

ORNL-M02-113973

**Building Assurance:
September 11 and National Security Implications
for the Built Environment**

White Paper

Prepared for the

Energy Efficiency and Renewable Energy's Buildings Program

U.S. Department of Energy

Stanton W. Hadley
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, TN 37831-6070
865-574-8018, fax:865-574-9338
hadleysw@ornl.gov

April 2, 2002

Building Assurance: September 11 and National Security Implications for the Built Environment

S. W. Hadley

Abstract

With the increased emphasis on security following September 11, DOE organizations are asking how their programs intersect or should intersect with DOE's mission of security. Risk can be thought of as the combination of threats, vulnerabilities, and consequences that a building faces. These risks can be targeted at the building's physical assets, cyber assets, systems interconnectedness, or interdependencies with other infrastructures. A vulnerability assessment measures the risk that a building faces, and can be simple or complex, broad or narrow. Various responses to alleviate those risks can be categorized by type: prevention, mitigation, detection, and recovery.

Numerous energy-efficiency technologies can also improve infrastructure assurance from intentional attacks. HVAC system performance is crucial for improved protection from chemical or biological attack. Improved zoning, tighter ductwork and building envelopes, high efficiency filters, UV light, desiccant systems, and rapid control of fans and dampers can all mitigate the consequences or speed recovery. Distributed energy resources can make the building more resilient from power grid attacks, as well as lower the peak stress on the grid. Energy management systems can be enhanced to incorporate emergency response systems that help protect the occupants and facilities. Cost savings from energy efficiency technologies can help pay for the enhancements for security, providing additional benefits to building owners and occupants.

While other organizations, such as the military, have long worked in this field, DOE's Office of Energy Efficiency and Renewable Energy (EERE) and its Buildings Program has a role to play. A number of programmatic options are presented. The EERE could play a role by incorporating assurance into its analyses and technology development. Its contacts and ongoing relationships with states and communities provide a natural outlet for distribution of assurance-related information. Together, these activities can incorporate DOE's security mission into the buildings program.

1. Introduction

The events of September 11, 2001, have reverberated throughout American society and government, leading people to ask how their ongoing activities are affected. In January 2002, the Building Technologies and State and Community Programs (BTS) office within the Department of Energy's (DOE's) Office of Energy Efficiency and Renewable Energy (EERE) requested a review of the implications of September 11 and national security on the built environment. (A recent reorganization within EERE has changed offices and responsibilities, so for this paper we refer to the former BTS as the Buildings Program.) What is the full set of potential national security concerns as they relate to homes and buildings? Who are the stakeholders exploring the issues? What is DOE's role in making homes and buildings more secure? How does the Buildings Program's current portfolio address national security considerations, if at all? If this is a Buildings Program issue, what role might it envision playing over the next five years or longer in terms of R&D, codes and standards, and deployment?

Secretary of Energy Spencer Abraham has declared that security is core to DOE's mission. To put this into practice, each office needs to consider its portfolio of activities to determine how its programs answer the call to action. Before an office can analyze its program, however, it must evaluate how national security issues interact with its activities.

This paper will evaluate how national security and infrastructure assurance intersects with energy-efficiency improvements in the built environment. We will first describe infrastructure assurance and risk,

and then examine the major elements of risk and the different approaches to manage those risks. We will then review the major risks faced by building environments and how to address these risks. We will consider how energy-efficiency improvements, especially those being studied by the Buildings Program, can influence the protection offered by buildings. The role of EERE and other stakeholders will be discussed, followed by an exploration of the uncertainties or gaps in knowledge that could be addressed in the future.

2. Infrastructure Assurance Basics

As one of the major infrastructures of this country, buildings have a wide array of functions: protect occupants from the elements, enable productive activity, and create a livable environment, among others. As was so vividly shown on September 11, buildings are also one of our more vulnerable infrastructures. New concerns about building safety require that their assurance be systematically examined. Now, besides the “traditional” threats of nature and accidents, we must consider those vulnerabilities and consequences posed by intentional threats. Our military has had to consider these factors for centuries, but even they are now looking into the new threats from chemical, biological, radiological, and cyber warfare.

In the late 1990’s, the concerns about Y2K problems with computers led many industries and the government to begin systematically analyzing their vulnerabilities. The President’s Commission on Critical Infrastructure Protection issued a report on the dangers that the country faced (PCCIP 1997). Following the report, President Clinton issued Presidential Decision Directive-63. Each department of the federal government was assigned national infrastructures and told to examine how the protection of those infrastructures could be assured. The built environment was not treated as a separate infrastructure but rather as a component within the sectors listed (e.g., energy, finance, transportation, communication.)

Buildings across this country are very heterogeneous. They range from the tallest skyscraper to the smallest shack; from factories to retail stores to homes and apartments. The functions they perform in society, their economic or symbolic importance, and the consequent level of security varies across the board. Hospitals will have different concerns than a military facility, offices will have different concerns than apartments, etc. A key issue is how to determine the level of risk that any single building faces and the responses that could be taken to improve its assurance.

The Department of Energy’s Office of Critical Infrastructure Protection (OCIP) was formed to conduct research on the energy infrastructure. Much of the information describing infrastructure assurance is available from DOE’s R&D Agenda (OCIP 2001). They have funded research in several areas, most notably in developing vulnerability assessment best practices and infrastructure interdependencies.

2.1 Three elements of risk

There are three elements that together comprise the risk that society bears with any infrastructure: the threats against the infrastructure, its vulnerability to disruption from those threats, and the subsequent consequences to stakeholders or society. Combined, these represent the risk from a facility being harmed or otherwise unable to fulfill its functions. The threats, vulnerabilities, and consequences can vary for any given building, meaning the risks that it faces could be low or high.

Threats

Threats can be natural, accidental, or deliberate. Natural threats include such things as earthquakes, hurricanes, or tornadoes. Such threats can cover broad geographical areas such as floods, or be limited to single buildings, as in soil subsidence. In general, these threats are well recognized and plans to avoid them, reduce the building’s vulnerability, or mitigate the consequences are incorporated in the building’s design and operations.

Accidental threats can result from equipment failure and/or operator error. Construction accidents, poor maintenance practices, and equipment malfunctions are all examples of accidental threats. Faulty

system interconnections or poorly managed cyber assets are more recent accidental threats as buildings become more automated and connected to the Internet. Accidental threats can be internal or external to the building, such as fires within the building or in neighboring buildings. Again, most accidental threats have long been recognized and plans have been established to deal with them. Many accidental threats are due to recent advances in technology, however, and may not have been fully analyzed. Cyber assets, system interconnectedness, and interdependencies have all become more prevalent in infrastructures such as buildings. Plans to deal with them may not have kept pace with the advances.

Following September 11, deliberate threats have come under intense scrutiny. These threats can come from either organizations or individuals that have both the intent and the capability to carry out harm to the infrastructure. They can be hostile outside governments, terrorists, organized crime, disgruntled employees, computer hackers, or anyone choosing to attack. Threats can be against any of the types of vulnerabilities: physical, cyber, interconnectedness, or interdependencies.

Vulnerabilities

The vulnerabilities of an infrastructure are those elements of its design and operation that would render it susceptible to a threat – be it natural, accidental, or deliberate (OCIP 2001). Typically, four areas of vulnerability are identified in a complex infrastructure: physical assets, cyber assets, internal system interconnectedness, and interdependencies with external systems. Buildings include these assets to various degrees, depending on the nature of the activities within the building, the construction and operating characteristics, and building location.

Physical assets represent the tangible property subject to physical attack. Buildings as a whole, as well as the physical property within, represent clear physical assets that may be vulnerable to attack. The people in the building are vitally important to protect and are the major “assets” for which protection systems and plans are developed.

Cyber assets refer to the information and communication assets of an infrastructure. Vulnerabilities can render them unavailable for use, compromise the integrity of their data, and/or breach the confidentiality of information. Buildings share these assets with other critical infrastructures, depending on the nature of the activities and the type of monitoring, controls, and communication within the building.

System interconnectedness refers to the interconnection of complex components within the infrastructure. Vulnerabilities include inadequate compatibility, especially during operation under stressed conditions. Buildings may face this vulnerability through such components as lack of connection between fire detection systems and ventilation fan controls or public address systems.

Interdependencies refer to the connections between one infrastructure and another. Vulnerabilities lie in the reactions of one system to the partial or complete failure in another. Buildings are reliant on a web of other infrastructures, such as electricity, natural gas, water, sewage, transportation, and communication. Both the physical building and the activities within can be affected by the failure of these other infrastructures. The level of failure or continued operation is dependent on the resiliency of the building’s own infrastructure.

Consequences

Besides threat and vulnerability, one must consider the consequences from harm done to the specific infrastructure. The loss of a major building such as the World Trade Center or the Pentagon, including the symbolic psychological damage, can be much greater than the loss of smaller or less vital facilities. Human cost, economic cost, national security, and heritage are all factors in evaluating the consequences should a facility or infrastructure be lost.

Further, the speed and level of recovery can change the long-term consequences should an attack happen. If redundancy or resiliency are planned for (e.g., backups of key information and equipment, alternate plans for operation, distribution of functions between multiple facilities) then the consequences from the loss of an infrastructure are reduced.

2.2 Vulnerability Assessment

A vulnerability assessment can identify the risks an entity faces by evaluating the threats, vulnerabilities, and consequences of the entire entity or of various infrastructures or operations within it. The entity could be a private company, a government organization, or some sub-unit within any of these. Various infrastructures could be singled out for analysis, such as computer networks, manufacturing plants, or single buildings. The focus of the assessment could be on just certain vulnerabilities such as physical asset protection or interconnectedness.

Vulnerability assessments can be very simple or very detailed. A concern arises that with increasing detail, the results are much more sensitive and require a great deal of confidentiality. Government information about threats can easily get into classified intelligence. It would not be good to evaluate an infrastructure for its weaknesses and then have that information easily accessible to outsiders. At the same time, the information needs to be shared within the organization with a need to know, in order that corrections can be made.

For buildings, it may be useful for the Buildings Program or another organization to create a simple checklist or rating system for the risks of a building. A template listing the main possible threats, vulnerabilities, and consequences could be distributed. Building owners could then evaluate their buildings and rate the risk as low, medium, or high. They could then decide on the best corrective actions based on the level of risk. Because building types and functions are so heterogeneous, they must be evaluated separately. A template can give a rigorous method for making the distinctions between building functions and types, helping to determine the appropriate response based on the actual building involved.

The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) has released guidance for risk management under extraordinary incidents (ASHRAE 2002). They had three major preliminary recommendations for building owners and managers:

- Understand the capabilities of buildings and their systems,
- Assure that buildings are performing as intended,
- Do not make changes to building performance unless the consequences are understood.

While they also had more detailed recommendations, they recognized that while changes may be needed in building design and operation to be better prepared for extraordinary incidents, recommending any sweeping changes is ill advised at this time. The responses for individual buildings need to be examined in the context of their overall risks and existing systems.

2.3 Response

Once the risks have been determined, various actions may be done to lessen them. The types of actions to respond to the risks are frequently categorized by how they reduce the risk: prevention, mitigation, detection, and recovery. Some corrective actions may influence more than one of these types. For example, added fencing around a facility may improve prevention by blocking intruders and also improve detection through added visibility of intrusion. Sprinkler systems provide both detection and mitigation in the event of fire. Energy-efficiency measures can both mitigate the vulnerability of an individual building to power outages and collectively make the grid less attractive as a target and so deter an attack.

Since threats can include natural and accidental threats besides intentional threats, responses can be very broad. Earthquake proofing of a building is an example of a mitigation action to reduce the impact of a natural threat. Some experts expand the types of actions, such as subdividing prevention into prevention

and deterrence, or recovery into emergency response and recovery. Regardless of the details, classifying responses into this framework facilitates analysis of risks and response in infrastructure assurance.

Prevention

Prevention covers actions or assets that are used to deter or prevent threats from happening. Typical responses such as fences, gates, and locked doors all are aimed at preventing intruders access to the facility. Warning signs, while not physically preventing access, may deter intrusions and thereby prevent an attack. Maintenance programs and training are to prevent accidental threats (of equipment malfunction or operator error) from happening. Natural threats are less amenable to prevention except in certain cases, for example, ensuring proper foundation construction to prevent soil subsidence problems.

Mitigation

Mitigation reduces the extent of damage if a threat is fulfilled. HVAC improvements can help in mitigating the consequences of an airborne biological or chemical attack. A tighter building envelope reduces infiltration, thereby reducing the consequences of attack. Evacuation plans, emergency lighting, back-up generation, and energy storage are examples of actions that can reduce the consequences by protecting people during an event.

Detection

Detection covers steps taken to better identify that an attack has taken place. Security cameras and smoke detectors are simple examples, as is passenger screening at airports. Sensors for more exotic chemical and biological threats are under development to provide enhanced capabilities in detection.

Recovery

Recovery, either short- or long-term, restores the assets or functions following an incident. Examples include power restoration following a hurricane, clean up following a fire or an anthrax release, or computer data restoration from backups. Plans made beforehand that speed up recovery or make recovery more complete may fall into this category, such as spare parts inventories or automated computer backup programs.

2.4 Building Assurance and Energy Efficiency

A building is a system of barriers that protects the occupants from the environment (U.S. Army Corps of Engineers 2001). As such, a critical measure of a building's security is how well it protects the occupants during an extraordinary event. In addition, a building functions within society. To the extent that the building reduces the vulnerability of the rest of the community, that building contributes to infrastructure assurance.

Buildings themselves face three main direct threats: fire, blast, and airborne contamination. (Activities within the building, such as finance, telecommunication, etc., may face additional threats.) Recent attacks (Oklahoma City, World Trade Center, Pentagon, Hart Office Building) have all involved one or more of these intentional threats. Major potential vulnerabilities to these threats involve the building's overall design and construction, HVAC systems, emergency plans, and interdependencies with outside infrastructures. Energy-efficiency technologies can play a role in all of these. In addition, energy-efficiency measures can increase the assurance of other infrastructures beyond the building and improve the community's security.

Building level energy efficiency

At the individual building level, energy-efficiency improvements can:

- Reduce chemical/biological infiltration through a tighter envelope

- Provide better control over air flows within the building
- Improve filtration to remove airborne hazards
- Help control moisture to retard biological growth and assist recovery
- Facilitate monitoring for rapid detection and correct response during emergency
- Increase visibility during power outages through better daylighting
- Increase resiliency and independence of the building from outside infrastructures
- Pay for infrastructure assurance improvements through energy savings.

Societal level energy efficiency

At the community and regional level, energy-efficiency improvements can:

- Reduce stress at peak times on the energy infrastructure
- Provide net energy to the community to reduce reliance on centralized systems
- Make energy infrastructure a less attractive target for terrorists
- Speed recovery following emergencies.

Conflicts between building assurance and energy efficiency

Some energy efficiency improvements may lower building assurance, just as some assurance improvements may come at the expense of energy efficiency. Increased zoning of a building may create the need for oversized equipment and less natural circulation. Filters can increase the energy needed for air movement. Increased natural lighting may increase the consequences of explosions, both in terms of weaker structures and increased flying glass. If a building has a fixed budget then funds may be diverted from energy-efficiency measures to building security measures. Even just the increased focus on building security may divert attention of builders from improving energy efficiency.

3. Energy Efficiency Programs and Infrastructure Assurance

With the new emphasis on security, how does energy efficiency intersect with infrastructure assurance? DOE has major programs in both R&D and technology deployment. First, we will examine the impact of technologies being developed. Then we will consider the role of deployment programs, such as codes and standards, community and state programs.

3.1 R&D

The U.S. Army Corps of Engineers has released draft guidelines on the protection of buildings and occupants from airborne hazards (USACE 2001). The Corps identify two major release points for chem/bio agents: outside or inside the building. For external releases, it is important to be able to stop the inflow of outside air during the attack and rapidly ventilate air after the attack. For internal releases, it is important to isolate the contaminated area from other zones in the building.

The Corps guidelines list various architectural and design improvements to improve assurance. These include elevating and securing fresh air intakes, securing mechanical rooms, isolating entry and storage zones, separation of zones, securing exterior windows, single-switch controls for fans and dampers used to isolate and exhaust individual zones for sheltering in place and purging, and adding vestibules.

Buildings research is being conducted in a number of areas to reduce energy use. Improvements in HVAC systems, building envelopes, lighting, and other appliances are being developed at laboratories across the country. These technologies can be examined for the value to infrastructure assurance.

HVAC systems

HVAC systems are a major route for chemical or biological attacks. Even if the attack is not initially airborne, as at the Hart Senate office building, an HVAC system can spread the attack throughout the

facility. Properly installed, outfitted, and maintained HVAC systems are crucial for protection from chem/bio attacks.

Energy-efficiency improvements in the HVAC system provide several mechanisms to improve assurance. High-efficiency filters help to trap bacteria or fungi used in bio warfare. Filters can also include activated charcoal or other adsorption chemicals to remove chemical agents. Ultraviolet light is being used within duct systems to clean the air of pathogens. This improves efficiency and lowers costs through reduced fouling of heat exchangers, creates a healthier indoor environment, and provides ongoing protection from biological agents. However, changes to HVAC systems without consideration for efficiency can increase the energy use (e.g., through higher pressure drops or excessive UV lighting). Here, energy efficiency considerations may be needed simply to keep total energy use the same.

Desiccant systems can provide protection from bacteria or fungi by maintaining a moisture level that limits growth. In addition, they add localized heat to the air that can kill bacteria. By using specific chemicals on desiccant drums, some harmful chemicals can be neutralized. These drums could be in place continuously or just used when threat levels are raised. Besides helping with mitigation of the damage, desiccant systems can improve recovery through assistance in control of humidity during cleanup. One mechanism used in the cleanup of anthrax at post offices was steam; desiccant systems can help to remove excess moisture to reduce damage to equipment and facilities.

Improved zoning and control of airflow will limit the spread of contamination. HVAC system upgrades for energy efficiency can provide an opportunity to increase the zones of control. One approach to reducing energy use is the ability to completely turn off the air system in unused spaces. This clearly could be very useful in a chem/bio attack.

Leaky duct systems can either allow leakage into, or pull air out of, zones other than what the operator intends. Tighter duct systems prevent the cross contamination that can spread any contamination. They also improve energy efficiency through better air handling, temperature control, and filtration.

The Corps of Engineers guidance emphasizes the importance of air control in the areas where people or materials first enter the buildings. Lobbies, mailrooms, and receiving areas should have their air systems isolated from the others.

Building Envelope

Just as a tighter duct system helps prevent the spread of internal contamination, a tighter building prevents outside infiltration and gives more control of the air system to the operators of the building. One factor to consider is the pathway of outside air into the building. For low-rise buildings, an external release may send a significant fraction of the agents over the building rather than around the building. Air-intake locations need to be secured. Another factor is the chimney effect from stairwells. In summertime, the cooler air in the stairwell will force air out at the bottom, but in wintertime, stairwells will naturally pull ground-level air from outside into the building. Over-pressurization may be needed to protect the building or stairwells from infiltration from the outside.

Windows are another key factor to consider. A building with good daylighting and electric lighting controls can lower energy use, but the fragility of windows in case of explosion must also be considered. Some windows use film layers to improve their energy efficiency; the films may also be helpful in making the windows shatter resistant. Smaller windows may be more resistant to breaking, but at the expense of less natural light. Good design practices will lead to buildings that provide good daylighting and minimize energy use, but are not over glazed.

Doorways and holding areas are valuable for increasing security. Isolating the air systems in vestibules, lobbies, or other entrances to the building will better protect the rest of the building from airborne releases. Vestibules or airlock-type arrangements also improve the energy efficiency through reduction of infiltration and heating/cooling loss.

Lighting and equipment

The main benefit for infrastructure assurance of energy-efficient equipment within the building is simply the reduced need for electricity. This benefits the building by lessening its dependence on the external grid. In cases where backup or emergency power is used by the building or by various equipment, higher efficiency increases the time that the equipment can be run before the backup source is depleted. Higher efficiency also helps by lessening the stress on the country's energy infrastructure during peak times. A building with good daylighting has the added benefit of making the building safer during a power loss because of increased visibility. Another potential technology is motion-controlled efficient outdoor lighting. This may offer better detection than constant lighting while saving energy. Photovoltaic (PV) powered outdoor lighting does not rely on the external grid.

Building-integrated energy supply systems

If buildings can become more independent from the central power system, then they are more likely to stay up and running despite the loss of the grid. This resiliency adds to infrastructure assurance, not just for the building itself but also for the infrastructures that use the buildings. If the building houses systems such as computer systems, telecommunications, financial systems, hospitals, law enforcement, or fire protection, then the redundancy and independence of the power system will help protect those critical infrastructures from the risks of interdependencies.

Even if the buildings are not crucial to the maintenance of vital infrastructures, the reduction in demand for power from the grid will relieve congestion and lessen the likelihood of an overstressed system. Residences or commercial buildings that generate power during peak times reduce the amount of power that needs to be carried on the transmission and distribution grid. Since these grids have seen increasing stress due to inadequate upgrades, any locally generated power will be helpful. In fact, if the houses or buildings could generate more power than needed (the 120% building), then these buildings could even provide power for neighboring buildings and support their functions in the event of an emergency.

There are several approaches for integrating energy supply into buildings. Distributed generation (DG) where the systems only provide electricity are frequently used as backup generation sources in buildings with critical needs. Hospitals, control centers, military facilities, or law enforcement buildings may have emergency diesel or turbine generators in case of sudden power outages. Fuel cells are currently under development that should provide highly reliable power at a scale appropriate for a single building.

PV systems incorporated into buildings can also lessen the need for grid power in buildings. Since PV systems will generate the most power at times of peak sunlight and consequent cooling needs (and peak grid demand), their power is especially valuable. Since PV systems may initially generate only a portion of the needs for the building, it may be designed to charge batteries for emergency backup. This assures that the redundancy the PV system provides is directed towards the most critical needs of the building, extending the time that emergency backup power can be provided. The PV power generated once the batteries are full can offset the building load. Research is still needed to make PV systems affordable, but the infrastructure assurance aspects provide additional incentive for their use.

Any building- or personal-level energy storage technology can provide additional mitigation and recovery support for buildings. Uninterruptible power sources are already frequently used in numerous building sectors. These can range from small battery systems for individual computers to large batteries or ultra capacitors for main computer systems or other critical equipment. DOE conducts extensive research in the improvement of energy storage technologies.

Combined heat and power (CHP) systems both generate electricity and provide thermal energy for steam heat, industrial processes, or absorption chillers. These systems can use the same prime movers as in distributed generation, with extra equipment to utilize the exhaust heat. The energy-efficiency gains from using the heat that is largely wasted at central power plants improves society's infrastructure

assurance through lower energy needs. Not only is electricity demand reduced, but the use of primary fuels (mainly coal or natural gas) is also reduced. Since the electric and natural gas infrastructures could be highly susceptible to attack, any steps to minimize reliance on them will improve assurance. Thus, having the on-site prime movers diversifying the fuels that they can run (e.g., bio-diesel) would improve their contribution to security. Since CHP systems interact with the HVAC system, introducing CHP provides an opportunity to upgrade HVAC systems at the same time.

One concept being studied by DOE that would enhance the value of distributed generation and CHP is microgrids (or μ grids). Current utility policies typically require distributed generation to disconnect from the grid in the event of problems, for a variety of reasons. Connecting multiple loads and generation sources into a semi-autonomous microgrid that jointly appears as a single load or resource on the overall grid could boost the reliability and quality of power. In the event of a broad outage, more buildings could remain powered using the microgrid, lessening the consequences.

Integrated Energy Management

Using an integrated energy management system for an entire building provides opportunities for energy savings through control of lighting and HVAC systems. The system can also include upgrades for assurance, such as sensors for chem/bio agents, fire and smoke detectors, single switch control of fans and dampers, and public announcement systems. This provides significant improvement in its overall functionality and can help to justify its development. DOE-sponsored models for evaluation of building energy performance could be enhanced for security issues and incorporated into energy management tools. They could include building simulations, airflow models, moisture detection and analyses, and HVAC performance models.

Integrated management systems can provide assistance in detection through widespread sensors that feed information into a central point. Visualization of readings or an automated expert system can more quickly identify a problem. Unusual patterns that may indicate a problem can be captured whereas individual systems may not combine these data. A pre-developed emergency action plan can be called up from a database of potential actions, depending on the specific incident. Fans and dampers for specific zones can be shut, evacuation or shelter-in-place announcements can be made, and emergency responders notified. These actions help both in mitigating the consequences during the event and speed recovery afterwards.

3.2 Summary matrix

As mentioned above, each technology can have an impact in one or more of the different responses to risks, be they from threats, vulnerabilities, or consequences. Table 1 shows a matrix identifying the major energy efficiency technologies and the response type they address.

While this matrix was developed by considering the technologies first and determining the types of responses they address, another analytical approach could be to start with the different types of response (prevention, detection, mitigation, recovery plus any subsets) and then see what programs DOE has or could pursue that may assist that response. More technologies and further details on their support of (or conflict with) the responses could be added to the matrix.

Table 1: Matrix showing building technologies and types of infrastructure assurance they address.

Technology	Prevention	Mitigation	Detection	Recovery
Any Energy Efficiency Technology	Lessens attractiveness of grid as target, lowers overall energy use	Lessens stress on power grid		Lowers amount of power needed for restoration
Advanced HVAC filters		Neutralize chem/bio weapons	Sensors identify attacks	Rapidity of cleaning air
Desiccant systems		Lessens spread of bio agents		Lessens damage from clean-up (e.g., steam, ClO ₂ gas)
Zoning and duct systems	Elevate and secure air intakes	Rapid closure reduces infiltration and cross-contamination	Duct sensors identify agents	Rapid flush of agents
Building envelope	Secure entry ways	Lower infiltration, add overpressure, added strength increases blast resistance		Stronger buildings suffer less damage so quicker to recover
Lighting and equipment		Improve visibility during emergency, longer backup operation	Motion-controlled efficient lighting	
Distributed generation		Continued power if grid lost, can provide power to other buildings	Monitoring of grid connection may give early warning	Supplies building following incident
PV and energy storage		Saves critical processes if grid lost	Activation can warn of interruption	Speeds recovery since critical files or systems not lost
Combined heat & power		Continued power and other services if grid lost, can provide power to other buildings	Monitoring of grid connection may give early warning	Supplies building following incident, including HVAC
Microgrid		Expands supply from DG and CHP to other buildings		Expands supply from DG and CHP to other buildings
Energy management systems		Whole building responses can be activated quickly to lower impact	Central system detects, reports problems, whole building view sees patterns	Zone control can isolate problems

3.3 Deployment Programs

Given that technologies could assist in both energy efficiency and infrastructure assurance, how should they be deployed? How does the information get distributed and new practices put into place? Some initial steps are already being taken. We mentioned that ASHRAE has developed draft risk management

guidance (ASHRAE 2002), and that the Corps of Engineers has developed draft guidelines for protecting buildings (USACE 2001).

Note that both of these documents are in draft form. Concepts regarding infrastructure assurance for general buildings are still new enough that definitive rules should not be put in place. Two recommendations from the ASHRAE paper stand out: what ASHRAE should NOT consider:

- Any changes in building codes to address issues of health and safety under extraordinary incidents.
- Requiring, or even recommending, that buildings be designed to enhance safety under extraordinary incidents **without** careful consideration of such parameters as initial and maintenance costs, energy consumption, indoor air quality, and site adaptability.

Michael Ivanovich, Editor-in-Chief of *Heating/Piping/Air Conditioning (HPAC) Engineering*, has written an article on “How to Make Buildings More Resilient to Airborne Chemical and Biological Releases” (Ivanovich 2002). He uses a frequently-asked-question approach that is targeted at building owners and managers. He includes discussions on threats, resiliency measures, action plans, and HVAC system improvements (quoting from the USACE and ASHRAE papers.) He concludes with a call for building professionals to become more knowledgeable and active in homeland defense discussions with government.

The Buildings Program, through its outreach programs, could assist in deploying energy-efficiency technologies that also improve building assurance. Energy-efficiency programs that may be marginal on a cost basis alone may be successful if they also promote security. At the very least, Buildings programs could work to prevent the downgrading of efficiency in the pursuit of building security. EERE’s Building Program roles are also discussed in section 5.

4. Stakeholder Roles

Historically, the major group studying infrastructure assurance for buildings has been the military. They have had to address the issue of protecting buildings both in this country and overseas for decades, if not centuries. However, they too have to learn and adapt as technologies change. The Defense Advanced Research Projects Agency (DARPA) is one of the major research arms for the military. Its Special Projects Organization has created a project for “Integrated System Experimentation for Immune Buildings.”

This program seeks to make military buildings (such as barracks, office buildings, and Command and Control centers) far less attractive targets for attack by airborne/aerosolized chemical or biological warfare agents (CWA, BWA), by modifying and augmenting building infrastructure to greatly reduce the effectiveness of any such attack. The main DARPA focus is on the challenging problem of protection from internal releases. Infrastructure modifications/augmentations could include changes to the ordinary HVAC infrastructure – such as real-time, active control of airflow patterns, and/or full-time, passive, highly efficient filtration – in addition to whatever other modifications might be appropriate – e.g., real-time neutralization of the aerosolized agent, or networked surveillance systems. The program has three goals: to protect the human inhabitants of such buildings in the event of an attack; to restore the building to full function as quickly as possible after the attack; and to preserve forensic evidence for treatment and retaliation. (DARPA 2001)

Currently under Phase II of this project, Battelle and Bechtel are each building test beds to integrate and evaluate various technologies in a military setting using former barracks. These will be operational July 2002. The integrators are currently examining potential technologies to include in these test beds.

Technology applications were submitted to DARPA as part of Phase I. These, plus others that the integrators select, are candidates for inclusion in the test beds.

As mentioned above, the Army Corps of Engineers and ASHRAE have both published guidance for building protection. The Corps is involved with military facilities and has a broader view towards protection of civilian facilities as well. ASHRAE has as its mission advancing the arts and sciences of heating, ventilation, air conditioning and refrigeration for the public's benefit. Building owners, operators, and public safety organizations are also concerned about the performance of building functions. Insurance companies have long studied risk management issues involving the buildings they insure. Some have made forays into evaluation of energy-efficiency measures that can lower a building's risk, although not necessarily in the context of intentional threats. Lawrence Berkeley Laboratory personnel have written several papers analyzing the insurance industry's participation in energy-efficiency and renewable energy products (Mills 2001, Vine et al. 1998).

Energy-efficiency technology development is carried out through DOE's EERE office. There has been a recent reorganization within the office such that previous organizational titles are not applicable. For this paper, we have assumed there will continue to be a concentration of research on buildings technologies in a "Buildings Program" office. In addition, distributed energy resource development is conducted through EERE's Office of Power Technologies. DOE's Federal Energy Management Program (FEMP) provides technical assistance and financial advice to federal agencies to help agencies meet their mandates to reduce energy and water use. With the recent reorganization, actual programmatic structure may be different from this.

5. DOE and Buildings Program Role

A key question asked by BTS for this paper was "Does DOE (and specifically BTS) have a role in addressing issues of security for the built environment?" Five reasons for DOE's involvement in addressing security in buildings are:

1. As shown above, systems that are the focus of DOE's building research are important in the understanding of risks related to buildings. HVAC, building envelopes, equipment, monitoring controls, among others, can all play a part at making buildings more secure.
2. Just as energy-efficiency technologies may improve (or degrade) security, security improvements can have an impact on energy-efficiency of buildings. DOE is in a useful position to evaluate both factors at the same time to see their relationship.
3. Buildings can contribute to the assurance of other infrastructures. For example, since buildings consume roughly a third of energy in the U.S., any improvements in building efficiency will have an impact on the energy infrastructure.
4. DOE and its contractors own or control a significant number of buildings across the country, with many of the facilities heavily involved in national security. These can provide significant opportunity to utilize these facilities as testbeds or to explore alternative designs and operations.
5. DOE is responsible for the national laboratories, which encompass some of the best scientists and technologists in the world and who can be a significant resource to address national interests in safe and secure buildings.

While many of the energy-efficiency technologies discussed above are the purview of other EERE programs, what is the Buildings Program role in advancing assurance in the buildings area? How can it include security in the development of its technology portfolio and deployment programs? What are the short-, mid-, and long-term actions the Buildings Program can take? Clearly there is an intersection between energy-efficiency technologies and building assurance. Protecting buildings from extraordinary events obviously makes "communities more livable", to quote from the BTS mission statement.

Technology development can be steered to incorporate assurance into its benefits. Deployment mechanisms require further study. Codes and standards are not developed yet and research could be undertaken to understand the issues involved. State Energy Programs such as Build America and Rebuild America could begin to incorporate information on the issues, such as that from ASHRAE, the Army Corps of Engineers, or this paper. These programs provide a natural outlet for distribution of information to states and communities on infrastructure assurance and buildings.

As an initial step, a method for classifying the risks that any specific building faces could be developed, as described in Sect. 2.2. This type of evaluation is carried out currently in some cases, but rarely from a security standpoint addressing the risk from intentional threats. This risk assessment template could help building owners, operators, and other stakeholders understand the threats, vulnerabilities, and consequences a building faces, allowing them to weigh the amount of protection they feel necessary. This template could be used in a combined energy/security audit, providing the opportunity to identify technologies that can help make the buildings either more energy efficient, safer or both. Some technologies that may be marginal with regard to one aspect or the other may prove to be of value when both functions are considered. However, combined audits may raise difficulties in protection of information.

A list of programmatic options that could be pursued by the Buildings Program was provided by Landis Kannberg of Pacific Northwest National Laboratory. A number of these options were also mentioned by other experts. The list includes ideas presented above, such as a risk characterization template, information dissemination, and codes and standards research. It also calls for extending research by evaluation of other organizations and facilities with long experience in securing critical functions.

- Developing a risk characterization methodology for the building industry, owners and operators that helps determine the relative robustness of energy related systems to various hazards/threats. This would require careful consideration of what building systems would contribute to making a structure more or less risky under various conditions.
- Aggregation and dissemination of readily accessible information related to building assurance to guide states and communities on what they can do. EERE has excellent delivery mechanisms for such information, and cities and states would likely welcome such information with open arms.
- Review new DOD building specifications to determine their impact on energy consumption, likelihood of deployment of various energy technologies, and opportunities for development and use of other energy technologies or building design features.
- Issuing a call for concepts that would enhance the energy performance of the building while also improving the risk condition of the building, then funding the preliminary analysis of the best of these concepts. Alternatively, if there are specific technologies known to increase risk, another solicitation could focus on alternatives to these technologies. A companion solicitation might be for retrofit technologies that would enable reduction of building risk. This might include emergency HVAC partitioning, positive pressure air source supplements, emergency circulation and lockouts, etc.
- Analysis of ancillary benefits that buildings could offer to support local infrastructures. An example is grid-friendly appliances that control their operation to ensure electric grid reliability, or facilitate recovery following an outage. The same could be done for other building functions where graceful degradation of services would be an orchestrated and planned activity.
- Analysis of emergency response measures that might be implemented by HVAC and other building energy related systems to increase safety or enhance survival of building occupants or critical systems. Linkage with DARPA, which is already funding research and studies in this area would be desirable.
- Rapid consideration of the codes and standards to enable adoption of emergency response HVAC (and similar energy related) systems. For instance installation of emergency air filtration systems that are

not energy efficient but are highly effective preventive measures for controlling spread of toxic materials. They would only be employed during an emergency. Amendment of code requirements to accommodate such systems might pave the way for wider adoption.

- Initiating a program to compare low-risk (secure and survivable) building designs and technologies employed for high threat or high consequence functions (such as embassies, military control centers, telecommunication control centers, etc.), and contrast measures employed there with technologies advanced under the DOE EERE banner. Again DARPA and other agencies are already conducting analyses on this topic (some of it classified). Lessons learned from the comparison might be valuable for directing EERE efforts.
- Evaluating the practices in other countries that have experienced far greater degrees of terrorist activity to determine if there are any systemic design features that differ from U.S. practice and that might be useful for U.S. implementation.

In the longer term, the “120% Building” concept, if expanded to encompass infrastructure assurance, could provide a unifying framework for building R&D. If individual buildings provide more power than they need, they provide a significant resilience to the energy infrastructure. Incorporating concepts of protection for occupants and the facility’s functions will enhance the value of such a program.

6. Uncertainties and Information Gaps

While building assurance has been examined for many years in the military, applying the concept to the private sector is only just beginning. Since most buildings do not face the threats that the military does, and because the cost varies tremendously for adding different levels of assurance, much research is needed to measure the levels of risk management needed. At the same time, too much detail on threats and vulnerabilities can create very sensitive or even classified information. Efforts are needed on how to balance information security and information availability so that the appropriate information, and only the appropriate information, is supplied to the appropriate people, and only the appropriate people.

Furthermore, buildings have a wide array of functions that could be compromised by excessive attention to security. For example, commercial buildings cannot afford to make their customers undergo excessive screening or delays. Since businesses are profit-driven, any security enhancements must be cost-effective. Energy efficiency can play a significant part in this through cost savings. However, the security aspects of the efficiency technologies must be understood, explained, and optimized. Adding security issues into the goals of energy efficiency R&D is needed.

7. Summary

With the increased emphasis on security following September 11, DOE organizations are asking how their programs intersect or should intersect with DOE’s mission of security. Many in the energy efficiency field have not had to consider the topic before, so a basic description of infrastructure assurance and vulnerability assessments is useful.

Risk can be thought of as the combination of threats, vulnerabilities, and consequences that a building faces. These risks can be targeted at the building’s physical assets, cyber assets, systems interconnectedness, or interdependencies with other infrastructures. A vulnerability assessment measures the risk that a building faces, and can be simple or complex, broad or narrow. Various responses to alleviate those risks can be categorized by type: prevention, mitigation, detection, and recovery.

Numerous energy-efficiency technologies can also improve infrastructure assurance from intentional attacks. HVAC system performance is crucial for improved protection from chemical or biological attack. Improved zoning, tighter ductwork and building envelopes, high efficiency filters, UV light, desiccant systems, and rapid control of fans and dampers can all mitigate the consequences or speed recovery. Distributed energy resources can make the building more resilient from power grid attacks, as well as

lower the peak stress on the grid. Energy management systems can be enhanced to incorporate emergency response systems that help protect the occupants and facilities. Cost savings from energy efficiency technologies can help pay for the enhancements for security, providing additional benefits to building owners and occupants.

The military has long studied the security of buildings, and other stakeholders such as ASHRAE have started to get involved. However, incorporating assurance into commercial and residential buildings on a broad scale has not been widely addressed, especially incorporating the lessons from September 11. The EERE could play a role by incorporating assurance into its analyses and technology development. Its contacts and ongoing relationships with states and communities provide a natural outlet for distribution of assurance-related information. Together, these activities can incorporate DOE's security mission into the EERE Buildings Program.

8. References

- American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) 2002, *Risk Management Guidance for Health and Safety under Extraordinary Incidents*, Atlanta, GA, January 12. <http://ashrae.org/about/task_force_rpt_12jan02.pdf>
- Defense Advanced Research Projects Agency (DARPA) Special Projects Office, 2001, *Immune Building Program*, <<http://www.darpa.mil/spo/programs/immunebuilding.htm>>
- Ivanovich, Michael, 2002, "How to Make Buildings More Resilient to Airborne Chemical and Biological Releases", *Heating/Piping/Air Conditioning (HPAC) Engineering*, in press.
- Mills, Evan 2001, *The Insurance and Risk Management Industries: New Players in the Delivery of Energy-Efficient and Renewable Energy Products and Services*, LBNL-43642, Lawrence Berkeley National Laboratory, Berkeley, CA, November.
<http://eetd.lbl.gov/EMills/PUBS/Insurance_Case_Studies.html>
- Office of Critical Infrastructure Protection (OCIP) 2001, *Energy Sector Critical Infrastructure Protection Research and Development Agenda*, Department of Energy, September.
- President's Commission on Critical Infrastructure Protection (PCCIP) 1997, *Critical Foundations: Protecting America's Infrastructures*, Washington, DC, October.
- U.S. Army Corps of Engineers (USACE) 2001, *Protecting Buildings and their Occupants from Airborne Hazards*, DRAFT, TI 853-01, October.
<<http://buildingprotection.sbcom.army.mil/basic/index.html>>
- Vine, Edward, Evan Mills, and Allan Chen 1998, *Energy-Efficiency and Renewable Energy Options for Risk Management and Insurance Loss Reduction: An Inventory of Technologies, Research Capabilities, and Research Facilities at the U.S. Department of Energy's National Laboratories*, LBNL-41432, Ernest Orlando Lawrence Berkeley National Laboratory, Berkeley, CA, August.
<<http://eetd.lbl.gov/CBS/Insurance/LBNL-41432.html>>