....	12
3.6 Conclusions and Research Needs	15
4. CURRENT RISK ASSESSMENT AND SECURITY DESIGN PRACTICES AND APPLICATIONS	17
4.1 Objectives and Scope	17
4.2 Methodology	17
4.2.1 Survey Questions.....	17
4.2.2 Participants	18
4.3 Survey Responses.....	18
4.3.1 Risk Assessment and Security Design Practices	18
4.3.1 Examples of CB Security Upgrade Projects	22
4.4 Conclusions and Research Needs	25
5. SECURITY MEASURE ASSESSMENT AND DESIGN TRAINING AND CERTIFICATION PROGRAMS.....	27
5.1 Objectives and Scope	27
5.2 Professional Security Certifications.....	27
5.3 Professional Development Training Courses	29
5.4 Conclusions and Research Needs	31
6. PRIVATE SECTOR DEVELOPMENT AND IMPLEMENTATION OF ADVANCED BUILDING SECURITY SYSTEMS.....	32

6.1 Objectives and Scope	32
6.2 Methodology	32
6.3 Advanced Security System Technology and Control Systems	33
6.4 Conclusions and Research Needs	34
7. SUMMARY OF EXPERT PANEL MEETINGS	35
7.1 Expert Panel Meeting 1 Summary.....	35
7.1.1 Literature Review (Subtask 1)	35
7.1.2 Review of Existing Methods and Protocols (Subtask 2).....	36
7.1.3 Identifying Projects, Industry Practices, Technology Development (Subtasks 3-6).....	37
7.1.4 General Discussion	37
7.2 Expert Panel Meeting 2 Summary.....	38
8. FUTURE RESEARCH NEEDS	39
9. REFERENCES	41
APPENDIX A - BUILDING SECURITY ASSESSMENT AND DESIGN QUESTIONS	43

LIST OF TABLES

Table 1. Description of Buildings Selected 11

Table 2. Comparison of Various Tools 13

Table 3. Numerical Classification 14

EXECUTIVE SUMMARY

The objective of this task was to perform a state of the art review of methods for assessment and selection of engineering controls and security measures to increase the resiliency of buildings to airborne chemical and biological releases. The focus was on buildings for which modifications are not mandatory and are subject to significant economic constraints, i.e., typical commercial and institutional buildings. For most buildings of this type, little or no security enhancements have been implemented in either new or retrofit construction despite the heightened attention focused on the possibility of chemical and biological terrorism since 2001. Methods employed in this task included a literature review of current practices and available evaluation and recommendation tools, a discussion of weaknesses in currently available tools, testing of available software tools and performing paper risk assessment procedures, investigation of current practices of security professionals, facility owners and managers, and others. Based upon this review, a program of future research and development aimed at the deployment of effective assessment protocols is proposed.

The literature review identified a number of significant areas in which further work is needed, including the definition of a performance metric, application of formal risk assessment procedures to buildings, accessible data to support formal risk assessment methods and verification/validation of risk assessment protocols. A list of existing risk assessment protocols was also assembled during the literature review and five representative tools were selected for further, detailed analysis.

The selected tools were HVAC Building Vulnerability Assessment Tool (Rhode Island Department of Health), Building Assessment Checklist (Los Angeles County Department of Public Health), Building Vulnerability Assessment and Mitigation Program (Lawrence Berkeley National Laboratory), Chemical/Biological Building Protection Tool (United Technologies Research Center) and FEMA 452 (Federal Emergency Management Agency). They were compared on the basis of ten evaluation criteria and were also given trial applications to four existing buildings. Based on the evaluation, a list of desirable characteristics for chemical/biological risk assessment tools and deficiencies of existing tools was developed. Overall conclusions reached were that a) tools should provide building specific evaluations (such as simulation of the consequences of incidents); b) should quantify risk so that the impact of security enhancements can be compared more effectively; and c) should incorporate cost/economic features. Most existing tools are deficient in one or more of these respects to varying degrees.

Questionnaire responses and interviews with 34 professionals engaged in various aspects of risk assessment, building design, and facility management provide a snapshot of industry attitudes and practices. It was found that while many are familiar with the most prominent guidance documents, the application of detailed risk assessment procedures in commercial/institutional buildings is relatively infrequent. Some make use of in-house procedures while the methods of others are ad hoc. Designers typically work to minimum code requirements. The use of non-mandatory security enhancements that increase total project cost were found to be rare, and questionnaire respondents indicated that most did not make use of “multiple benefit” arguments (for example, the effect of improved filtration on air quality) to justify security measures.

A search for certifications and training programs related to building CB security identified three main certification programs: Certified Protection Professional (ASIS), Physical Security Professional (ASIS) and Building Security Certified Professional (Building Security Council). The eligibility requirements for these certifications tend to exclude professionals whose primary job function is design and are more relevant to providing the necessary credentials for individuals who might serve as specialty consultants during the design process. A number of short courses in recorded, on-line and live instructor format have been prepared by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) and others. These courses are well suited to informing design professionals of basic

principles of risk management as applied to protection of buildings from CB incidents. Little training in the modeling of CB incidents and methods to reduce their impact is provided.

Contacts with a number of companies engaged in the manufacture of advanced CB security technology yielded only general descriptions of available and developing capabilities due to confidentiality concerns. The main areas of technology under development are specialized air treatment equipment and active, sensor-based control systems. Given the highly cost-driven commercial/institutional security market, it would seem that such systems will receive limited application in lower risk facilities until their cost decreases substantially.

Two industry expert panel meetings provided valuable feedback on information assembled during this project and conclusions drawn from it. Much of this critique focused on clarification and qualification of assessments. Although this task has involved substantial effort and a wide ranging effort to gather a cross section of opinion, it is far from exhaustive and should be interpreted in the context of assessments found in other sources in the literature.

Based on the overall findings of the project, the following areas in which further research and development are needed were identified:

- Improved metrics. The variety of performance metrics for CB security proposed in the literature (such as relative risk based on time and space-averaged exposure, area or occupant weighted exposure criteria) have significant limitations. More effort needs to be devoted to developing a weighted single factor which weights occupant impacts, remediation costs, countermeasure costs, and others—in a formula simple enough to be useful and detailed enough to be accurate and which would serve as the objective function which needs to be minimized. This factor should characterize the CB threat and risk to building owners in terms of cost, and how potential consequences could be reduced by implementing certain security strategies.
- Better understanding of the decision-making process, i.e., identifying the various steps which decision-makers tend to (or must) follow in order to implement (or not implement) certain security enhancements in new and retrofit construction projects.
- Improvement in incident modeling capability of detailed tools paralleling those in allied applications (such as fire safety). There also exists the need to develop analysis methods that are relatively quick while allowing building-specific recommendations to be determined. The gap between detailed tools and those used (or can be used) by practitioners should be reduced.
- Application/adaptation of formal risk assessment procedures (both simplified and rigorous) to the domain of indoor building environment and development of supporting data necessary to exercise them. These procedures need to be coupled to the incidence modeling capability stated above.
- Multiple benefits research. Because the decision criteria for lower-risk commercial and institutional buildings identified in this study are primarily economic, it is essential that professionals engaged in risk assessment be able to quantify secondary benefits of security measures, including health and productivity benefits of better indoor air quality and energy savings from HVAC system changes, increased envelope air-tightness, reduced ventilation made possible by enhanced air treatment, and other possible sources. Methods to ascertain the uncertainty of these benefits also needs to be developed.
- Verification and validation of available modeling tools vis a vis accuracy and the reliability of claims of effectiveness for various protection strategies. In order to building confidence in the owner/designer communities, credible field studies to document the performance of analysis tools and protective technologies are needed.

In addition, there is a consensus that increased education and training efforts directed at increasing the knowledge of risk assessment and modeling techniques of practicing engineers is needed.

1. PROJECT OBJECTIVES

The ultimate objective of the work initiated through this project is to develop tools and methods that will increase the resiliency of buildings against intentional and accidental airborne contaminant releases by supporting selection and successful implementation of measures that are commensurate with the level of threat. This task is a scoping study intended to provide a baseline assessment and set the direction for potential future work. It focuses primarily on engineering controls to mitigate the consequences of both indoor and outdoor releases of gases, vapors, and aerosols rather than physical security (fences, card access and other measures intended to prevent releases) and managerial measures (evacuation plans and training). The task scope is limited to buildings that do not house high profile political figures or are symbolic in nature such as the World Trade Center or Sears Tower. This includes buildings such as office buildings, hospitals and schools for which security enhancement budgets may be very limited and for which the likelihood of an attack is very low. Such buildings may be “high regret” in the event that an incident actually occurs, but the calculus of very small and uncertain risk combined with the cost of security enhancements and other factors frequently results in a decision not to do anything.

2. LITERATURE REVIEW

2.1 OBJECTIVES AND SCOPE

The literature review performed in Subtask 1 of this project [Bahnfleth et al., 2008a] summarized existing knowledge on chemical and biological (CB) attacks to non-critical buildings and methods to enhance a building's resiliency in response to such an incident. Gaps in the available open literature were also discussed. Reviewed literature included 148 publically available documents, guidance, and tools targeting the following topics:

- risk assessment procedures
- airborne CB agents and building attack scenarios
- metrics used to quantify building security
- design methods, available technology and existing guidance to enhance resiliency of new buildings as well as existing buildings
- an overall classification of the various analysis methods
- published guidance, procedures, and protocols on risk reduction
- identifying the multiple related impacts of security design
- identifying the impact of operation and maintenance on building resiliency
- the economics of building resilience for "non-critical" facilities

The engineered system most vulnerable to an airborne CB attack in building is the heating, ventilation, and air conditioning (HVAC) system. Since most CB hazards, either intentional or unintentional, are aerosols, air movement plays a key role in occupant exposure. Therefore, the literature examined was specific to securing the building's HVAC system as well as other metrics that affect airborne contaminant distribution. Prior to the September 11th 2001 attacks, guidance documents on securing HVAC system components were directed toward government facilities or "critical" infrastructure. Specifically, CB security design was never considered a priority for other types of buildings such as commercial office buildings, schools, and hospitals.

In terms of building security design, a distinction must be made between government and non-government facilities. Some government buildings (e.g., the White House, Congress, the Pentagon) are of such great symbolic value that the cost of protection is a secondary consideration in decisions regarding protective technology. Other government facilities already have in place access controls and physical security that are not found in the vast majority of private buildings. For other types of facilities, the ability to quantify risk and cost-benefit is critical. The likelihood of a CB attack on any one of the roughly five million commercial buildings in the U.S. [EIA, 2003] is essentially zero. Thus, any expenditure on increased CB resiliency is at the expense of other business-enhancing investments and, therefore, should be made based on assessments performed on a rational basis. The review performed in Subtask 1 of this project [Bahnfleth et al., 2008a] surveys and describes available guidance and tools for making such assessments.

2.2 SUMMARY OF EXISTING KNOWLEDGE

The literature review for this task was published as a separate report, to which the interested reader is referred for details [Bahnfleth et al., 2008a]. A summary of topics reviewed and conclusions reached is provided here.

- *The CB threat and metrics to quantify it*- Many potential CB weapon agents have been identified and described in the literature. A number of reasonable approaches to the definition of performance measures have been proposed and used by various organizations and researchers, but all have limitations and no consensus standard has yet emerged.
- *Technologies and design practices for enhancing resiliency*-The literature deals at length with alternatives for making new and existing buildings more resilient, but recommendations are rarely supported by quantitative data. Few studies have analyzed the effectiveness of resiliency upgrades quantitatively through either field studies or simulations. A clear recommendation from current guidance is that layering of multiple modes of protection is advisable to protect against the many different threats that may arise.
- *Analysis methods, tools, and simulation programs*-Process flow charts, checklists, and software have been developed to assist in the process of evaluating building security. Most of these tools rely heavily on human judgment, and those that are more objective require data that may be difficult or impossible to obtain in an actual application.
- *Risk reduction procedures and guidance*- Protocols published to date are fairly consistent with one another since, in many cases, they have evolved from common sources. Many documents suggest a risk management procedure or protocol that consists of several steps such as threat analysis, vulnerability analysis, and consequence analysis. While there is not a consensus nomenclature or process, each protocol includes essentially the same steps.
- *Costs and benefits of enhancing resiliency*-While it is possible to describe the costs and benefits of enhanced resiliency, those costs have not been extensively or reliably quantified to date.

2.3 CONCLUSIONS AND RESEARCH NEEDS

Based upon the literature review [Bahnfleth et al., 2008a], the following research needs were identified:

- A variety of performance metrics for CB security has been proposed in the literature. These include relative risk based on time and space-averaged exposure, area or occupant weighted exposure criteria and, in a few cases, weighted combinations of exposure and cost. No consensus exists on metrics and significant limitations can be identified for every metric published to date. Without an appropriate measure of performance, decisions revert to professional judgment, rendering formalism and analytical detail of little value. Consequently, more effort needs to be devoted to expressing multiple factors—occupant impacts, remediation costs, countermeasure costs, and others—in metrics that are simple enough to be useful and detailed enough to be accurate.
- The well-accepted and mature formal risk analysis procedures applied to infrastructure systems have yet to be adopted for buildings. Though there are several papers that address aspects such as threat specification, relative risks, and impacts, they are largely heuristic and lack adequate analytical maturity in framework and industry acceptance. For example, the list of indoor CB attack scenarios may be incomplete (the same ones are repeated in the numerous documents) while the relative risks are inadequately quantified. Translating the threat into resulting impact to occupants also needs to be improved.

2. LITERATURE REVIEW

- There exists a large and growing gap between detailed tools and practical tools. This suggests the need for more training and education of practicing professionals on existing tools (and on other associated benefits of enhanced IAQ to occupants) so as to acquire real-world experience.
- Published evaluation and recommendation guidelines developed are heuristic and apply to generic rather than specific buildings. There is a pressing need to develop analysis methods which are relatively quick and allow building-specific evaluations and recommendations to be performed.
- To the extent that published procedures are quantitative and rigorous, their use is hindered by insufficient data—on resiliency upgrade costs, on the effectiveness of specific recommendations relative to a sufficiently broad range of threat scenarios, and on quantifiable secondary or “multiple” benefits that may result.
- Though many of the evaluation guidelines have appeared in the published literature for years, not a single paper/report was found which evaluates the guidelines against each other or in absolute terms. There is a need to evaluate the guidelines’ practical applicability and relevance, and also ways to either reduce/expand the list of questions depending on the building type, use and number of occupants. Hence, more case studies are needed.

3. IDENTIFICATION AND EVALUATION OF EXISTING TOOLS

3.1 OBJECTIVES AND SCOPE

The objective of this subtask was to evaluate tools and protocols available in the open literature whereby building owners can evaluate the current state of their buildings vis-a-vis airborne vulnerability, and determine the reduction in vulnerability given the implementation of specific countermeasures. The approach was first to identify all tools (software, reports,...) by performing an exhaustive literature review and then to select a smaller set of tools which are deemed to be developed or targeted towards practical and pragmatic use by building security professionals, consulting engineers, owners and maintenance personnel. Subsequently, these tools have been applied to a few carefully selected buildings in order to evaluate their responses both in terms of risk assessment and identifying resiliency measures. The ease in using the tools, the quantity and specificity of the suggestions they provide, and the extent to which the responses differ between tools were issues which were evaluated and reported in this document. This section summarizes the various issues investigated which are fully described in Bahnfleth et al. (2008b).

3.2 EVALUATION METHODOLOGY

3.2.1 Identify Tools

The methodology for evaluating guidance and risk assessment tools first involved identifying those tools that are sufficiently developed for practical application, as opposed to analysis procedures or methodologies or case study examples.

3.2.2 Evaluation Criteria

The following criteria were used to identify the selected tools:

- What information is needed and who from the facilities staff is best able to provide this information? Would the services of specialists be required to obtain it?
- How difficult is it to get the necessary information needed by the tools?
- How long does it take to insert the necessary information in each tool?
- How do they describe a building's vulnerability? What types of categories or distinct sub-systems are used? How logical are they?
- What type of guidance do they provide and what is its quality?
- How comprehensive and building-specific are the risk evaluations?
- How do the recommendations generated by the tools compare with one another?
- How sensitive are the recommendations to changes in the inputs?
- How user-friendly and intuitive are the tools in their inputs?
- How opaque/transparent are the tools in how they determine or assess risk and propose mitigation measures? How sound are the suggested enhancements to reduce vulnerability?

3. IDENTIFICATION AND EVALUATION OF EXISTING TOOLS

3.2.3 Risk Assessment Questionnaire

The first step in evaluating these tools was to become familiar with each of them in terms of how their checklist or questionnaires were grouped and which specific questions were asked. Since there would be a great deal of overlap in questions among these tools, the need to develop a single concise checklist was considered. The concerned personnel of the buildings being assessed would then only have to fill out one questionnaire rather than several questionnaires with repetitive questions.

3.2.4 Identification of Representative Buildings

A final and important step in the evaluation procedure was to identify a few buildings on which the questionnaires could be administered. Since the scope of this research was targeted towards secondary importance buildings (as against high profile or high risk buildings), a logical choice was to select buildings which fall under the office and hotel categories.

3.3 TOOLS IDENTIFIED

A comprehensive list of screening documents and software were identified and described in section 6 of the subtask 11.1 Literature Review report (Bahnfleth et al., 2008a). Subsequently five tools were identified which were deemed to be developed to the extent that they could be used by practicing engineers and field professionals intent on getting practical and pragmatic risk assessment and guidance on how to enhance their facilities for indoor airborne risks. These were:

- the HVAC Building Vulnerability Assessment Tool (BVAT) developed by the Rhode Island Department of Health [2004],
- the Building Assessment Checklist (BAC) developed by the Los Angeles County Department of Public Health [Fielding et al., 2006],
- the Building Vulnerability Assessment and Mitigation Program (BVAMP) developed by the Lawrence Berkeley National Laboratory [LBNL, 2005],
- the Chemical/Biological Building Protection Tool (CBT) developed by the United Technologies Research Center [UTRC, 2004], and
- the document/software program FEMA 452 developed by the Federal Emergency Management Agency [FEMA, 2005]

The BVAT and BAC tools are both simple checklist documents that assess the building through a questionnaire to be filled out by the building assessor and which provide recommendations in the form of generic responses. Each question in the checklist has a corresponding guidance statement/recommendation in the appendix of the document. The BVAT document deals specifically with HVAC systems and airborne contaminant attacks by asking questions about the type of air ventilation/conditioning, air handling units, air intakes, recirculation modes/return air, mechanical rooms, filtration specification, system operation and maintenance, and other considerations. The BAC document also deals specifically with airborne contaminant attacks; however, it asks questions on various building systems rather than just the HVAC system. The BAC checklist also includes questions on architectural features such as entry, lobby, mail, delivery, and storage spaces, air zone separation, windows, walls, and roofs. Questions involving the mechanical system include air intakes, mechanical rooms, and HVAC units. The document also includes questions regarding interior security (mail, shipping/receiving, and

3. IDENTIFICATION AND EVALUATION OF EXISTING TOOLS

storage), personal security, evacuation, sheltering-in-place, purging, protective masks, and emergency personnel. These tools allow for a written assessment of the building and can indicate where vulnerabilities exist in the building and what can be done to increase building resiliency to airborne attacks. These checklists are also “user friendly” due to the ease of use and the short amount of time needed to complete them. However, these checklists provide only general recommendations that are by no means building specific. Also, neither document provides a measure of the building risk or vulnerability or offers a cost analysis corresponding to the given recommendations.

The BVAMP tool consists of a “building walkthrough” document as well as a Java™ based software program that involves a simple questionnaire. The purpose of the building walkthrough document is to allow the assessor to gather the information needed to complete the software-based questionnaire. The walkthrough document asks questions regarding the building exterior, the roof, building entrances, the main lobby, the mail room, the garage and loading dock, stairwells, tunnels or skyways to other buildings, storage areas, hazardous materials storage, HVAC maintenance and utility rooms, rooms with HVAC controls, air-handling units, HVAC filters, dampers, exhausts, ducts, return air grilles, divisions between HVAC zones, emergency response plan, building plans/drawings/documents, and general security measures. Once these questions have been answered, the assessor can easily complete the software questionnaire that is broken into four categories of questions: (i) emergency response plan, (ii) HVAC systems, (iii) building access, and (iv) HVAC controls. The software program frames each question so that it can be answered with simply a “yes” or a “no.” Once all questions have been answered, the assessor can generate a Recommendations File. The recommendations given are dependent on the answers to the questionnaire and are thus slightly building specific. However, they are still general recommendations. The recommendations given by the program are listed in order of cost of implementation. Therefore, this program allows for a qualitative and preliminary economic analysis. BVAMP also organizes the guidance by giving recommendations first for all facilities, and then for higher risk facilities. However, no measure of risk is given by the program. This program is easy to use and little time is needed to complete the questionnaire. The program, however, does not provide a measure of how vulnerable the building is or how the building resiliency will improve by implementing the given recommendations.

The CBT tool is a software program that contains broad categories (General Information, Vulnerability Assessment, Potential Solutions, Air Filtration and Final Summary). The vulnerability assessment questionnaire is further separated into the following eight categories: physical security, building configuration, monitoring, HVAC, training/communications, CB specific, air intake design, and air intake operation. The program has drop-down menus providing the various choices for answers to each question. These questions are listed in a hierarchy of security level. Next to each question is a “help” button that explains in more detail the question and the meaning of each answer choice. Once all questions have been answered, the program generates a protection level matrix dependant on the answers chosen. This matrix gives protection levels (represented by a number from 0-100) for two classifications (mitigation and prevention) and for four attack scenarios (internal, external proximate, external remote, and external warning). Color-coding is used in the matrix to give an idea of the level of vulnerability in each classification for each attack scenario. Next, the program provides a list of possible solutions to help improve the building’s protection levels. These solutions, however, are simply the answer choices (of higher security level) that weren’t chosen previously. The program shows “before” and “after” matrices so that the assessor can visualize how the improvements affect the protection level matrix. Finally, the program includes a separate feature on air filtration/pressurization information. This allows for an economic analysis of implementing various filtration/pressurization techniques.

The CBT tool is a “user friendly” interactive program that gives a measure of the building’s risk and vulnerability, makes recommendations for improvement, shows the effects of those improvements, and allows for a preliminary economic analysis. The potential solutions or improvements are categorized using two different schemes. The first classification scheme gives a measure of the first and operating costs that can be expected for each improvement. The second classification scheme gives a measure of

3. IDENTIFICATION AND EVALUATION OF EXISTING TOOLS

the maturity of the improvement (availability of the technology, how well it has been developed, and how much it has been proven to help in CB attacks). In terms of protection levels, solution recommendations, relative costs between different options, and relative feasibility of implementing them, this program does not provide specific and detailed information. Also, it is unclear as to how the protection levels are calculated from the answers chosen in the questionnaire. Another ambiguity lies in the impact of questions that may not apply to a particular building being assessed. Since each question must be answered to calculate the various protection levels, it is unclear which answer to select if the question does not apply.

The FEMA tool consists of an extensive document, FEMA 452, and a software program in the form of a Microsoft Access™ file. This software tool has three functions:

- it allows an information database to be created that stores building information, assessment team information, points of contact, references, site plans, GIS portfolios, photographs, building assessment information, etc.;
- it allows risk analysis to be done by explicitly performing the three previous steps of threat identification, asset value assessment and vulnerability assessment to be made with the help of worksheets that include a threat rating matrix and a critical infrastructure matrix; and
- it provides assessment checklists.

An advantage of this tool is that it can be used by several assessors at the same time. Various assessors with different specializations can answer the questions provided in the FEMA 452 appendix that apply to their specialization. The information in these assessor databases can then be linked to a Master database that collects all the information. In terms of a vulnerability analysis, this program combines two features, risk matrices and an assessment checklist. The two matrices generated in this program are a Critical Function matrix and a Critical Infrastructure matrix. The matrices list the various critical functions and critical infrastructures (which can be user defined) versus different attack scenarios. For each combination of function/infrastructure and attack scenario, the user specifies a threat rating, an asset value, and a vulnerability rating (all 1-10) based on the scales described in the FEMA 452 document. The program then calculates a risk rating and color codes it by the level of risk. This provides a measure of the building's vulnerability and risk to various attack scenarios. A difficulty with application of the FEMA matrix approach is that it is difficult to rationally assign realistic weights for the various categories. CBT has fewer such categories, but does this automatically.

The final feature of the program is the assessment checklists. FEMA 452 provides the questions of this checklist which are organized into the following categories: architectural, structural, building envelope, utility systems, mechanical systems (HVAC and CBR), plumbing and gas systems, electrical systems, fire alarm systems, communications and IT systems, equipment operations and maintenance, security systems, and security master plan. It is recommended that the assessor answering the questions in each category be professionals educated in that building system. Along with each question, standard guidance is provided by FEMA. The program provides space for the assessor to answer the question, make observations, write their own recommendations, and check whether or not there is a vulnerability. The final part of this program is the facility vulnerability process. Once all the assessments are collected in the Master database, a spreadsheet is formed based on all the identified vulnerabilities. From here, the administrator can search and prioritize (1-5) all the vulnerabilities. Space is also provided for cost estimates for each remediation. This program can be used to store, search, and analyze collected data. Also, results can be archived from a number of assessments, reports can be printed, and vulnerabilities common to all the buildings in the database can be searched.

The two threat matrices and the various assessment checklists lead to a complete vulnerability analysis of the building. However, *determination of the threat ratings, asset values, and vulnerability ratings from FEMA 452 is quite subjective. Also, assessors that are experts/educated in the areas they are assessing are needed.* This program also only provides general guidance that is associated with each question

regardless of the answer. Finally, this program is fairly complex to use and requires a significant amount of time to collect all the data that can be input into the database.

3.4 BUILDINGS SELECTED

Two Drexel University buildings and two buildings at the Pennsylvania State University’s campus were selected, whose characteristics are representative of a large portion of building stock that would qualify as secondary importance level (see Table 1). The first building selected was a typical residence hall on the Drexel campus. Residence halls typically have fairly simple HVAC systems and repeated floor plans which make them easy to analyze and model if necessary. They also have a high occupancy of students making them a significant target for a potential attack. The next two buildings were typical office/classroom buildings, while the fourth was a large auditorium. These four buildings were chosen because they are all typical buildings that make good case studies since they would apply to a large portion of existing buildings.

The Director of Plant Maintenance in the Facilities Management Department at Drexel University and the Senior Mechanical Engineer in the Office of the Physical Plant at Penn State University were interviewed to obtain the answers to the questions from each assessment tool. As mentioned earlier, in order to make this process more efficient, a compact vulnerability questionnaire was assembled before performing the interview. This questionnaire contained all the unique questions necessary to apply each tool in terms of an airborne contaminant attacks. The Director of Plant Maintenance and the Senior Mechanical Engineer answered all the questions in the compact questionnaire for the four buildings being assessed. With these answers, each tool could be applied to all the buildings.

Table 1. Description of Buildings Selected

Type of building	Dormitory	Office/classroom	Office/classroom	Auditorium
Name	DU#1	DU#2	PSU#1	PSU#2
Location	Drexel campus	Drexel campus	PSU campus	PSU campus
Gross floor area	108,535 sq.ft.	29,444 sq.ft	31,1000 sq.ft	45,000 sq.ft
Number of floors	7	4	3 floors + mechanical room in basement	-
Total Occupancy	300	30-40 office personnel, 300-50 students in class	Normal occupancy of 140 + up to 170 floating students and professionals	2,595 seats+ ticket office + ushers+ concession workers
HVAC system characteristics	Water source heat pump in each suite, centralized ventilation, AHU with heat recovery located on roof	Rooftop-packaged units with VAV and gas heat	VAV chilled water AHU with hot water heating coils	Multiple VAV and CAV chilled water AHUs with hot water heating coils
Other information	4-6 person per suite	Mixed office-classroom	-	-

3.5 EVALUATION RESULTS

A summary comparison of the various tools in terms of the various characteristics described earlier to evaluate the tools is given in Table 2. Specified in the table is the time required to use each tool, the ease of use, the type of user input, the type of guidance, the basis of evaluation of building vulnerability, the basis of guidance, any ambiguities, and any unique features. While BVAT, BAC, and BVAMP require little time to fill the questionnaires and are based on yes/no type of answers, the FEMA tool is much more demanding of time and user skill. It requires descriptive inputs while CBT has drop-down menus of preset answers that make it very user-friendly and convenient to use. While the guidance is generic for BVAT, BAC, and FEMA, and does not depend on the answers to the questions, guidance given by BVAMP and CBT is specific to the answers provided by the user. BVAT, BAC, and BVAMP do not provide a metric for building vulnerability, however, the user does acquire a sense of it through the process of thinking through the questions. FEMA and CBT do provide a quantitative index of risk; however, FEMA requires that the user provide the weights for the various threats. Except for CBT, all the remaining four tools provide generic guidance. CBT provides a color coded metric of risk broken up into separate sub-categories and also performs a cost analysis on the filtration/pressurization process.

Table 3 provides an overall classification of each tool in terms of the guidance/recommendations it provides and in terms of the vulnerability (threat) evaluation it conducts. A value of “0” means that the tool omits this feature. A value of “1” means that the tool provides general or low-level guidance/threat evaluation. A value of “2” means that the tool provides guidance/threat evaluation that is still heuristic but somewhat building specific. As can be seen from this table, BVAT, BAC, and BVAMP do not provide any means of measuring building vulnerability or risk. By using these tools and answering the questions given, the building assessor may get an idea of where vulnerabilities are but the tool itself does not provide a measure. FEMA and CBT each provide a means of measuring building vulnerability, but both methods are heuristic. FEMA’s vulnerability evaluation is highly user specified whereas the CBT vulnerability evaluation is provided by answering all the questions it provides.

Each tool provides some type of guidance. BVAT, BAC, and FEMA provide general/low-level general guidance that is associated with each question. BVAMP and CBT also provide general, heuristic guidance; however, they have features that make the guidance somewhat building specific. BVAMP eliminates some of the guidance that is not needed for a particular building depending on how the questions in the program are answered. CBT also provides guidance based on how the questions in the program are answered making it somewhat building specific. One note of caution, however—the guidance CBT provides is simply the answers that weren’t chosen previously that would result in a better building vulnerability rating. The program does not provide detailed guidance in the form of text as do the other tools.

Table 2. Comparison of Various Tools

Tool	Time Required/Ease of Use	Type of User Input	Type of Guidance	Basis of Evaluation of Building Vulnerability	Basis of Guidance	Ambiguities	Unique Features
BVAT - Rhode Island	Little time required to complete checklist. Simple to use, self-explanatory. May need qualified assessors to answer some questions.	Mostly Yes/No Inputs with some short answer questions (# of AHU's, locations, areas serviced, etc.)	General guidance to each question, independent of answer.	No visual/numerical output but user acquires a sense of building vulnerability by answering questions and reading recommendations.	General, heuristic guidance in paragraph form.		
BAC - Los Angeles	Little time required to complete checklist. Simple to use, self-explanatory. May need qualified assessors to answer some questions.	OK/Not OK Inputs	General guidance to each question, independent of answer.	No visual/numerical output but user acquires a sense of building vulnerability by answering questions and reading recommendations.	General, heuristic guidance in paragraph form.		
BVAMP - LBNL	Little time required to answer questions on the program. May need qualified assessors to answer some questions.	Yes/No Inputs	General guidance to each question. Guidance given depends on answers or inputs user gives to the program.	No visual/numerical output but user acquires a sense of building vulnerability by answering questions and reading recommendations.	General, heuristic guidance in paragraph form given in order of cost to implement. Also divided into guidance for all buildings and guidance for higher risk facilities.		Questions asked are dependant on answer to previous questions. Program eliminates questions that do not apply after a certain answer has been provided.
FEMA	Complex database capable of storing a large amount of information. Significant time required to answer all questions and fill out all matrices. Time required to read FEMA document. Learning curve associated with use of program. May need qualified assessors to answer some questions.	Descriptive input in the user's own words.	General guidance to each question, independent of answer.	User selects weights from given tables which provide a quantitative index of risk that is color coded.	General, heuristic guidance in paragraph form (user defines cost information).	Selecting threat rating, asset value, and vulnerability rating.	Database format (image and information storage), ability to link databases, risk matrices, ability to organize and prioritize noted vulnerabilities.
CBT - UTRC	User friendly program, relatively self explanatory. Little time required to answer questions. Some time required to evaluate recommendations and explore other features. May need qualified assessors to answer some questions.	Drop down menu of preset answers (in hierarchy of security level) to each question.	Guidance provided are the answers to the questions that weren't selected during the assessment.	Weighted matrix calculated depending on answers showing vulnerability that is color coded.	Answers not selected, characterized in terms of cost and maturity.	What to select when question does not apply to building being assessed.	Automatically produced color coded matrix, air filtration/pressurization cost analysis.

3. IDENTIFICATION AND EVALUATION OF EXISTING TOOLS

Table 3. Numerical Classification

	BVAT	BAC	BVAMP	FEMA	CBT
Threat Evaluation	0	0	0	2	2
Guidance	1	1	2	1	2

0 = Omitted

1 = General or low-level guidance/evaluation

2 = Heuristic guidance/evaluation, specific to the building (eliminates some possibilities)

3.6 CONCLUSIONS AND RESEARCH NEEDS

The investigations performed in this sub-task identified features and capabilities of an ideal assessment tool for indoor airborne risk. These are listed below:

1. Tools should be easy to use and intuitive. Developing interactive software programs is highly recommended. Ways of combining the information storage and database capabilities of FEMA with the interactive features of CBT should be explored.
2. It is a good approach to use questionnaires that allow answers specific to the building to be captured in the interactive tools. However, these questionnaires should be designed to be more sophisticated than lists of questions with yes/no answers (like BVAMP). A drop-down menu of possibilities is one appealing approach. Along with drop-down menus, there should be space for the user to enter other observations or elaborate on the answer. FEMA's database capabilities allows for this.
3. All tools should explicitly compute building risk in some way by including the three different aspects of threat identification, probability of occurrence and consequence of event. CBT does not do this, while FEMA does. One possibility is to have a common method (mathematical formula) for calculating risk, which should be determined so that the numerical results from one tool can be compared to the results from another. Currently, FEMA and CBT cannot be compared in this way.
4. Building risk assessments should take into account more than physical building features. Political, religious, economic, historical, and occupancy issues, for example, should also be considered when determining risk. How one does this without assigning arbitrary or subjective weighting values to each issue? Such questions need to be explored as should additional solutions to this problem.
5. Existing building risk assessments are general in nature, and largely heuristic. Although this approach is the logical one at the onset, it is recommended that assessments become more quantitative and building specific and use some broad characteristics that can be measured or estimated (like air-changes per hour, time constant,...). Simple two-zone models, which allow analytical solutions and can thus provide additional insights should be investigated.
6. Integrate these tools with simulation programs (CONTAM) and modeling programs (such as Autodesk's Revit) so that guidance can truly be building specific and not just general.
7. The tool should only provide guidance specific to the building based on the answers to the questionnaire portion of the tool (this is done by CBT but not by the others). Even if the guidance is generic in nature, it is better to list only items applicable to the specific building rather than all types of guidance applicable.
8. The tool should integrate the strong features of these tools into one tool. For example, the database features of FEMA, the easy to use and automatic vulnerability calculation of CBT, the guidance sorting of BVAMP, etc.
9. All tools should have some cost/economic analysis features. These features should be integrated with the guidance provided by the tool. The user should be able to get a sense of how implementing the suggested guidance/potential solutions will affect the building from a cost perspective.
10. The tool should integrate more realistic first, operating, and maintenance costs figures for potential solutions.
11. The tool should compute cost of consequences (loss of lives, clean-up, lost work time, etc.) to produce an all cost metric (perhaps life cycle cost) to aid in decision making.

3. IDENTIFICATION AND EVALUATION OF EXISTING TOOLS

12. The tool should provide more detailed guidance, including common methods and procedures for implementing the various recommendations. It should provide more detailed procedures on what to do for different attack scenarios. Even though attacks are building specific, tools can provide general guidelines and a list of “do’s” and “don’ts.” Attack scenarios include chemical agent vs. biological agent and indoor release vs. outdoor release for example.
13. Each tool should have a feature similar to CBT where one can visualize how implementing various recommendations improve the buildings risk/vulnerability ratings. The guidance features and risk evaluation features of all tools should be integrated rather than separate.

4. CURRENT RISK ASSESSMENT AND SECURITY DESIGN PRACTICES AND APPLICATIONS

4.1 OBJECTIVES AND SCOPE

The objective of subtasks 3 and 4 was to identify and summarize current practices followed by professionals engaged in risk assessment and security design for buildings. An additional objective was to identify representative buildings that have undergone vulnerability evaluations and enhancements for which information is available. The Subtask 1 literature review [Bahnfleth et al., 2008a] identified many reference documents and tools for assessing a building's vulnerability from a CB attack. These guidance documents and tools also describe methods and technologies that may make buildings more resilient to a CB attack. This section examines the extent of use of these guidance documents and tools during the evaluation and design phases of typical commercial and institutional buildings. It also describes other security design practices being used aside from the published documents.

4.2 METHODOLOGY

A questionnaire (Appendix A) was developed and sent to engineering design professionals and to researchers who have helped in the development of risk assessment guidance and protocols. Architects, HVAC engineers, and air cleaning product suppliers in the Philadelphia, New York, and Washington D.C. areas were also contacted. In addition, questionnaires were sent to representatives of experienced security design engineering and consulting firms and security management consulting companies. The methodology used is anecdotal rather than statistically rigorous, but it provides a useful sample of practices and attitudes from a number of groups involved in security evaluation and security measure implementation.

4.2.1 Survey Questions

Participants were asked questions about buildings on which they have worked, of which they are aware, or which they own that have undergone any type of CB security analysis or design. The questions are broken down into two categories: *design phase* and *design decision*. The design phase set of questions are intended to determine what vulnerability assessment methods, if any, were applied. If the assessment followed one of the published documents, such as FEMA's Building Vulnerability Assessment Checklist or LBNL's Building Vulnerability Assessment and Mitigation Program, the questionnaire asks for input on the evaluation tool and to identify any gaps in the procedure that were found as it applies to the building. Other questions in the design phase section focus on how security enhancements are chosen and evaluated. Additional questions seek to identify any modeling or testing methods used on the building to understand the effectiveness of the enhancement against an airborne release.

The design decision set of questions is directed at determining the conclusions and outcomes that resulted from the security design phase and vulnerability assessments. The questionnaire seeks information about the effectiveness of the designs implemented and what types of attacks (inside release, outdoor air intake release, etc.) were considered, including costs associated with security measures for the representative building. Cost-related questions addressed the type of cost benefit analyses performed and the weight given in the decision process.

4. CURRENT RISK ASSESSMENT AND SECURITY DESIGN PRACTICES AND APPLICATIONS

4.2.2 Participants

The time and efforts of the 34 professionals, those listed below and those wishing to remain anonymous, in filling out our questionnaire as well as providing valuable information on this research topic are greatly appreciated.

Pran Chandra
Tri State HVAC Equipment

Scott Detienne
URS Corporation

Othon Estrada
US Department of State

Jeff Gilbeaux
Gilbeaux Associates

John Gregowitz
SRS-Enterprises

Mike Gressel
Center for Disease Control and Prevention

Sue Haupt
Penn State University Applied Research Lab

Eve Hinman
Hinman Consulting Engineers, Inc.

Jennifer Holcomb
KPFH Consulting Engineers

Mike Kaminskas
Raytheon UTD

John Lowe
WDG Architecture

Ken Magsam
Burns Engineering, Inc

Rudy Matalucci
Rudolph Matalucci Consultants, Inc.

James Miller
Syska Hennessy Group

Michael Oliver
Arora Engineers

George Rossi
General Aire Systems

Jon Schmidt
Burns & McDonnell

David Stephenson
Siemens

David Thompson
RTKL Associates

Fred Zagurski
Fred Zagurski Consultants

Joe Zagorski
Burns Engineering, Inc

4.3 SURVEY RESPONSES

4.3.1 Risk Assessment and Security Design Practices

This section presents responses to the questionnaire. The information presented in this section reflects the viewpoints of the responding professionals and not necessarily those of the authors and sponsor of this report. The purpose of this subtask was to obtain information to characterize the current state of CB security design and assessment in the building industry, and the responses indicate how well industry is informed on the subject. The information gathered during these subtasks is organized into three parts. The first subsection summarizes general information on risk assessment and security design practices from the responses to the questionnaires. The second subsection summarizes responses from companies that use (or would use) a published risk assessment procedure or guidance document during a security design. Several responses described company specific security design practices and risk assessment procedures. These are summarized in the third subsection.

a. General Information

Respondents indicated that unless building codes require specific designs and technologies that reduce the impact of CB releases, building design does not consider CB risk assessments or advanced security design practices. The responses indicated that security design practices are typically included in codes after an incident occurs. The 2001 anthrax mailings did not pose a sufficiently large threat to typical commercial and institutional buildings to mandate the implementation of CB security technologies. Only recommendations have been published.

In assessing threats to buildings, owners and decisions makers have few good options for acquiring information relevant to the risk to their facility. One source noted by respondents is that the Department of Homeland Security (DHS) Daily Open Source Infrastructure Report (DHS, 2008), which includes information on what is happening on the state, national, and international level. The report along with information passed on to the state police departments provides information on potential threats. Information on the risk of a CB threat would be qualitative and include either a prior incident, or reported suspicious activity involving CB agents.

Generally, the responses to the questionnaire imply that designs simply follow “good practice”, as long as there are no adverse effects to the project budget. The initial and operating costs of implementing a security measure seem to be principle factors that weighs into the decision. Secondary benefits of security enhancements, such as improved air quality, are mentioned to building owners. However, without quantifiable evidence that proves the design’s benefits outweigh their costs in a timely fashion, expensive security designs are not being installed into “non-critical” buildings.

b. Security Design Practices Based on Published Guidance

The vast majority of responses to the questionnaire indicate that few clients associated with lower profile commercial and institutional buildings have any interest in specifically designing their building for protection against a chemical or biological attack. According to the responses, such buildings rarely undergo a security assessment. However, implementation of certain CB security design measures is considered good practice as long as it does not result in major cost increases. Roughly half of the contacted HVAC designers were well educated in what designs and technologies are available for CB security. These engineers indicated that if a CB security design was requested, they are knowledgeable of the available reference documents to aid in the process.

Many design professionals indicated that they reference the guidance provided by FEMA 427 document [FEMA, 2003] and the NIOSH [2002] document Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks. However, a clear indication of the usefulness of these documents or security improvements implemented as a result of their use could be drawn from questionnaire responses. Common CB security designs that are implemented or recommended for owner/occupants to consider include:

- Locating the air intakes serving occupied areas as high on the building as possible and control access to them
- Zoning of public areas such as the lobby or mail room with separate air handling units that create a negative pressure relative to surrounding spaces along with constructing physical barriers
- Providing a single air handling unit fan shut-off switch which is easy for facility personnel to access but which is hidden or inaccessible to the public
- Include the ability to close outside air intakes completely and quickly
- On buildings that have the capability to go into 100% outdoor air, providing a purging mode, similar to smoke removal, which is particularly useful for the lobby

4. CURRENT RISK ASSESSMENT AND SECURITY DESIGN PRACTICES AND APPLICATIONS

- Providing a space for a detection and/or filtration system in the future
- Commissioning of the building to make sure that leakage through the walls is minimized at window and door openings

It was noted that all buildings in the Washington D.C. area that house a government agency must meet the minimum requirements found in the U.S. General Services Administration (GSA) Facilities Standards [GSA, 2005]. However, according to one respondent, no more than what is explicitly required is typically implemented due to the high costs. The minimum GSA particulate filtration requirement is what is typically installed. Pressure drops of higher efficiency particulate filters were thought to be too high for building owners to consider as a design option. Security features listed by the GSA mainly focus on physical security, such as restricting access and locking doors. For HVAC systems, the GSA only requires that outdoor air intakes be raised to the fourth floor or higher on high rise buildings or located on the roof for low rise buildings.

None of the guidance that responding design professionals recommend or implement includes HEPA and gas phase filters. One respondent commented that the use of such technology is not recommended to clients because maintenance (filter replacement) and energy (fan pressure drop) costs are high. Further, the opinion of the professionals was that these filters, particularly gas-phase adsorbent filters, deteriorate very rapidly in an urban atmosphere, making them impractical for use in low-risk buildings. The urban pollution is absorbed by the filter material exactly as would a chemical agent, hence reducing its active life span.

Ultraviolet Germicidal Irradiation (UVGI) filtration technology had mixed reviews. From one respondent identified UVGI as an available technology, but not one that is highly recommended. The design professional indicated that UVGI filters are very effective against airborne bacteriological agents, but are less effective against airborne viruses and not very effective against airborne spores without very high UV intensities or extended residency time exposed to the lamps. Further, it was mentioned that spores and bacteria can be filtered without excessive pressure drop. Using a MERV 16 filter or a HEPA filter that can remove up to 99.7% of particles approximately 1.5 microns in diameter was at odds with the recommendation of using UVGI in low-risk buildings.

However, another design professional stated that UVGI provided the best benefit in combination with the least cost filtration technology. Besides the security upgrade advantage, the low pressure drop attribute was highlighted along with secondary health and disease transmission benefits.

Finally, a few design professionals felt that a detection system is the best overall counter-measure. However, no information on projects that have implemented such technologies was provided and one respondent noted that sensors are still too expensive for non-government installations. It was noted that chemical sensor technology is more advanced than biological sensor technology and that fast acting chemical detection systems are needed because of the characteristics of response to chemical agents.

c. Company Specific Security Design Practices

This section summarizes each of the company specific responses that add detail to the overall responses summarized above.

- One design firm representative indicated that the company uses their own custom checklists for performing vulnerability assessments. The checklist is used by a multidisciplinary team of experts in various aspects of security, led by an architect to ensure a holistic, balanced approach. Prior to the vulnerability assessment, a threat assessment is conducted to serve as the basis for prioritizing assets and hazards for both the vulnerability assessment and development of the security master plan. This methodology is similar to the risk assessment procedure outlined in FEMA 427 [2003]. While the assessment team is familiar with the current published guidance documents, they rely on their own

4. CURRENT RISK ASSESSMENT AND SECURITY DESIGN PRACTICES AND APPLICATIONS

practice and experience in selecting the best protective requirements for high value assets against the owner specified threat. The firm's own methodologies and formats have been developed over a 15 year period. While every other response indicated that no modeling or testing methods were used to analyze the effectiveness of the security enhancements against a CB attack, this particular firm has performed airflow modeling studies during the design phase.

- Another design firm performs vulnerability assessments without a formal checklist. The primarily MEP design firm recently brought on staff that has experience and knowledge to conduct a broad overview of building site security assessments. The security staff along with the MEP design engineers creates a knowledgeable site survey team for the company. The team conducts a walk-through of the site and building with the operating staff to observe the built conditions and is briefed on both normal operating procedures and emergency plans. Although no formal guidance document or tool is used in assessment phase of security design, the design firm uses a wide range of publications to aid in selecting resiliency enhancements, all of which were cited in subtask 1 of this project [Bahnfleth, et al., 2008a].
- The design firm has found that private building owners do not consider their facilities to be at high risk of a CB attack. Therefore design phase security enhancement modeling that carries a significant cost, such as CFD, is not seriously considered. The company does not quantify multiple benefits from using security designs since documentation on worker productivity improvement and reduced sick leave as the result of improved indoor air quality is cursorily maintained (if at all). Detailed cost-benefit analyses are not used in the decision process. The decision to implement a design comes from a joint discussion involving the technical assessment team, maintenance engineers, and the building owner's representative.
- One firm's respondent stated that, for non-government facilities, vulnerability assessments are performed by first looking at the use and activities of the target building to determine what potential assets may exist and need to be accounted for in the vulnerability assessment. Using this information and drawing from a large number of resources such as FEMA guidance, questionnaires are developed for the tenant or client to. One questionnaire is for the physical assessment (completed prior to the site visit), and one is for questioning the client while on site. The reasoning behind this company's assessment methodology is that an accurate evaluation for each unique facility is difficult with a "universal" vulnerability assessment. Assessors use their best judgment to determine if additional investigation is appropriate. After the assessments are completed, the decision to implement a recommended design must be made based on the level of risk the client is willing to accept. The cost-benefit analysis is an important tool for the client to determine what upgrades or changes will be implemented. When recommending security solutions, multiple benefits as well as the creation of new risks as a result of modifications are discussed with the client.
- A security consulting firm that specializes in protecting infrastructure and architecture performs full security risk assessments and management procedures for buildings that include threat, consequence, and vulnerability analyses as a complete package. The specific procedure that the company applies follows has been published in the handbook "Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures," [Bringer et al., 2007], which was reviewed in subtask 1 of this project [Bahnfleth et al., 2008a]. Through experience, the company has found that using a checklist is helpful for completing a site survey and taking inventory of a facility. However, they feel that checklists do not provide sufficient information for an assessment of actual security shortcomings, nor provide a basis for justifying required cost-effective mitigation measures.
- The company selects security enhancements based on the results of the risk assessment. They interact with the owner and management throughout the process to ensure that the stakeholders are making the decisions on acceptable risks, upgrades required, and the basis for the design criteria that are imposed on the facility. Implemented changes to the building are tested by applying gas dispersion

4. CURRENT RISK ASSESSMENT AND SECURITY DESIGN PRACTICES AND APPLICATIONS

models. The company has applied this analysis and selection process to identify appropriate locations for airborne contaminant sensors. However, the company feels that the ultimate approach in selecting an appropriate design is still the standard security risk assessment procedure, not a modeling-based methodology.

- The company feels that cost-benefit analyses resulting from a full risk assessment process are the key to a valid decision by the stakeholder. This process ensures that risk reduction is required, and certain security upgrades and mitigation measures offer the best means for risk reduction. The specifications for the security upgrades and consequence mitigation options become the responsibility of the designer once the stakeholder agrees on the required protection and risk acceptability levels. In all situations, the company's methodology insists that the stakeholder make all decisions based on the data and analysis results provided by the analyst and the suggestions for alternatives provided by the team of technical experts that are involved in the security, operations, engineering and management processes. The company also strongly believes that there is a need for a complementary (multiple benefit) design evaluation. For CB security designs, increased health benefits from applying air quality improving technologies are examined and provided to the stakeholder to justify implementation.
- In addition to professionals working in design firms, several equipment suppliers were also asked to fill out the questionnaire. For CB building security, the companies contacted supply air treatment products. One of these has been doing risk analysis for several years, and consults FEMA and homeland security documents for guidance. The company has a comprehensive facility management team and they perform risk assessments even without the owner's request. They constantly watch for emerging technology and changing regulations while advising their clients about threats and risks as well as changing legislation. They also try to get external funding to encourage building owners to implement security measures. However, the company representative commented that only a handful of customers have implemented recommended measures (mostly immediately after 9/11) for reasons of cost.

Other equipment supplier respondents indicated that usually consulting engineers and architects perform the risk and vulnerability assessments. Equipment suppliers become involved during the design phase of a project. These company representatives were under the impression that during the risk analysis phase the consulting engineer identifies the type of contaminant, concentration levels, source locations, and identifies ways of reducing source strength. The engineers then hold discussions with the building owners and managers resulting in identifying the specific measures to be implemented. Only then are the contractors contacted who then select, size, and supply equipment to meet the pre-determined requirements.

4.3.1 Examples of CB Security Upgrade Projects

Few examples of CB security upgrade projects were identified during this study. Furthermore, and not surprisingly, it was found that firms that have performed security evaluations and designs for buildings encourage the owners and operators not to share the findings of the evaluations with anyone other than those who need to see the reports, such as contractors. Leading HVAC control companies were also interviewed to identify any projects in which their control systems were integrated with CB security designs. Responses ranged from "no project has requested such technologies," to "any information that we may have in these areas of inquiry would be confidential".

- A generic example of the many facilities (most of which were government buildings) that have been assessed and upgraded for CB security by one design firm was returned by one respondent. The retrofit project was for a 200,000 square foot, 4 story office and data center. The HVAC system consisted of central chillers, a boiler plant, and zoned roof-top air handling units with no pre-existing CB security systems implemented in the original design.

4. CURRENT RISK ASSESSMENT AND SECURITY DESIGN PRACTICES AND APPLICATIONS

- In the design phase of this project, a vulnerability assessment was performed, but the details of what was assessed were owner specific, not based on a published checklist. To evaluate the effectiveness of the security design options, the design firm used airflow modeling to simulate the design's performance during a CB incident. Specific enhancements analyzed are confidential, but all involved changes to the HVAC control sequences. Upgrades to air side systems were implemented to assure uninterrupted operations and survivability. Other associated systems were upgraded including envelope integrity and controls sequences based on the type of release and its location.
- The design firm reported that the conclusions from the vulnerability assessment combined with other threat mitigation analyses produced a balanced and affordable response to airborne threats within the operational framework of the client. A layered approach to threats was employed i.e., some risk was accepted and not all areas of the facility were protected to the same level. The actual designs or technologies implemented in the building were withheld, but were stated to enhance the building's resiliency from an inside release, outdoor release, and outdoor air intake release. Finally, cost information on this retrofit project was withheld and no cost-benefit analysis was performed.
- A security consulting firm listed examples of projects that have undergone a security assessment. Identities of the buildings were not provided due to confidentiality reasons. The buildings included:
 - ▶ Municipal buildings (< 10,000 occupants)
 - ▶ Federal buildings (> 10,000 occupants)
 - ▶ High rise administrative offices (over 50 stories, 1,000 to > 10,000 occupants)
 - ▶ Laboratory facilities and storage complexes (> 500 occupants)
 - ▶ Data centers with varieties of information technology systems (> 500 occupants)
- Full security risk assessments were performed on each of the facilities, after which all vulnerabilities and security system weaknesses were identified and upgrades were proposed to the stakeholders, who then made the decisions regarding which to implement. Security enhancements implemented varied among the projects and included HEPA filtration, kill switches (to completely shut down HVAC systems) that are activated by a detection system consisting of chemical sensors and verification methods, and interior space pressurization to combat against toxic agents entering the buildings. The techniques were applied with careful investigations and analysis procedures so that they are effective and reliable to perform the intended purpose. In most cases, the company found that the cost-effectiveness of a recommended upgrade is the primary factor in the decision. Therefore, they stress the importance in detailing how the security risk is reduced and to clarify the confidence levels determined if the mitigation suggested are in fact implemented. During most of the decision processes, there were discussions about the normal uncertainty in the actual performance of the mitigation measures proposed, and the likelihood that the attack would be executed in accordance with the predicted scenario. There were also the usual considerations that the decision process is based partially on scientific engineering principles, and partially on an art form inherent in the risk assessment procedure.
- When asked to comment on the usefulness of published guidance documents, the security consultant responded that the gaps in current systems cause them to be limited in value. The obvious tendency for professionals is to rely on the desires of the owner because of costs involved, and to defer the sub-standard and checklist methods that do not protect the facility mission and occupants, and usually provide a sense of false security to the public. Full risk assessment methodologies are available; however, the consultant felt that most professionals do not engage in such processes with clients because there are no building codes and standards of practice do not mandate protection levels. In the consultant's judgment, the current perception in the United States is that since there has not been an event since September 11th, 2001 there is little reason to be concerned about a malicious threat that the government has already eliminated. A final gap in security design pointed out by the professional

4. CURRENT RISK ASSESSMENT AND SECURITY DESIGN PRACTICES AND APPLICATIONS

is that engineers are risk averse, and therefore do not wish to engage in activities that might bring increased liability on them.

- Speaking generally on security assessment, the consultant felt that personal biases become part of the decision making process. In most situations, the astute analyst will highlight to the stakeholder the areas that were the most uncertain in the risk assessment, and provide some guidelines on the effectiveness and sensitivity of each recommended alternative, including the option of using redundant systems, recovery and emergency action plans, and alternative facilities in the event of an attack. The consultant felt that risk assessment procedures are usually difficult for risk averse engineers and managers. This is analogous to the tendency of increasing the design level with safety factors when there is uncertainty, such as in structural system design. Finally it was the security consultant's opinion that engineers might be better served if they were offered more risk assessment, probabilistic, and statistical education in during their university education.
- Other information on buildings that have implemented CB security features came mainly from equipment suppliers. A company representative that supplies a particular air treatment line of products provided information on projects that have implemented these technologies. The company only provides equipment and does not perform risk assessment or analysis on how the products will perform in the building. Systems were installed to create customized shelter-in-place areas. The designs involve pressurizing the room and treating the incoming air with various air cleaning technologies. These technologies included:
 - ▶ particulate air treatment using HEPA filters
 - ▶ gaseous contaminant air treatment using a combination of carbon and permanganate based media
 - ▶ additional carbon filtration for radioactive gases for high risk applications
 - ▶ treatments for incoming outside air using UVGI.
- These systems were self-contained systems and were implemented in high schools, embassies, and a bank located in the financial district of New York City. The products were also implemented in retrofit projects, more specifically air handling unit (AHU) alterations to a high risk building in the Washington D.C. area.
- A major CB project to a building in the Washington DC area involved AHU modifications to incorporate gas phase filtration and enhanced particulate filtration. While the building is not a high profile building, it is located in close proximity to one. The building was over 1 million square feet in floor area, but only 300,000 square feet were retrofitted. The project cost was about \$7 million and the project engineer performed an economic analysis for the design options and evaluated the recommendations. A risk assessment was performed for the project by a separate company, however the report is confidential.
- The retrofit proposal included a long list of preliminary options with costs associated with each measure. When detailed cost estimates were performed, the cost increased from the original estimates, which prompted the building owner to further reduce the CB mitigation measures. The implemented design included the installation of CB sensors around the building and providing extra filtration in the existing AHUs (especially ground level AHUs). Due to the high costs, the building owner rejected the "safe haven" design option, and was not willing to give up parking space where some of the equipment would have been installed.

From the answers of the contacted professionals, it is evident that few non-critical building owners are addressing the possibility of a CB attack to their facility. Of the example buildings found, most were located in high risk areas, or were high profile buildings. Even in projects that attempted to address a heightened risk of a CB incident actually occurring, design options were not implemented due to high costs. Finally, there exists a feeling among the design professionals that the push to design buildings to

be more resilient to a chemical or biological attack has run its course in the panic following the 2001 anthrax mailings, and has since then been relegated to the backburner if not entirely forgotten.

4.4 CONCLUSIONS AND RESEARCH NEEDS

The information gathered from the design professionals, building managers, owners, and security management consultants in this subtask make it is clear that CB security analyses or full risk assessment procedures are rarely requested by owners. Additionally, due to high costs, designs and technologies are not implemented specifically for security purposes in non-critical buildings. Without codes driving the decision process, engineers and security consultants rely on the priorities of the building owner, which typically is focused on economics. Most design professionals, however, are aware of available tools and guidance if such an opportunity should occur, quoting the documents produced by FEMA [2003] and NIOSH [2002] most frequently. A few unique risk assessment procedures and vulnerability assessments were found, but all generally involve the same steps.

The security enhancements described in published guidance documents are implemented as best practice by design professionals only if they do not impact the project budget. Passive security designs, such as elevating outdoor air intakes, are most commonly implemented in lower profile buildings. Expensive enhancements are well known, but are never considered as an option for this building category. Furthermore, no modeling procedures that aim to prove the effectiveness of CB security designs against an attack were reported and designers have a lack of confidence in the results. Without actual field verified data proving the validity of multizone modeling, the time and cost to model a building for CB security during design phase is unreasonable. Therefore, only enhancements with low initial, operating, and maintenance costs are being implemented without much understanding on how they will perform during an extraordinary incident.

The most detailed and distinctive responses came from design firms with their own risk assessment teams, security consultants, and equipment suppliers. The approach within this group of respondents is that a diverse panel including architects, engineers, facility managers, building owners, and equipment contractors should be present at the beginning of a security design project. A manufacturer involved in security system design continuously researches advances in CB security, performs risk assessments without the request from an owner, and seeks information on ways to fund the implementation of security enhancements. This multi-disciplinary team approach aims to implement the most appropriate system that meets both security and financial goals. The methodology is similar to the current trend in sustainable building design. However, due to the lack of examples, it is evident that there are driving forces (most likely cost coupled with the lack of information on the risk of a CB attack) preventing this assessment process from becoming popular in the design of non-critical buildings.

Finally, there are two very different views on risk assessment and CB security design. The companies and individuals that specialize in security design and risk assessment strongly encourage use of a full, formal procedure and feel that they can recommend the best solutions. However, little modeling or verification are employed to demonstrate that CB security measures are effective is performed by the same group. HVAC engineers and designers along with architects will not perform a risk assessment procedure unless asked to do so by the owner. In an industry where keeping costs low is a high priority, security enhancements are not implemented or even recommended to owners without significant proof of their effectiveness. The validity of modeling methods is also questioned by this group of professionals.

Responses to the questionnaire suggest the following future research needs.

- CB security risk assessment occurs in typical commercial/institutional building design only if requested by the owner. The decision to perform such a procedure or implement a security enhancement is almost entirely driven by economics. There is a need to have an assessment

4. CURRENT RISK ASSESSMENT AND SECURITY DESIGN PRACTICES AND APPLICATIONS

procedure that describes the CB threat and risk to building owners in terms of cost, and how potential consequences could be reduced by implementing certain security strategies. Without a quantifiable metric to prove that the threats could have serious impacts, such as lives lost and economic losses, there is no motivation to assess and evaluate the potential of implementing expensive technologies.

- Passive systems are being implemented in non-critical building design as good practice. However, according to published guidance, these common security designs protect against very few CB release scenarios. Therefore, research is needed to further develop more advanced active and passive security systems so that they can be implemented with low initial and operating costs.
- Computer simulation of CB security enhancements is rarely performed in industry. One reason for this is that the validity of available models is questioned. Therefore more field experiments to test the modeling results are needed, and based on the results, alterations to current simulation models will be required. More training courses on how to use programs that model building performances during a CB release would also be required, especially for design engineers and architects.
- Accurate modeling that can be coupled with a universally accepted evaluation metric that communicates both risk and risk reduction found from implementing resiliency enhancements will create a design procedure that gives design engineers the ability to assess and evaluate designs, proving their effectiveness in making the building more resilient from CB releases. This design procedure will require training workshops that illustrate the time to perform the process, the expected results, and all precautions found with using the procedure so that engineers are aware of any risks involved with relying on the models and guidance.
- Since almost all decisions on security design come from the building owner or stakeholder, better communication on the benefits and importance of CB security needs to occur between researchers, engineers, architects, and the general public. Disseminating further information on insurance and legal issues associated with CB incidents will illustrate risks to building owners and potential economic coverage benefits from implementing known security features.

5. SECURITY MEASURE ASSESSMENT AND DESIGN TRAINING AND CERTIFICATION PROGRAMS

5.1 OBJECTIVES AND SCOPE

The objective of this subtask is to summarize the activities of organizations involved in the development of procedures, training, and certification related to security assessment. Organizations that offer security certifications to individuals after completion of training courses and examinations were reviewed. Short courses and professional development seminars that focus on assessing the risk of a CB attack to buildings and methods to enhance its resiliency were also researched and summarized.

5.2 PROFESSIONAL SECURITY CERTIFICATIONS

Three of the major security certifications that are commonly acquired by professionals in the building industry are the Certified Protection Professional (CPP) [ASIS, 2008a], the Physical Security Professional (PSP) [ASIS, 2008b], and the Building Security Certified Professional (BSCP) [BSC, 2008a] certification. The CPP and PSP are offered by the American Society for Industrial Security (ASIS) and nearly 10,000 professionals have earned the CPP designation. The BSCP certification is offered by the Building Security Council.

Eligible applicants must meet one of the following requirements to be accepted as a CPP candidate:

1. Earned bachelor's degree or higher from an accredited institution of higher education and seven years of security experience, including at least three years in responsible charge of a security function.
2. Nine years of security experience, including at least three years in responsible charge of security function.

These eligibility requirements would seem to eliminate most building designers. ASIS defines "experience" as the individual having been personally engaged in security or loss prevention on a full-time basis, or as a primary duty. However, if an engineer or architect does security design regularly, he or she is eligible to earn the CPP certification by being involved "with companies, associations, government, or other organizations providing services or products, *including consulting firms*, provided the duties and responsibilities substantively relate to the design, evaluation, and application of systems, programs, or equipment, or development and operation of services, for protection of assets in the private or public sectors" [ASIS, 2008a].

If eligible, a CPP candidate must then successfully complete an examination to achieve the designation. The CPP exam consist of 200 multiple-choice questions covering tasks, knowledge, and skills in eight broad subject matter areas that current CPPs identify as important in security management. All exam questions come from ASIS's official reference book (Protection of Assets Manual), and no questions on the exam are taken from any other source. The categories covered in the exam include:

3. *Security principles and practices* - ability to plan, organize, direct, and manage the organization's security program to avoid or control losses and apply the processes necessary to provide a secure work environment. This section of the exam also assesses the abilities of the professionals to develop, manage, and conduct threat or vulnerability analyses to determine the probable frequency and severity of natural and manmade disasters.
4. *Business principles and practices* -ability to develop and manage budgets and financial control to achieve fiscal responsibility.

5. SECURITY MEASURE ASSESSMENT AND DESIGN TRAINING AND CERTIFICATION PROGRAMS

5. *Personal Security* – topics range from the development, implementation, and management of background investigations in coordination with other departments and agencies for the purpose of identifying individuals for hiring to developing and managing policies, procedures, and programs for personnel protection to provide a secure work environment.
6. *Physical Security* –how to survey facilities in order to manage and evaluate the current status of physical security, fire detection, and emergency capabilities. This category also covers the selection, design, and implementation of security measures to reduce the risk of a loss, and to assess the effectiveness of the security measures by testing and monitoring.
7. *Information Security* – this category covers the development and implementation of polices and standards to ensure information is evaluated and protected against from all forms of unauthorized access, use, disclosure, modification, destruction, or denial.
8. *Emergency practices* –how to mitigate potential consequences of emergency situations by identifying and prioritizing potential hazards and risks and developing plans to manage exposure to loss.
9. *Investigations* – this category explains how to develop and manage investigative programs. These programs include managing and conducting surveillance processes and investigative interviews.
10. *Legal aspects* – The final topic covered by the training and examination includes the development and security policies, procedures, and practices which comply with relevant elements of criminal, civil, administrative, and regulatory law to minimize adverse legal consequences. Currently, any legal issues associated with acts of terror or a chem./bio attack are not covered by the CPP.

ASIS also offers the PSP [ASIS, 2008b] certification for professionals whose primary responsibility is to conduct threat surveys, design integrated security systems that include equipment, procedures, and people, or install, operate, and maintain those systems. Eligibility PSP candidates must satisfy the following requirements with “experience” defined as it was for the CPP certification:

- Five years of experience in the physical security field
- High school diploma or GED equivalent
- The applicant must not have been convicted of any criminal offense that would reflect negatively on the security profession, ASIS, or the certification program.

Like the CPP exam, eligible candidates must successfully complete an examination to achieve the designation. The categories covered in the PSP certification exam include:

- Physical Security Assessment
- Establishing security system requirements and performance specifications
- Outlining criteria for pre-bid meeting to ensure comprehensiveness and appropriateness of implementation.

The Building Security Council’s (BSC) Building Security Certified Professional (BSCP) [BSC, 2008a] certification program was created in 2006 to provide design and security professionals with a credential that demonstrates a comprehensive, multidisciplinary understanding of building security issues. Eligible candidates for the BSCP certification are building security professionals who possess a license to practice architecture, landscape architecture, or as a professional engineer, or the ASIS International PSP or CPP credentials. Currently 49 individuals have achieved the BSCP credential.

The certification signifies that BSCPs have a broad knowledge and understanding of security considerations and can address them effectively in the integrated planning, design, construction, operation, and risk assessment of buildings. In particular, the BSCP is familiar with the building classification and field evaluation procedures described in the BSC’s Building Rating program,

5. SECURITY MEASURE ASSESSMENT AND DESIGN TRAINING AND CERTIFICATION PROGRAMS

Promoting Logical Unified Security (PLUS) [BSC, 2008b]. Similar to the CPP or PSP, a BSCP receives the credential after successfully completing the examination.

Training for BSCP candidates is held in the BSC's Building Security Certified Professional Seminar. The last seminar, held in September 2008, covered 7 domains of building security knowledge:

1. Project process
2. Risk assessment
3. Site considerations
4. Building envelope
5. Interior space
6. Facility operations
7. BSC rating system

One design professional contacted for information relating to Subtasks 3 and 4 of this project (see section 4) who holds the BSCP certification commented on the confidentiality of building security upgrades. It was stated that the understandable desire for both public and private buildings managers to keep their upgrades confidential has an inhibiting affect on the ability of technical professionals to communally learn together and for society to keep building security in the spotlight. This design professional feels the BSCP program is one way of maintaining the technical and awareness momentum, yet regulate the dissemination of sensitive information.

5.3 PROFESSIONAL DEVELOPMENT TRAINING COURSES

Several organizations have offered professional development training courses on the threat of CB terrorism to buildings and how to reduce the building vulnerabilities to an attack and some are still being offered. The short courses train professionals associated with the design and construction of buildings in risk management procedures, pros and cons associated of implementing security designs, and costs enhancing a building's resiliency. Most of the short courses identified are based on a guidance document published after the September 11th, 2001 terrorist attacks.

- The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) held one-time satellite broadcast short courses on homeland security for buildings in 2004 and 2006. Recordings of these presentations are available as DVDs. Topics included the threat of biological weapons, the role of filtration with building security in the post 9/11 world, personal protective systems, and multiple benefits solutions for enhanced building security [ASHRAE, 2007]. The sessions presented an overview of the protection of buildings and HVAC systems against intentional and accidental threats primarily to building airflows.
- The goal of the ASHRAE broadcasts is to teach the fundamentals of protecting building systems from both terrorist incidents and accidental events, and how to mitigate the consequences should an event occur. Resuming operations after an event and maintaining operations during a pandemic are also covered. Both design for new construction and retrofits are considered [ASHRAE, 2007]. The content of the courses is based in part on ASHRAE's *Report of Presidential Ad Hoc Committee for Building Health and Safety under Extraordinary Incidents* [ASHRAE, 2003].
- One of the features of the ASHRAE's satellite broadcasts that differ from others is that they are specific to the CB risk to buildings. Other professional development courses focusing on building design cover all aspects of terrorism risk. The ASHRAE broadcasts were developed so professionals would:

5. SECURITY MEASURE ASSESSMENT AND DESIGN TRAINING AND CERTIFICATION PROGRAMS

- ▶ Learn the difference between risk and vulnerability assessment and methods for their evaluation
 - ▶ Learn methods for choosing how to allocate resources among multiple buildings
 - ▶ Learn methods for designing security systems to help avoid releases
 - ▶ Become aware of software design tools and other resources that can be helpful
 - ▶ Become aware of other benefits of some of the solutions for ordinary operation to help justify their cost and synergies with other building systems such as blast protection.
- An ASHRAE professional development seminar entitled *Facility/HVAC Terrorism Threat and Vulnerability Reduction* [Dobbs, 2007] is also a building HVAC specific training course focusing on CB terrorism and threat mitigation strategies. The course provides a brief overview of the guidance documents published by ASHRAE since the September 11th terrorist attacks. It is scheduled periodically for presentation at ASHRAE conferences (for a separate fee) and could also be purchased for presentation to other groups (for example, in-house corporate training). The CB threats to buildings are outlined along with a brief history of CB incidents occurring in buildings. Based on the 2003 ASHRAE guidance document [ASHRAE, 2003], the presentation illustrates the steps involved with its risk management procedure.
 - This seminar concludes with a discussion of vulnerability reduction design methods. Differences between CB attack prevention methods to mitigation strategies are discussed along with examples of each. The resiliency enhancements discussed included air intake operation, the design of pressurization and filtration systems and controls, and the design of shelter in place areas of refuge. Multiple benefits that are possible with implementing certain designs were also covered in the short course.
 - A website, pdhengineer.com [Liescheidt, 2008] offers professional development hours for purchasing and completing an online course or webinar. A printable certificate is then offered instantly on the website. One online training course offered by pdhengineer.com, Design of Commercial Buildings to Mitigate Terrorist Attacks, gives an overview of the FEMA 427 document of the same title [FEMA, 2003]. The training consists of the professional engineer downloading the free FEMA document, studying it, and passing an online quiz. The goal of the course is to have the participant gain knowledge on terrorist threats, weapons effects, building damage, multi-discipline design approach, design guidance, occupancy types, and cost considerations.
 - The University of Wisconsin, Madison, offers continuing education courses for engineering and technical professionals. In the engineering, architecture, and construction field, one course is offered that focuses on building security [Maher, 2008]. The course entitled *Paying Attention to What We Protect and How* aims to answer the questions raised after the September 11th, 2001 attacks of:
 - ▶ Are government entities and individuals overreacting to security threats?
 - ▶ Is there a balanced approach to protecting buildings and the people who use them?
 - ▶ What should we be protecting and how?
 - The course examines the different threats to buildings with the objective to redirect thinking towards hazards that have a greater chance of occurring. For example, a scenario of leaking chlorine tank cars or other accidental discharges of hazardous agents is more probable than terrorist attacks for many buildings. These are threats, along with workplace violence, assault, theft, vandalism, and accidents due to faulty construction or poor maintenance, that pose a greater daily risk to most Americans than a terrorist attack. The course presents a negative view of protecting buildings specifically from a terrorist attack because of the low probability of occurrence compared to other incidents. Further, the course approaches balancing security designs between being proactive and reactive. The central

5. SECURITY MEASURE ASSESSMENT AND DESIGN TRAINING AND CERTIFICATION PROGRAMS

theme of the course is that it is equally important to protect against workplace crimes and accidents as it is to install complex security systems that may alter the impact of future terrorist attacks.

- A continuing education seminar hosted by the American Society for Civil Engineers (ASCE) provides a systematic and robust risk assessment and management (RAM) process for the evaluation of buildings and infrastructure security. This RAM process was developed by Sandia National Laboratories (SNL) and the seminar is based on their publication Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures [Biringer et al., 2007] which was also covered in the Subtask 1 literature review of this project [Bahnfleth et al., 2008a]. The purpose of the seminar is to teach participants the risk assessment process as developed by SNL with topics in [ASCE, 2007]:
 - ▶ Screening for critical assets
 - ▶ Assessing the threat of an attack to those assets
 - ▶ Evaluating the consequences that would result from an attack
 - ▶ Performing vulnerability assessments
 - ▶ Achieving a reasonable measure of security
- The Center for Energy Research and Technology at North Carolina A&T State University, along with the EPA, hosted a workshop in 2005 entitled Building Vulnerability and Protection against Chemical and Biological Agents [N.C. A&T, 2005]. The training course addressed the vulnerabilities found in most buildings and aimed to give participants an appreciation of the threat posed by various chemical and biological agents. The workshop's intent was to keep participants informed with current detection methods, available active and passive protection systems, as well as remediation techniques for decontaminating the building after an incident. Another subject covered was the legal ramifications before, and in the aftermath of a CB attack on a building.

5.4 CONCLUSIONS AND RESEARCH NEEDS

Professionals in the building industry have many options for receiving knowledge and training on understanding the threat of a CB incident and how to protect buildings from future attacks. Professional certifications on building security ensure that individuals have a thorough understanding on these subjects. However, individuals who receive the ASIS certifications generally are not involved with building design due to its restrictive eligibility requirements. Usually, if a CPP or PSP certificant is involved with building design it is as a security consultant who describes different risks to the building owner, not as a consulting engineer or architect. Furthermore, after contacting a few CPPs it was found that having a security consultant involved with CB building security issues is a rarity. The BSCP seems to be the only applicable security certification that has reasonable eligibility requirements for individuals directly involved with the design of buildings.

There are many short courses and professional development workshops available to individuals who have an active role in the building industry. Most are based on publically available documents and guidelines that most designers mentioned they were already familiar with from our Subtask 3 and 4 investigations, but they do vary in focus. While all training programs are based on security threats to buildings and mitigation, the University of Wisconsin short course takes the approach the threat is too small and should not overshadow other preventable hazards. Training courses based on publications such as FEMA 427 or ASHRAE's guidance document stick to the theme of "the threat of CB terrorism is real", and describe methods to make buildings more resilient.

6. PRIVATE SECTOR DEVELOPMENT AND IMPLEMENTATION OF ADVANCED BUILDING SECURITY SYSTEMS

6.1 OBJECTIVES AND SCOPE

The objective of this subtask is to summarize the activities of private sector commercial organizations focused on developing and implementing “advanced” building security systems. An attempt was also made to identify technologies produced specifically for CB security and to understand how they are integrated into a building. Information on projects that have implemented the products and any cost information were also of interest. The final goal of this subtask was to identify the direction in which this field of study is moving in terms of research, development, and implementation of “advanced” building security systems.

6.2 METHODOLOGY

Questionnaires were developed and sent to HVAC control contractors and companies that specialize in CB detection in an attempt to identify products and services offered by the companies regarding CB security. The questionnaire requested details on projects in which they have implemented special designs or products as a CB resiliency enhancement. The HVAC control contractors and developers were all asked a similar list of questions that was slightly modified to solicit information about specific products and services that each company offers and makes public. The questions included:

1. Have any “non-critical” building projects requested any CB security design solutions?
2. What products or CB security solutions does the controls company offer?
3. What technologies are integrated with their control systems for CB security?
4. What companies work with the controls company to provide security solutions?
5. What security designs solutions or technologies are currently being developed or perfected?
6. Are security designs tested for their effectiveness against a CB attack? If so by what methods are they tested, and can any data be provided?

A slightly different list of questions was sent to companies that specialize in the research and development of CB security technologies. These technologies are intended to be integrated with CB security control strategies, such as air handling unit fan shutdown, fast opening and closing outdoor air intake dampers for building purging, or activating stand-by filtration. Again, the questionnaires were slightly modified to get more specific information from each company but generally included:

1. What are the CB security solutions that each company offers for buildings, and can examples of designs that have been implemented be presented?
2. Have any CB security technologies been integrated with other companies’ control systems?
3. Have any of the security solutions been integrated in what would be considered a low-risk building, particularly non-government buildings?
4. How often are chem/bio security controls requested, or is this still a rare feature in most low-risk buildings?
5. Are the security solutions tested or modeled for their effectiveness against a chem./bio attack? If so, can any data or information on the security benefits buildings receive from implementing the technologies (such as more time to vacate the building, less people exposed, etc.) be provided?

6. PRIVATE SECTOR DEVELOPMENT AND IMPLEMENTATION OF ADVANCED BUILDING SECURITY SYSTEMS

1. Is any cost information available, either on the company's services cost, or on costs of recent projects that requested chem/bio security control systems?
2. Comments on where this field of research is moving in terms of product development or security solutions for buildings?

6.3 ADVANCED SECURITY SYSTEM TECHNOLOGY AND CONTROL SYSTEMS

Responses to the questionnaires indicated that the major control companies either wish to keep such information confidential, or do not offer/have not implemented any CB specific security designs in lower-risk buildings. If such a design was requested, the control companies indicated that ICx Technologies would be contacted to partner with them in reaching a CB security solution. No cost information or explanations on security solutions under development was offered in response to the questionnaires.

ICx Technologies products related to CB building security include a continuous indoor biological air monitor that is designed to detect biological threats by assessing changes in ambient air biological particulate levels [ICx, 2008a]. Response to a biological release in a building can occur from integration of these monitors with the building's existing control systems. The device can also be integrated with a sample capture technology to identify the exact agent. The biological air monitor detects concentration changes in airborne biological particles with a diameter range of 1 to 10 microns. The monitor can be located in a duct, on a wall, or be ceiling mounted and the event output can be integrated with LonWorks and other control systems for an appropriate response to a biological release.

For chemical detection, however, ICx does not offer any continuous air monitoring devices. Instead they offer agent detection kits which provides first responders with the ability to conduct surface, solid, and liquid interrogation of nerve, blood, and blister agents [ICx, 2008b]. All other detection and identification technologies offered by ICx are used after an attack in the "hot zone" to understand what building material is contaminated and with what agent.

Smiths Detection [2008] has developed a fixed site chemical warfare agent and toxic industrial chemical detection system designed with the intent of being used for HVAC system monitoring. The CENTURION system operates continuously to simultaneously detect chemical warfare agents and toxic industrial chemicals while being unattended. The detection system can be programmed to automatically actuate responses to an alarm, such as shutting down dampers and turning off fans.

The CENTURION system consists of multiple detectors remotely located throughout the building's duct work communicating to a central PC-based command center over a Local Area Network (LAN). Each detector has on-board supplies of verification substances and can be programmed to periodically run self-test. Chemical warfare agents that are detectable by the CENTURION system include nerve and blister agents such as Tabun, Sarin, Vx, and Mustard. Toxic industrial chemicals detected by the system include Ammonia, Ethylene Oxide, Chlorine, Hydrogen Chloride, and others [Smiths Detection, 2008].

Proegin [2008] has produced a chemical warfare agent detector that detects, in real time, almost all chemical warfare agents and numerous toxic industrial materials simultaneously. The instrument can detect all agents under vapor, aerosol, or liquid form. The unit is typically installed at the air intake of buildings or critical infrastructures. The product boasts the ability to be networked with other instruments so that upon alarm it can trigger the closing of the building ventilation system without initial calibration.

Genesis Air [2008] products use a three step approach to air cleaning that does not use ozone or produce by-products. The technology uses high-efficiency particulate filtration, UV lamps, and Genesis Air Photocatalysis. The goal of the air cleaner is to reduce particulate matter, neutralize and destroy biological contaminants, disinfect the air passing through, and destroy odors and toxic gases and organic compounds all from one unit. Genesis Air has a sizable range of products for different applications and budgets. While the published installations for CB security purposes were for high-profile government

6. PRIVATE SECTOR DEVELOPMENT AND IMPLEMENTATION OF ADVANCED BUILDING SECURITY SYSTEMS

buildings, the products were also implemented in non-critical buildings for tobacco smoke control (mostly casinos and bowling alleys).

New World Associates [2008] has developed a packaged air handling unit with a CB filter system. The AirePod™ CBR Filter System with Environmental Control adds heating, cooling, and humidity control to create a complete ready-to-deploy system for collective protection. The goal of this technology was to give buildings the ability to have CB security upgrades without the cost and inconvenience of disruptions found from implementing upgrades to the existing HVAC equipment. The AirePod unit is custom built to meet all needs.

6.4 CONCLUSIONS AND RESEARCH NEEDS

Recent development of advanced CB building security solutions has focused on high efficiency air cleaning technologies and real time continuous air monitoring for contaminant detection. Understandably no companies that are involved with the research and development of these products were willing to release any information other than what is already publicly available. New high efficiency air cleaning products package various technologies (particulate filtration, Gas Phase, and UVGI) into a single unit to increase resiliency from multiple threats. Convenience also is the focus of the new filtration equipment, with many new products that advertise easy installation without significant down time of the building's current HVAC system.

While detection equipment is designed to be integrated with the building's HVAC control sequences, no specific information on projects that have implemented the products in this manner or for CB security was found. Many of the existing CB sensor and detection technologies are being implemented in labs or industrial facilities where there is serious concern of a toxic substance being accidentally released. Information on the effectiveness of the designs against a CB release is still missing from this field of study. Detection equipment currently on the market claims rapid recognition and identification of a substance in the air. However, information on the time to detect an agent and activate a building response, such as system shut down, and the effect this procedure has on building exposure is still needed to justify implementing these expensive technologies for CB security purposes.

7. SUMMARY OF EXPERT PANEL MEETINGS

An expert panel comprising of architects, HVAC engineers, researchers, and insurance consultants was assembled to review and discuss findings and conclusions of this study. The panel meetings, both held at Penn State University, took place on October 6th and December 10th, 2008. The first meeting reviewed the findings and conclusions of the Subtask 1 and 2 reports. The second meeting's discussion focused on discussing the findings from the remaining subtasks as well as developing future research needs. This section summarizes the discussions and conclusions from the meetings as well as different viewpoints and additions to the Subtask 1 and 2 reports found from the panel's reviews.

7.1 EXPERT PANEL MEETING 1 SUMMARY

7.1.1 Literature Review (Subtask 1)

The assertion of calling the 2001 anthrax mailings a terrorist attack was also questioned. The incidents have not yet been identified with any terrorist organization. The only other event that terrorist used CB as a tool was the relatively unsuccessful Tokyo sarin gas incident. The questions and uncertainties associated with this particular incident raise questions about the ability to determine the probability of a CB event occurring in lower risk buildings.

It was noted that standard CB attack scenarios in the literature ignore possible motives beyond high casualty counts. For example CB agents could be used to neutralize security personnel at an entrance to achieve a primary objective of gaining entry to conduct an attack with firearms or explosives. For this and other reasons, guard personnel who control access should be in protected enclosures with separate HVAC systems from the lobbies. This design suggestion is also included in many guidance documents, but may be very impractical for most buildings.

Additional airborne release scenarios of concern identified by reviewers included an interior release by employees and accidents in laboratories and other areas where select agents are handled and stored. Means of CB releases other than airborne incidents were mentioned. Powder forms of agents sent through the mail has already occurred, but distribution could also take place through food and water, including vending machines.

While many airborne release scenarios have been studied and published, the list is incomplete. A motivated individual may use any means necessary to perform a CB terrorist attack, which poses the question of how should a stakeholder or building designer select a scenario to protect against? For an overall prevention protection scheme, physical security which includes having the appropriate amount of personnel may be more effective than a few engineering features that are only effective in certain situations.

One of the major criticisms leveled at existing risk assessment procedures is that they rely excessively on human judgment. The question raised by the expert panel was: what amount of human judgment is essential for the procedures, and how much can be replaced by a formal analysis or automation? The amount of subjectiveness embedded in the procedure will affect the decision to implement a mitigation strategy. Moreover, from the discussion, the first decision in the risk assessment process that could change which measures are considered is determining whether a particular CB attack is more of a risk to the facility than an accidental event. The feeling amongst the panel was that multiple events need to be considered in the assessment, not CB incidents alone, to justify implementing a security design.

Development of information on cost justification of engineering security enhancements was stressed as being an important future research need in the literature review. The expert panel suggested that more

7. SUMMARY OF EXPERT PANEL MEETINGS

information on the economic impacts due to the loss of use or mission of the facility is critical to understanding consequences that could occur from a CB incident. There is a problem with the current method of quantifying the indoor air quality benefits found with certain security designs. Assessing and evaluating multiple benefits need to be based on quantitative IAQ analyses.

Limitations of whole-building metrics cited in the literature review were also discussed. Building exposure averages may not be useful if concentrations in some areas such as the lobby are lethal while other areas in different zones are zero. One reviewer also commented on the fraction of building exposed (FBE) and fraction of occupants exposed (FOE) metrics by suggesting that it may be more important to know who is infected and to what extent rather than how many.

Comments on the CB resiliency enhancements covered in the literature review are summarized below.

- In new building design, spatial and HVAC zoning as a security design method begins with space planning and organization of functional adjacencies so that potential target areas are segregated from other areas. Also, circulation among areas needs to be zoned.
- A security feature which needs to be addressed is proper sealing of doors between areas of different pressures. Seals are very tight and the pressure differential is so great that doors are difficult to open. This can be especially hazardous for persons with disabilities and for everyone at emergency exits, such as doors leading into fire stairs.
- There is a gap in knowledge in regards to the decision making process, and more specifically the consequences of erroneous decisions or false alarms.
- Egress management during emergencies should be managed by planning and operations to allow safe egress without penetrating contaminated zones (such as lobbies) or without breaking air-tight seals.
- Different access control technologies were described in one review. Mechanical locks such as cylindrical or mortise locks are simple, if not highly effective against determined breach. Ordinary six-pin keyways are not as effective as various forms of high-security keyways. Card access and other systems which track and segregate authorized users are more complex and more effective.
- Decontamination issues mentioned included the fact that many plenums are shared by multiple building systems from structural to lighting that all can have complex surfaces, sometimes including sprayed-on-fire proofing, all of which make decontamination much more difficult than smooth ductwork.
- In the literature review, enhanced filtration efficiency was mentioned to be dependent upon maintenance and installation quality. The reviews also mentioned that achieving high filtration efficiency also requires infiltration control, stressing the importance of envelope tightening.

7.1.2 Review of Existing Methods and Protocols (Subtask 2)

The expert panel discussion on the Subtask 2 findings was primarily focused on the usefulness and applicability of the tools in assessing risk and leading to an implementation decision. There were disagreements among the panel members on whether or not the tools and analysis methods should be the same for new and existing buildings, which then led to the discussion of the subtask's evaluation of the CBT. The CBT, which was deemed an appropriate tool for both types of projects in the Subtask 2 analysis, was actually developed for the architect's use during early building design. The goal of developing the CBT was to create a tool that would influence which measures need to be evaluated in detail. Providing high fidelity in the outcomes was not the objective of the program. While the intended use of the tool was strictly for early building design, some panel members supported the use of the tools and analysis procedures to be applicable for both retrofit and new construction projects.

The panel commented that perhaps CBT overstates the importance of having an emergency response plan in place. The tool's embedded calculations assign a high value for the vulnerability rating when there is no plan, indicating that the building and its occupants are less vulnerable to a CB attack when an emergency plan is in place. The tool, however, does not give a high level of credit for a building that implements engineering or architectural features without an emergency plan. The reasoning behind the tool's methodology is that training is needed for building occupants or facility managers to operate the advanced security features. Furthermore, emergency response plans are intended to train occupants how to react during an extraordinary event so to minimize consequences, which were stated to be a reason why many lives were saved during the September 11th, 2001 attacks on the World Trade Center.

Other comments on Subtask 2 suggested future research needs for risk assessment tools design guidance documents. One suggestion includes having an intelligence based analysis where databases are embedded into the tools which can hopefully provide a more accurate assessment of the risk to a facility. There panel also emphasized the need for more validation of the tools.

7.1.3 Identifying Projects, Industry Practices, Technology Development (Subtasks 3-6)

Findings of Subtasks 3 and 4 of this project showed that it is uncommon of engineers and architects to perform CB risk or vulnerability assessments for most commercial and institutional buildings as part of planning and design. The consensus of the expert panel was that engineers and architects should not do these assessments unless they are professionally qualified and insured for liability, which implies the individual has formal training and certification in security.

7.1.4 General Discussion

Since the literature review focused on security enhancements to make buildings more resilient from airborne contaminants, engineering designs and technologies associated with the HVAC system was the primary target. However, reviewer comments state that security design begins with site selection and goes on to include site planning and engineering. For retrofits, engineering solutions can be applied to overcome building features that make the structure vulnerable to CB and other hazards.

More specific non-government and non-symbolic building types that could be very attractive target for CB terrorism was offered in clarification of this report's broad categorization of commercial/institutional buildings as lower risk. These include:

- Research laboratories – especially university based
- Communications centers, including TV and radio stations
- Entertainment venues
 - ▶ Theaters
 - ▶ Arenas
- Religious buildings, both the worship and central denominational administration offices
- Transportation centers such as airports, bus, and railway stations
- Financial centers
 - ▶ Securities trading floors
 - ▶ Banks (both the front and back of the house)
 - ▶ Data centers

7. SUMMARY OF EXPERT PANEL MEETINGS

- Manufacturing and distribution

Estimating the probability of a CB incident from the very limited history of such events seemed unreasonable/impractical to one panel member. The scarcity of such events suggests that the use of CB agents is unattractive to potential perpetrators because of the difficulty of obtaining the agents and the danger of handling them. Explosives, on the other hand, are readily available and cheap and can do far more spectacular damage.

The expert panel identified the differences that exist between owned and leased buildings when determining how to assess risk or evaluate security designs. Assessing risk and liability concerns becomes even more difficult when dealing with multiple-occupant leased buildings. Another mentioned research need was to develop a better understanding of the details on liability concerns associated with CB incidents and the decision to implement security enhancements.

7.2 EXPERT PANEL MEETING 2 SUMMARY

The second expert panel meeting took place at Penn State University on December 10, 2008. The discussion focused on critiquing the information gathered during subtasks 3-6 and on developing a list of research needs. The panel's main concern with the information found during the work of subtask 3-4 was that the design professionals contacted were mainly from a fairly restricted geographical region (Mid-Atlantic States). Furthermore, the panel disagreed with some of the viewpoints provided by the contacted professionals. Statements that professionals generally are not implementing high efficiency filtration beyond than the base requirements as laid out by ASHRAE or the GSA as best practice due to potential of air pressure drop increases were disputed by some. Higher efficiency particle filtration, such as MERV 13 filters, are being implemented for air quality purposes to meet the requirements for LEED certification (not as a security measure). Given this difference of opinion, it was concluded that there may be a communication gap between research and industry on this topic.

Another issue discussed was that designing HVAC systems to mitigate a CB attack may add a new level of complexity and sophistication to already complex control systems, making commissioning of systems as well as training of operators even more important. Recent post-occupancy evaluations performed by the GSA found strong evidence that many systems do not operate as designed, partly due to an utter misunderstanding of the design intent. Therefore, while much effort is being made in research and development to create advanced CB security systems, commissioning and re-commissioning needs stressed to insure the building and any CB security features are operating properly.

8. FUTURE RESEARCH NEEDS

Based upon the entirety of the information gathered during this review, analysis of risk assessment tool performance, and input from a panel of experts, six areas of high-impact research were identified. Each of these proposed areas of investigation addresses a key gap in knowledge or barrier to adoption of a risk management approach to CB security of buildings.

Improved Metrics

The variety of performance metrics for CB security proposed in the literature (such as relative risk based on time and space-averaged exposure, area or occupant weighted exposure criteria) have significant limitations. More effort needs to be devoted to developing a weighted single factor which weights occupant impacts, remediation costs, countermeasure costs, and others—in a formula simple enough to be useful and detailed enough to be accurate and which would serve as the objective function which needs to be minimized. This factor should characterize the CB threat and risk to building owners in terms of cost, and how potential consequences could be reduced by implementing certain security strategies. An initial phase of metric development could be based primarily on literature survey and modeling. The estimated duration and cost for this phase would be a 2 year effort at roughly \$150,000 per year. This initial development phase should be followed by a testing and verification phase involving applications to example buildings at roughly the same level of effort.

Better Understanding of the Decision-Making Process

It is clear that the vast majority of building owners and occupants who have taken the time to consider CB security have decided not to implement any security measures. The most common explanation for why this is the case is that the owner's perceived risk is low and the cost of protection is significant. Nevertheless, buildings are routinely protected against many other natural and man-made hazards for which the risk to a typical commercial or institutional building is low. Questionnaire respondents and expert panel members agreed that the decision hinges on economic arguments. Consequently a productive area of research may be further study of the process by which owners make decisions in order to identify what further decision support tools may be needed that have not already been identified, or how the decision-making process should be modified. Such research might lead in the direction of a conclusion that what are needed are changes in mandatory building codes and standards to ensure that an acceptable minimum level of security is provided in all new buildings. A preliminary investigation involving extensive surveys of decision-maker behavior might be a 1-1/2 to 2 year effort requiring a substantial number of interviews and case studies at a cost of \$150,000 per year.

Improved Incident Modeling Capability Coupled to Formal Risk Analysis

One of the key barriers to a quantitative economic analysis of CB incident consequences is the ability to quantify the consequences of an incident for a specific building. Another barrier is the perception that currently available modeling capabilities are not sufficiently reliable/realistic. Although sophisticated general purpose air and contaminant flow models capabilities are available to the HVAC design community in the form of computational fluid dynamics programs and multizone modeling programs, these tools lack an equally sophisticated capability to simulate CB incident scenarios in a realistic way (release scenarios, system and occupant movements, etc.) and direct coupling to formal risk analysis procedures based on metrics derived from building-specific modeling. Efforts to improve air flow and

8. FUTURE RESEARCH NEEDS

contaminant dispersion modeling have been ongoing for years and literally millions of dollars have been expended on the effort. However, a group of 2-3 year, \$200,000 - \$300,000 per year projects could make significant strides forward on various aspects of this problem: metric definition, occupant movement, dynamic models including sensor-driven system response, and others.

Formal Risk Assessment Procedures and Supporting Data

This review of available security enhancement protocols and methods actually in use has indicated that formal risk analysis by properly trained professionals is not employed to the degree that it should in the evaluation of CB security measures for buildings. Underlying reasons range from the limitations of available tools to the lack of data needed to perform a formal analysis to the attitudes of some security professionals. Clearly, there is room for development of procedures that address the entire process from concept study to implementation, and for their implementation in user-friendly software. A significant effort would be required to produce computer-based, building specific methods together with the data needed to exercise them. To fill gaps in existing methods and validate the methods used might require 2 – 3 years and expenditure on the order of \$250,000/year.

Multiple Benefits Research

Because the decision criteria for lower-risk commercial and institutional buildings identified in this study are primarily economic, it is essential that professionals engaged in risk assessment be able to quantify secondary benefits of security measures, including health and productivity benefits of better indoor air quality and energy savings from HVAC system changes, increased envelope air-tightness, reduced ventilation made possible by enhanced air treatment, and other possible sources. Simulation-based demonstration of such benefits might require a 1-1/2 to 2 year effort at a cost of \$150,000 per year. Demonstration of benefits through field or laboratory investigations would require a much greater investment over a longer period of time, but may be necessary to build credibility. A shortcoming of current multiple-benefit literature, particularly that relating to health and productivity, is the level of uncertainty associated with the benefits. Annual savings calculated in the tens of billions of dollars on the national scale \pm billions of dollars are not easily applied to a particular project and tend to be brushed aside in deference to first cost in many projects.

Verification and Validation of Risk Assessment Methods and Security Measures

A number of expert panel members, as well as questionnaire respondents expressed concerns about the accuracy of available modeling and the reliability of claims of effectiveness for various protection strategies. In order to building confidence in the owner/designer communities, credible field studies to document the performance of analysis tools and protective technologies are needed. The cost for such efforts would be very significant—potentially millions of dollars for multi-year projects.

9. REFERENCES

- ASCE, 2007. Risk Assessment and Management for Buildings and Infrastructure Security seminar information flyer. American Society of Civil Engineers. Reston, VA.
- ASHRAE, 2003. Risk Management Guidance for Health, Safety and Environmental Security under Extraordinary Incidents. American Society for Heating, Refrigerating, and Air Conditioning Engineers.
- ASHRAE, 2007. Facility/HVAC Terrorism Threat and Vulnerability Reduction seminar series. <http://www.ashrae.org/education/page/763>. American Society for Heating, Refrigerating, and Air Conditioning Engineers.
- ASIS, 2008a. Certified Protection Professional information website. <http://www.asisonline.org/certification/cpp/index.xml>. American Society for Industrial Security International. Alexandria, VA.
- ASIS, 2008b. Physical Security Professional information website. <http://www.asisonline.org/certification/psp/pspabout.xml>. American Society for Industrial Security International. Alexandria, VA.
- Bahnfleth, W., J. Freihaut, J. Bem and T.A. Reddy, 2008a. Development of Assessment Protocols for Security Measures- A Scoping Study. Subtask 06-11.1: Literature Review, submitted to the National center for Energy Management and Building Technologies, Alexandria, VA, prepared for U.S. Department of Energy, February.
- Bahnfleth, W., J. Freihaut, J. Bem and T.A. Reddy, 2008b. Development of Assessment Protocols for Security Measures- A Scoping Study. Subtask 06-11.2: Identification and Evaluation of Existing Tools, submitted to the National center for Energy Management and Building Technologies, Alexandria, VA, prepared for U.S. Department of Energy, July.
- Biringer, B.E., Matalucci, R.V., O'Connor, S.L. 2007. Security Risk Assessment and Management. A Professional Practice Guide for Protecting Buildings and Infrastructures. John Wiley & Sons, Inc. Hoboken, NJ.
- BSC, 2008a. Certification for Building Security Professionals information website. www.buildingsecuritycouncil.org/certification.html. Building Security Council. Reston, VA 20191.
- BSC, 2008b. "Building Rating System Version 1.2." Building Security Council. Reston, VA 20191.
- DHS, 2008. "Daily Open Source Infrastructure Report." The U.S. Department of Homeland Security. http://www.dhs.gov/xinfoshare/programs/editorial_0542.shtm.
- Dobbs, Greg, 2007. Facility/HVAC Terrorism Threat and Vulnerability Reduction ASHRAE Professional Development Seminar Presentation. ASHRAE Learning Institute, 2007.
- EIA, 2003. "Commercial Building Energy Consumption Survey (CBECS)." Energy Information Administration. Retrieved from
- FEMA, 2005. Risk Assessment A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings. FEMA 452. Washington, DC: Federal Emergency Management Agency.
- FEMA, 2003. Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks. FEMA 427. Washington, DC: Federal Emergency Management Agency.

9. REFERENCES

- Fielding, J.E., Schunhoff, J.F., Aguirre, A., 2006. BAC-Building Assessment Checklist Protection Against Airborne Hazards. County of Los Angeles Public Health, Los Angeles, CA.
- Genesis Air, 2008. Genesis Air Product Catalog and Example information presentation. Retrieved from <http://www.genesisair.com/products.html>. August, 2008.
- GSA, 2005. Facilities Standards for the Public Buildings Service. U.S. General Services Administration Office of the Chief Architect.
- ICx, 2008a. AirSentinel 1000B Ambient Aerosol Detector Product Literature. ICx Technologies. Albuquerque, NM.
- ICx, 2008b. Agentase Disclosure Spray Product Literature. ICx Technologies. Albuquerque, NM.
- LBNL, 2005. BVAMP - Building Vulnerability Assessment and Mitigation Program, Lawrence Berkeley National Laboratory, Berkeley, CA.
- Liescheidt, Steven G, 2008. Design of Commercial Buildings to Mitigate Terrorist Attacks professional development course. http://www.pdengineer.com/Course%20Web/Building%20Design%20Courses/building_design_mitigate_terrorist_attacks.htm. Retrieved August, 2008.
- Maher, Mary, 2008. Serious About Security professional development seminar information website. http://epdweb.engr.wisc.edu/AEC_Articles/17_Security.lasso. University of Wisconsin Madison. Retrieved August, 2008.
- N.C. A&T, 2008. Building Vulnerability and Protection against Chemical and Biological Agents workshop information flyer. North Carolina A&T State University and the Environmental Protection Agency. November, 2005.
- New World Associates, 2008. AirePod™ CBR Filter System with Environmental Control product information website. http://www.newworldassociates.com/products/cbrn_and_wmd_defense/airepod_cbr_filter_systems/index.php. Fredericksburg, VA.
- NIOSH, 2002. Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks. National Institute for Occupational Safety and Health, May 2002.
- Proengin, 2008. Proengin AP4C-F real time chemical warfare agent detector product information webpage. http://www.proengin.com/index.php?option=com_content&task=view&id=24&Itemid=32. Retrieved August, 2008.
- Rhode Island Department of Health, 2004. BVAT - HVAC Building Vulnerability Assessment Tool, Office of Occupational and Radiological Health Indoor Air Quality Program, RI.
- Smiths Detection, 2008. CENTURION product information website. <http://www.smithsdetection.com/eng/Centurion.php>. Smiths Detection, Smiths Group plc.
- UTRC. 2004. CBT-Protection Improvement Design Protocol- Chem/Bio: User's Guide. East Hartford, CT, United Technologies Research Center.

APPENDIX A - BUILDING SECURITY ASSESSMENT AND DESIGN QUESTIONS

BUILDING SECURITY ASSESSMENT AND DESIGN QUESTIONS

The Design Approach

1. How do you perform vulnerability assessments on buildings?
2. Do you use any of the available design guidance documents in your vulnerability assessment such as FEMA's Building Vulnerability Assessment Checklist or LBNL's Building Vulnerability Assessment and Mitigation Program?
3. Have you used any of the design guidance documents in selecting resiliency enhancements? If so, which ones? If not, what is the basis of design decisions?
4. Do you test or model potential implemented changes to the building to understand their effectiveness against an airborne releases? If so please describe the process.
5. Are cost-benefit analyses used in the decision process? How much weight does the cost-benefit analysis hold in a decision compared to increased security?
6. Have you try to identify and quantify any multiple benefits (in addition to increased security) that result from using the designs such as improved Indoor Air Quality or energy savings?

Security Design Process for Specific Buildings

This section includes questions specific to buildings that have undergone a security assessment or has had resiliency upgrades implemented. With the understanding that this is sensitive information, only information approved for publication by you or the owner, as appropriate, will be published.

Please answer the following questions concerning the assessment process for each building.

General

1. Owner name and contact information. Would it be preferable for us to contact the owner directly?
2. Basic building data: occupancy type, size, number of stories, etc.
3. HVAC system type(s)?
4. New building or retrofit project? If an existing building, where any CB security features already in place?

Design phase

1. Was a vulnerability assessment performed on the building?
2. Were any assessment and design guidance documents used in the vulnerability assessment or selection of enhancements such as FEMA's Building Vulnerability Assessment Checklist or LBNL's Building Vulnerability Assessment and Mitigation Program? If not, can you please describe the design and assessment methods used?
3. If one or more of the current guidance documents were used, can you please comment on the evaluation? Did you notice any gaps in the procedure?

APPENDIX A - BUILDING SECURITY ASSESSMENT AND DESIGN QUESTIONS

4. What criteria and procedures were used to evaluate the effectiveness of security designs or technologies?
5. Did you test or model potential implemented changes to the building to understand its effectiveness against an airborne release? If so please describe the process.
6. Were multiple benefits, other than increased security, that result from using the designs such as improved Indoor Air Quality or energy savings assessed, and what was found?

Design decision

1. What conclusions were produced from the vulnerability assessment and design procedure?
2. What designs or technologies were implemented to the building?
3. Please describe the effectiveness of the security designs implemented in enhancing the building's resiliency from an attack. What types of attacks (inside release, outdoor release, outdoor air intake release, etc.) were these designs proven to be effective against?
4. What types of costs were involved with the design, and what were the approximate values? If possible, can you provide any other cost data, such as \$/ft² or \$/cfm?
5. How much weight did a cost-benefit analysis, if performed, hold in the decision process compared to increased security?

Please provide any other information or comments about the assessment, design process, and implementation of designs based on your experience.

Would you be willing to answer follow-up questions on this topic and questionnaire in the future? If so, can you please provide your preferred means of contact and contact information?

NATIONAL CENTER FOR ENERGY MANAGEMENT AND BUILDING TECHNOLOGIES

601 NORTH FAIRFAX STREET, SUITE 250

ALEXANDRIA, VA 22314

WWW.NCEMBT.ORG

